

Sheffield Hallam University

Digital accountability for LEAs: balancing technical possibility, legal permissibility and societal acceptability

SAMPSON, Fraser

Available from the Sheffield Hallam University Research Archive (SHURA) at:

<http://shura.shu.ac.uk/27861/>

A Sheffield Hallam University thesis

This thesis is protected by copyright which belongs to the author.

The content must not be changed in any way or sold commercially in any format or medium without the formal permission of the author.

When referring to this work, full bibliographic details including the author, title, awarding institution and date of the thesis must be given.

Please visit <http://shura.shu.ac.uk/27861/> and <http://shura.shu.ac.uk/information.html> for further details about copyright and re-use permissions.

**Digital Accountability for LEAs: Balancing Technical Possibility, Legal
Permissibility and Societal Acceptability**

Fraser Sampson

**Published works submitted in partial fulfillment of the requirements of
Sheffield Hallam University for the degree of
Doctor of Philosophy on the
Basis of Published Work**

June 2020

I hereby declare that:

1. I have not been enrolled for another award of the University, or other academic or professional organisation, whilst undertaking my research degree.
2. None of the material contained in the thesis has been used in any other submission for an academic award.
3. I am aware of and understand the University's policy on plagiarism and certify that this thesis is my own work. The use of all published or other sources of material consulted have been properly and fully acknowledged.
4. The work undertaken towards the thesis has been conducted in accordance with the SHU Principles of Integrity in Research and the SHU Research Ethics Policy.
5. The word count of the thesis is 65,000.

(Signature) F. Sampson

Name	<i>Fraser Sampson</i>
Date	<i>June 2020</i>
Award	<i>PhD</i>
Faculty	<i>College of Business, Technology & Engineering</i>
Director(s) of Studies	<i>Professor Dave Waddington</i>

Contents

Abstract	5
Critical Appraisal	6
Overview of Research Theme	6
Theoretical Position	7
Research Methodology	9
Research Method	11
Original Independent Contribution to Knowledge	12
Conclusion	14
Note regarding co-authored works and research carried out in collaboration with others	15
Analysis of the Publications, their contribution and synthesis	17
Item 1	17 - 18
<i>"Plotting Crimes: too true to be good? The rationale and risks behind crime mapping in the UK."</i> in Policing: a Journal of Policy and Practice, Oxford University Press 2010 Vol 4 Issue 1 pp15-27 https://doi.org/10.1093/police/pap015 (with Kinnear, F)	
Item 2	18 - 19
<i>"Cyberspace: the new frontier for policing?"</i> 2015, Chapter 1 pp 1-10 in "Cyber Crime and Cyber Terrorism Investigators' Handbook Akhgar, B., Staniforth, A., Bosco, F. (Eds) Elsevier eBook ISBN: 9780128008119 Paperback ISBN: 9780128007433	
Item 3	19 - 20
<i>"The Legal Challenges of Big Data Application in Law Enforcement"</i> 2015, Chapter 15 pp 229 – 237 in "Application of Big Data for National Security – A Practitioner's Guide to Emerging Technologies." Akhgar, B., Saathoff, G., Arabiana, H., Hill, R., Staniforth, A., Bayerl, S. (Eds) Elsevier eBook ISBN: 9780128019733 Paperback ISBN: 9780128019672	
Item 4	20 - 21
<i>"Whatever You Say...The Case of the Boston College Tapes and How Confidentiality Agreements Cannot Put Relevant Data Beyond the Reach of Criminal Investigation."</i> in Policing: A Journal of Policy and Practice, Oxford University Press, 2016 Vol 10 Issue 3 pp 222-231 https://doi.org/10.1093/police/pav034	

Item 5	21 - 23
<p><i>“Intelligent Evidence: Using Open Source Intelligence (OSINT) in Criminal Proceedings”</i> in The Police Journal: Theory, Practice and Principles 2016 pp 1-15 Sage Publications https://doi.org/10.1177/0032258X16671031</p>	
Item 6	21 - 23
<p><i>“Following the Breadcrumbs: Using Open Source Intelligence as Evidence in Criminal Proceedings”</i> Chapter 18 in “Open Source Intelligence Investigation – From Strategy to Implementation.” Akhgar, B., Bayerl, S., Sampson, F (Eds) Springer 2016 ISBN 978-3-319-47671-1</p>	
Item 7	23 - 26
<p><i>“The ATHENA Equation – Balancing the Efficacy of Citizens’ Response to Emergency with the Reality of Citizens’ Rights.”</i> in The Police Journal: Theory, Practice and Principles 2017 pp 1-19 Sage Publications https://doi.org/10.1177/0032258X17701321</p>	
Item 8	23 - 26
<p><i>“Legal Considerations Relating to the Police Use of Social Media”</i> (with Lyle, A), pp 171-188 in “Application of Social Media in Crisis Management: Advanced Sciences and Technologies for Security Applications” Akhgar, B., Staniforth, A., Waddington, D (Eds) 2017 Springer International Publishing, Switzerland ISBN 978-3-319-52418-4 ISBN 978-3-319-52419-1 (eBook) DOI 10.1007/978-3-319-52419-1 Library of Congress Control Number: 2017932904</p>	
Item 9	26 - 27
<p>Principles for Accountable Policing – a taxonomy of legal and ethical principles of practical use to the police and oversight bodies and the public Accepted by the Scottish Universities Insight Institute Oct 2019 https://www.ScottishInsight.ac.uk/Programmes opencall201516/principlesofaccountablepolicing.aspx</p>	
Appendix	28
The Published Works (numbered as above).	
References from Critical Analysis	226-227

Abstract

The expansive proliferation of social media, electronic devices and data processing capabilities has presented Law Enforcement Agencies (LEA) with a dilemma. On the one hand there is a need for/opportunity to expand capability, adapting practices and policies to capitalise on what is now technically possible (not only in the application of data technology but also in the context of what can be achieved within the technical conventions of the law), utilising citizens' data and actively encouraging their collation and sharing as part of everyday community policing. On the other, the development in data technology has been accompanied by a rapid expansion in public expectation and a need for greater legal regulation, all combining to bring an important extension of police accountability. The focus of the research is thus how can LEAs balance that which is technically possible against what is legally permissible and societally acceptable?

Moving from the known to the needed, the published work draws upon and addresses the size and shape of the dilemma, identifying gaps and supplying "evidence-informed management knowledge" (Tranfield *et al* 2003) at both an individual and organisational level. Providing a themed and coherent new praxis for LEAs the work identifies how LEAs must balance the availability of data with the rapidly increasing public expectations of privacy, security, confidentiality and accountability, collecting and connecting the qualitative knowledge and practice that resides in distributed places and people, in order to establish a previously unrecognised body of work that focuses on both opportunities and obligations, in order to promote an understanding of the 'law in context' and ultimately increase police effectiveness. The direction of the work follows a series of influences and confluences, tributaries and deltas of change flowing towards the same unequivocal destination: an original contribution to "*knowledge about the traditional elements of the law and also about the quickly changing societal, political, economic and technological ... aspects of relevance.*" (Langbroek 2017).

References

Tranfield, D., Denyer, D., Smart, P. 2003 "Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review" *British Journal of Management* vol 14 pp 207-222
Langbroek, P., van den Bos, K., Thomas, S.M., Milo, M & van Rossum, W "*Methodology of Legal Research: Challenges and Opportunities*", *Utrecht Law Review*, Volume 13, Issue 3, 2017

Critical Appraisal

Introduction

Writing the foreword to mark the launch of the *Blackstone's Police Manuals* - a series of professional knowledge texts that I researched, designed and authored for the police service (Sampson 1998) Chief Constable Peter Hermitage provides a backdrop to my specific work submitted here. Pointing out that: "Knowledge is a prerequisite for policing. If the police are to be effective players within the Criminal Justice System then they need to know and understand the legal framework in which they work." Hermitage, as the first Director of National Police Training, identifies a clear link between the operational efficacy of Law Enforcement Agencies (LEA) and the extent to which their actors understand the legal parameters which delineate their operating environment. Since the launch of the Blackstone's Manuals both variables - knowledge and legal framework - have changed almost beyond recognition and the published work submitted here has sought to explore, identify, explain and apply one critical aspect of that prerequisite.

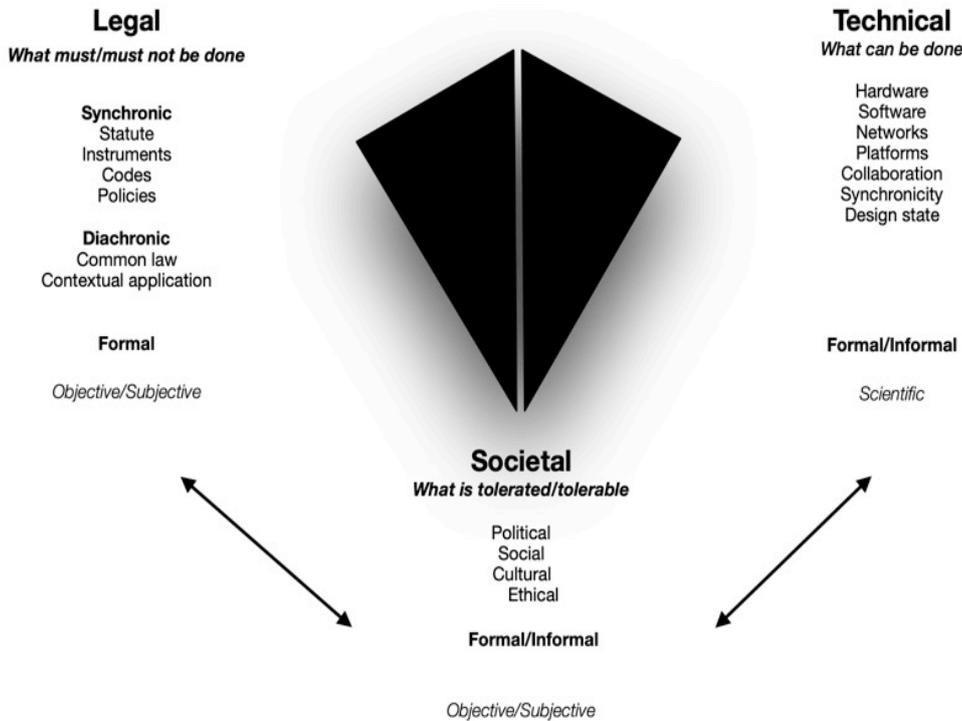
Overview of Research Theme

My research theme arises from the recognition that the proliferation of social media, the ubiquitous everyday use of portable electronic devices and the exponential expansion in capabilities for data processing have presented Law Enforcement Agencies (LEA) with a fundamental dilemma. Developments in data processing have brought both a pressing need and an unparalleled opportunity for LEAs to expand their capability, adapting practices and policies to capitalise on what is now technologically possible, not only utilising the yottabytes of citizens' data now available to them cheaply and quickly, but also actively encouraging data sharing as part of everyday community policing. At the same time, the burgeoning development in what can be achieved technologically has brought a rapid expansion in public expectation and legal regulation of data processing by the police who must work within the existing legal parameters most of which remain sets of 'analogue' rules to be applied in an increasingly digital world, all of which has become an important extension of police accountability. My critical research question is how LEAs can begin to balance the triptych of that which is possible against what is permissible and acceptable and what specific legal knowledge is needed by practitioners, managers and their respective organizations. This is a new and rapidly developing area of accountability for LEAs and the body of work in which I answer the research question, identifying the direction of those developments, together with posited considerations and practical solutions, is an original contribution to knowledge.

Theoretical Position

The theoretical position from which I have approached my research question is this: that LEAs must balance the technically *possible* against the legally *permissible* and societally *acceptable* in order to be publicly *accountable*. Doing so requires a careful analysis of the component parts which can often operate in divergent and interdependent ways as set out in the diagram below:

Theoretical Position



While each of the elements would lend a viable and valuable ‘lens’ through which to examine and evaluate the dilemma, the frame of reference from which I have chosen to apply my theoretical position and analyse the issues in my research question is primarily a legal and jurisprudential one. The legal and jurisprudential aspect brings a mixed approach of both formal, synchronic objectivity in terms of the law as is and the subjective diachronic application of it to a set of given circumstances under consideration by a court, (see Methodology *infra*), linking with and representing a form of societal acceptability at least insofar as that is understood and given effect by the court. This frame of reference thus addresses societal acceptability in this context, however some of the work also identifies how this concept extends far more widely as discussed in the practical projects such as ATHENA where participants in a 3-year research programme found some aspects of what was being proposed to represent an unacceptable request for LEA use of their data and also within my contribution to the Principles for Accountable Policing which followed on from my research. However, it is important to note that a subset of societal acceptability is political acceptability, both in general (in terms of ministerial accountability) and specifically in the setting of this policing areas having a governance model that centres around locally-elected officials. There is also that element of political possibility which manifests itself in the policy considerations driving legislation which in turn will extend/limit the use of new technologies. The theoretical position of my work is therefore largely focused in the area represented by the asymmetrical directional arrows in the lower left quadrant of the diagram. The socio-political and technical interaction - both formal and informal - as represented by the arrows in the bottom right of the diagram are not addressed and lend themselves readily to further viable and valuable research in the future.

The Dilemma

By way of practical illustration, on 8 September 2020 the elected PCC for Cleveland resigned unexpectedly and with immediate effect¹. The reason for his doing so was that he had been using a social media platform (WhatsApp) to conduct official business during the restrictions of the Covid-19 pandemic. The platform offers ‘informal’ group conversation capabilities within a secure, end-to-end encrypted environment using participants’ own devices and offering as technically capable and suitable a solution as any formal data processing facility, thereby meeting the element of the technically possible. There was nothing inherently ‘unlawful’ in the use of this technology and in fact it had been used successfully by many public bodies during the pandemic, thus satisfying the element of formal legal permissibility. The reason then why it impelled the resignation of the Commissioner was the third dimension, the informally unacceptable nature – politically, and more broadly societally - of his admitted use of the platform which enabled the routine deletion of messages at the end of each week. While it might be argued that this deletion practise was itself in accord with legal data protection protocols and international framework for data retention, the *societal* aspects of this data solution were to prove fatal to his continuing in office as a publicly accountable police and crime commissioner. And this vignette encapsulates precisely the dilemma for LEAs identified and addressed throughout my work.

Identifying the specific legal issues that my research question presents for LEAs, my work has delineated the extent and implications of the relevant knowledge requirement in order that operators can know and understand the law and legal framework when balancing the technically *possible* against the strictures of legal *permissibility* and the risks of societally *acceptable* in order to be publicly *accountable*. The submitted work achieves this in the following way:

First I have identified the dilemma itself, illustrating how it has emerged in criminological form from within the wider meta-evolution that has taken place within the communities on whose behalf the police operate and on whose active cooperation the police depend. Secondly, my research has identified and illustrated how, in order for LEAs to improve capability and exploit opportunity (the ‘possible’), many well-established, taken-for granted, legal considerations within the current ‘knowledge requirement’ for police officers (Hermitage 1998) will need to be revisited, technical considerations such as jurisdiction over criminal offences, rules of evidence and the role of criminal intelligence, the availability of inculpatory data sets that may prove – or disprove – criminal liability, the data entitlements of suspects and citizens at large and even fundamental human rights such as those preserved for remand prisoners to examine and understand the case against them. My work shows how, where and why these ‘givens’ need to be re-evaluated against the technological realities of the context in which the police now operate. Former staples of criminal investigation (a geographically static crime scene, an offender with a single, verifiable identity etc.) will have to be re-thought in the setting of Big Data capabilities, cyber crime and cyber-enabled crime.

Turning next to the dilemma’s second aspect (‘permissible’), I have researched and identified new areas of law such as those governing the collation, protection and processing of citizens’ data and how they have brought specific requirements for LEAs which they must understand if they are to be effective, along with further challenges in the areas of intelligence, prosecution and accountability, requirements and challenges which, if left unaddressed, will have a significant impact on the ability of LEAs to meet the first aspect of the dilemma and be “effective players in the Criminal Justice System”.

¹ <https://www.bbc.co.uk/news/uk-england-tees-54071912>

And finally, I explore and address the dilemma's third aspect: what are the boundaries within which society expects the police to operate ('acceptable'). The litigation literature demonstrates a growing unease and mistrust of LEAs as Big Data capabilities have grown, a feature borne out by my own research.

In identifying and illustrating the dilemma, defining the legal parameters and proposing very practical new ways of achieving a balance, my published work tracks the dilemma from the genesis of the conundrum with the arrival of community crime mapping in which I was involved in 2009/10, the early challenges of legal 'technicalities' such as jurisdiction represented by 'cyberspace', the subsequent developments in community demand for access to wider data sets held by the police and the rapid 'digitization' of communities, through practical settings such as criminal intelligence and social media, building towards a substantial example of the legal framework in action (in a three-year European Commission funded project) and culminating in a multi-jurisdictional research programme to produce a taxonomy of Principles for Accountable Policing across democratic societies in which the research theme is specifically enshrined. This then is the research theme. My methodology and method are set out below.

Research Methodology

"A precondition for legal research in any form has become that the researcher should *not only have knowledge about the traditional elements* of the law, but also about the *quickly changing societal, political, economic and technological contexts and, possibly, other aspects of relevance.*" (Langbroek *et al.* 2017) [emphasis added].

My work both follows and exemplifies this observation particularly in relation to the socio-political and technological issues as described above. Although legal rules are necessarily expressed in general terms as Hart's (1961) well-understood 'open texture', I have not been engaged here in classical nomothetic legal research to identify general laws of equal applicability but have very much focussed on the application of a complex system of established 'analogue' laws and principles within the rapidly developing digital societal, political and technological "contexts" as they affect the law enforcement community. This has necessitated an idiographic approach in part, researching and analysing the facts of very specific events and cases and conducting an examination of the underpinning law before constructing an explication of how both individual data-specific laws and established general principles (pure law) can and must be deployed in these situations (applied law). My published work has necessarily involved *a combination of knowledge management methodology* (Holsapple & Joshi 2002) and legal research (Arthurs 1983; Chynoweth 2008; Langbroek *loc cit*), identifying core critical legal knowledge, categorising and cataloguing laws, legal principles and cases; revealing both opportunities and obligations by processes of research and practice, positing solutions, evaluating options and promoting new approaches to individual, group and ultimately organisational effectiveness.

Within the work there is an element of doctrinal research² both below the horizontal axis (legal theory) and necessarily above it (expository) of the Arthurs legal research matrix at *fig 1*. Such research is consistent with both the publication of 'academic' legal texts and the dominant form of legal research generally (Chynoweth).

² adopting a definition of doctrine as "*a synthesis of various rules principles or norms interpretive guidelines and values*" (Mann 2010)

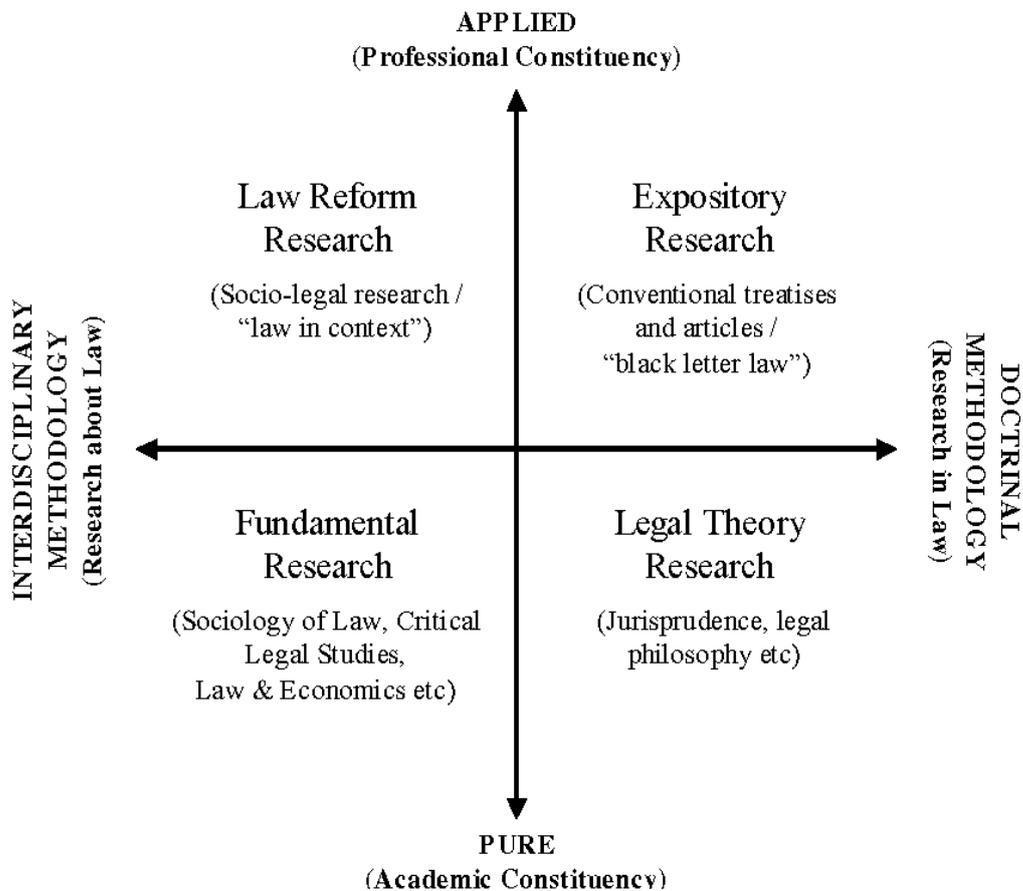


fig 1 Arthurs (1983)

Utilising both Arthurs' (*op cit*) internal approaches – doctrinal research methodologies studying the texts of the law from the inside ('what the law is') and external approaches - empirical research methodologies studying how that law works in societal contexts from the outside I have researched the specific legal issues identified and encapsulated in my research theme. I have applied the doctrinal rules, principles and norms to create interpretive guidelines for practitioners, the LEA 'actors' operating within the applicable socio-legal contexts. In this way the published body of work proceeds by applying coherently not just one but a combination of legal rules to a given set of facts, either naturally arising in the ordinary course of the criminal justice system, or within the careful design of wider research projects in which I have been involved. In this way I have attempted to move the discussions towards the upper left quadrant of Arthurs' model and offer my contribution as principally 'law reform research', with the studies being interdisciplinary in nature and having an express intention of bringing about change in policy and practice.

Chynoweth observes (*ibid* p35) “...it is probably *incorrect to describe the process of legal analysis as being dictated by a ‘methodology’, at least in the sense in which that term is used in the sciences.* The process involves *an exercise in reasoning and a variety of techniques are used ... with the aim of constructing an argument which is convincing according to accepted, and instinctive, conventions of discourse within the discipline.*” [emphasis added]. My published pieces of work proceed with precisely that aim: constructing a convincing line of argument within the knowledge requirement for law enforcement in England and Wales, evidenced and corroborated by the accepted conventions of discourse within the discipline of police law. I have nevertheless proceeded with some care and trepidation given the suggestion from some that legal research and the epistemological origins of law are themselves unscientific and somehow subordinate to or “less dignified” (see Feldman 1989) than other areas of research. The challenge for me as legal researcher here has been that, beyond the necessary synchronic elements of the applicable law ‘as it is now’, I have had to track how the relevant law has developed diachronically – particularly in our common law system and that of other jurisdictions – in order to predict how this may be applied to the rapidly evolving new digital contexts in which LEAs must work. Adapting and adopting a well-established definition of *knowledge management* – the promotion of an integrated approach in identifying, capturing, evaluating, retrieving and sharing information assets, including case decisions, affidavits and pleadings in litigation, correspondence from the public, from decision-makers and policy leads; minutes and notes from meetings, strategic documents, policies, procedures, and previously uncaptured expertise and experience (Duhon *loc cit*) - my published work directly answers the research question by following a knowledge management approach and making a direct contribution to LEA’s understanding of the competing legal considerations arising from the digital dilemma.

Research Method

In the production of the publications that follow I have followed something close to classical *action research* (see Rapoport 1970) and utilised a five-stage model of *diagnosing, action planning, action taking, evaluating and specifying learning*. Throughout the period of publication I have worked as a practising solicitor and chief executive within the policing sector, utilising the attendant opportunities to acquire qualitative data from internal reports, business cases, closed forum discussions, operational and organisational briefings and interviews with practitioners and executive level challenges to knowledge, understanding and performance management. Having had access to practitioners, bloggers, technical data experts, senior leaders, politicians and policy makers, I have developed my work along a logical and focused progression, using the three principal ‘influences’ on knowledge management generally (*managerial, resourcing and environmental* – Holsapple & Joshi) led by practical need in an environment of conservatism and conventional policing methodologies rapidly being left behind by the ‘digitization’ of communities, scoping out the dilemma presented by the new capabilities/obligations/expectations for LEAs and critically evaluating how those LEAs will need to recognise and reconcile the legal issues I have identified. In developing my work for publication I have been directly involved in the *planned organisational change* being sought, simultaneously *creating* that change and *analysing its potential impact* (per Baburoglu & Ravn 1992) identifying *previously uncaptured expertise and experience in individual workers* (per Duhon 1998) and, in the synthesis of the published work, I have set out my visions of *best practice for effective operators* in this most topical and controversial of policy areas. The published works have been designed to address individual legal learning gaps revealed by my research at the level of the relevant practitioner, published within broader learning texts that fill much wider knowledge gaps within the technologically burgeoning environment and *consolidating the knowledge in a way that is necessary for changes in formalised procedures to begin taking hold in their organisations* (Belasen 2000; Jost & Bauer 2003). In this I have gone beyond knowledge articulation and produced a themed original contribution to legal knowledge management in the advancement of police

effectiveness. Professionally I trace a coherent and cohesive theme over an eight-year period, challenging the understanding and adequacy of extant legal frameworks, knowledge procedures and ethical/operational considerations by which LEAs are held accountable. Academically these settings provided a practical *locus* for action research in which I designed and contributed to practitioner workshops, interviewed LEA operatives in various jurisdictions, conducted accountability and challenge meetings with experts in legal doctrine and practice, specialists in communications, technological, systems and policy fields across a wide range of jurisdictions. Working with trainers, supervisors, managers, fellow senior lawyers and executive leaders I monitored and evaluated LEAs' responses to informatics, intelligence and innovation. Using the product of these extensive data gathering activities I *identified* the focused research questions, *acquired and analysed available information, noting the results and applying the learning within areas of policy and practice* using discrete published examples to bring the challenges and posited solutions to the intended audience. The outcome is thus a product of careful and selective identification and inferential analyses of the legal considerations, the isolation and synthesis of the principles, existing law and doctrine with its inconsistencies and *lacunae*, consistent with the discipline of legal research. My method involved close scrutiny of the relevant legal provisions that were 'in play' within contemporary law enforcement activity and an analysis of the approach of the courts, both domestic and EU-wide (in conjunction with selected academic discourse from the literature) to make diagnostic statements of the legal and ethical implications for LEAs in the course of which I collated real examples from the workplace, testing understanding and opinion, hypotheses and working assumptions against the prevailing legal norms, ethical expectations and the *zeitgeist* within LEA communities.

Original Independent Contribution to Knowledge

The publications form a coherent body of work, beginning with the early emergence of community demands for crime data sets that were formerly regarded as the exclusive property of LEAs and how the dilemma of balancing the possible with the permissible can be traced from this movement. Having introduced this new *societal* context (Chynoweth) I then move to a series of socio-technological settings and examples, deliberately taking specific elements of contemporary policing in order to illustrate and develop the research theme for practitioners. The topical relevance of this as the research theme's backdrop and its genesis in crime mapping is directly corroborated by a RUSI research paper³. Published at the same time as my summative publications (items 7 & 8) RUSI recommend that LEAs develop - as a matter of urgency - a decision making framework to ensure that they are "able to make effective use of [Big Data] capabilities without fear of violating citizens' right to privacy", particularly in the context of the next generation of crime mapping technology/methodology. This is precisely what my body of work encapsulates and enables. The evidence underpinning that claim and the relative contribution of each piece of work to the research theme is particularised in the following synopses. In terms of knowledge management, commentators have contended that all learning starts with *individual* learning and that effective individual (and group) learning has a generally positive impact on organisational learning (Lim *et al* 2006). My published work has been targeted largely at advancing the knowledge of the individual: the operational practitioner, the trainee and trainer, the supervisor and manager. I believe that this impact has been amply made out in my submission. Some specific examples include the use of my works in the development of training materials with overseas police forces such as the Abu Dhabi Police, the provision of workshops to LEA personnel and the development of professional knowledge by operational LEA expert managers from the WyFi team in West Yorkshire who worked within the CENTRIC research teams and who subsequently returned to directly relevant roles in policing such as Regional Cybercrime covering Yorkshire

³ Babuta, A, "Big Data and Policing: An Assessment of Law Enforcement Requirements, Expectations and Priorities" 6 September 2017 Royal United Services Institute

& the Humber police forces and the development of the 'app' for Europol to assist operation LEA agents to interpret and apply the Law Enforcement Directive when processing personal data. Further impact is evident in the contribution made by my works to the Europe-wide research projects in which the University is a research partner, projects such as ATHENA (*infra*), AIDA (Artificial Intelligence and Data Analytics for LE) and most recently in my adaptation of the Peelian Principles in constructing the University's bid for a 2-year research H2020 project to develop European legal and ethical principles for AI in Law Enforcement. In addition, the sharing of the Principles for Accountable Policing with the College of Policing and with the governance bodies of An Garda Síochána and the City of Seattle Police Department following the public protests about policing governance in the US in 2020 also evidence the ongoing impact of my research work.

However, while the phenomenon of *organisational* learning is discursive and sometimes hard to delineate (Wang & Ahmed, 2003), I have also evidenced the contribution of my published work to this higher level as well as those of the individual and group. My work has also been aimed directly at, and received by policymakers, senior executives, political leaders and researchers. Taking the perspective proposed by Belasen (2000) and Jost and Bauer (2003) -that learning at the organisational level involves *consolidation* of knowledge generated from the individual and group level which leads to changes in formalised procedures within an organisation – I believe I have evidenced a significant degree of consolidation, of meta-synthesis of knowledge achieving a significant tri-level impact. Riege and Lindsay (2006) summarise the main drivers for the adoption of knowledge management in the public sector and contend that knowledge management initiatives can facilitate knowledge transfer and sharing among employees, adding to the 'knowledge capital' on which all employees, managers and supervisors can draw. A number of my works have been direct contributions to knowledge capital in the professional development of police officers and staff and the creation of learning and reference materials, but also in relation to policy making for groups and organisations and the prevailing culture. Applying their (Riege and Lindsay) analysis of knowledge management I aver that my published works have improved, developed or updated existing knowledge repertoires and established new ones in a way that makes the existing knowledge within the boundaries of the organisation accessible and protected. These feature strongly in my published work in which I have not simply protected but *extended* those boundaries and individual/organisational repertoires and made the composite legal arguments and references accessible to practitioners. Relying on knowledge to inform decisions and policies should, they go on to argue, increase the likelihood of success and achieving the desired outcomes and make the decision-making process transparent and coherent. Placing the relevant legal knowledge at the heart of decision and policymaking has been a central tenet of my published works, driving for transparency and coherence and contributing to the overall 'professionalisation' of policing. And while it is never easy to measure accurately how one's work might have been received, let alone applied, the combined effect of my published work has been directly related to advancements at the taxonomical levels of knowledge, understanding, skills and behaviours (Bloom 1956) within the relevant data law, governance and ultimately accountability of the police in England and Wales – and sometimes beyond. This, I suggest, goes beyond mere knowledge articulation and is evidence of an original independent contribution to knowledge in the advancement of police law and effectiveness.

The specific knowledge contribution flowing from my research is to be found in the identification of the dilemma and the synthesis of diverse legal principles, extracts of statutory and common law and other relevant legal literature into a collection of readily identifiable and applicable principles for LEAs to use in addressing it. By bringing that compendium of legal principles to bear upon the very specific challenges and topical considerations identified within my publications I have created a repository of legal argument and authority to which LEAs must turn their minds if they are to address the dilemma of my research theme and

legitimately exploit the opportunities to increase their capabilities created by the digitization of their communities. Taking the form of statutes, codes of practice, legal instruments and case decisions from the criminal law, the rules of evidence and procedure, the international framework for the protection of human rights and fundamental freedoms, the specific legislative response to the proliferation of data capabilities such as privacy, social media and citizen journalism, along with the different approaches of domestic and international courts in different jurisdictions, the body of work is an original synthesis that directly addresses *and extends*, cogently and coherently, the legal knowledge requirement both for police officers/staff as individuals and for LEAs as accountable public entities, improving their respective abilities to act with legitimacy and to meet the burgeoning expectations of their communities. That is the *leitmotif* clearly evident within my work's progression through linked, themed case studies; its *coda* is in the formal framework for LEAs in the ATHENA project and the content of the LEA data management 'app' designed for, and accepted by Europol in May 2020 for practical adoption across all Member States, and finally in the inclusion of the research theme directly within the international accountability tool published by the Scottish Universities Insight Institute. These three tangible examples provide clear evidence of my original independent contribution to knowledge.

Conclusion

Following the terrorist attack on the Palace of Westminster in March 2017 the Metropolitan Police Service requested all LEAs in the UK to review and report back *on how they capture, store, process and analyse social and citizen-sourced media data* from major incidents. This request was a stark recognition that these new informatics, this hugely powerful and expanding source of intelligence, potential evidence and mass communication capability was becoming routinely harnessed to prevent and investigate crime, to plot criminal activity and prosecute offenders, and to communicate with communities – virtual and geographical – in times of civil crisis. The subsequent proliferation of citizen-created datasets during the COVID-19 pandemic generally, and those shared on social media platforms by US citizens as potential *evidence* to be used in prosecutions of police shooting cases that occurred during May/June 2020 in particular, validate the importance of my research theme and underscore the continuing dilemma that faces LEAs in this regard. If it is to be of positive value to LEAs and their communities, the product of these data grabs by LEAs and citizens must be *demonstrably compliant* with the legal framework protecting citizens and their data and balanced against the respective expectations of citizens and LEAs who are being driven inexorably to relying upon data sets created and shared with extraordinary speed. My published work thus demonstrates contemporaneity with the emergence of new digital police/citizen relationships while my research and publication contribute both new thinking about, and practical solutions to this critically developing area for LEA actors. Operating at the three levels of influence on knowledge management (Holsapple & Joshi) to bring about change through the publication of the work I have set out the planned organisational change being sought, created the setting for that change and studied in part its impact simultaneously. All of the published work formed part of a national knowledge-sharing workshop in early 2019 coordinated by the Cabinet Office Emergency Planning College and Sheffield Hallam University (CENTRIC) attended by senior officers from policing, counter terrorism and intelligence portfolios along with local authorities and representatives from the new – and wonderfully acronymed - Yorkshire Office for Data Analytics (YODA).

Having recognised and identified the peculiar legal challenges for, risks to and requirements of LEAs from a range of professional vantage points, I have interrogated the legal literature and existing regulation, capturing experiences, collating data and testing hypotheses. I have applied and published the results contemporaneously with a series of live cases, culminating in a substantial contribution to knowledge within the parameters of an EU-wide research programme. The prescriptions I offered for policy and

practice are now embodied in the ATHENA prototype, an acutely practical framework for LEAs and emergency services which subsequently influenced the roll out of a yet more ambitious international project led by the University: the Security Communications & Analysis Network (SCAAN) designed and developed by one of the ATHENA partners - the UN IOM – to provide a digital platform providing communication and enhancing situational awareness during crises in the field. They are also formally incorporated in the Principles for Accountable Policing, an international policy framework, the Explanatory Guide for which I wrote in July 2019. Having been funded and published by the Scottish Universities Insight Institute, and developed over three years, the Principles are intended to be adopted by LEAs *and the public* across, not only the UK and Ireland, but also any jurisdiction in which the police purport to be democratically accountable. The Principles have already been requested by a US police department following the civil unrest during the spring of 2020. Finally I have specifically and directly applied my research findings within a CENTRIC project commissioned on behalf of Europol in the production of the ‘app’, analysing in detail the relevant legislative framework and case authorities from my research to ensure LEAs understand and apply data processing legislation and case decisions when balancing the technologically possible with the legally permissible. That product is, at the time of writing, in *beta*-testing phase and is likely to be formally adopted by Europol shortly.

Were I to begin the research anew I would limit the focus primarily to the context of civil contingencies as provided for within the Strategic Policing Requirement (see s.37A Police Act 1996). This is principally in light of the scale and impact of what was to follow in the form of the Covid-19 pandemic and its relevance to and amplification of the areas in my critical research question. During the pandemic I was invited by Professor Hamid Jahankhani at Northumbria University to contribute a chapter identifying the legal and ethical data issues arising from the pandemic to a book that will be published by Springer at the end of this year. Researching and compiling this has reinforced the conclusions within my research while the exigencies of the pandemic have underscored the attendant dilemma for LEAs.

In sum, I have addressed the research question of how LEAs must balance the opportunities from burgeoning availability of data with the rapidly increasing public expectations of privacy, security, confidentiality and accountability, collecting and connecting the qualitative knowledge and practice that resides in distributed places and people, disciplines and databases in order to establish a previously unrecognised body of work that focuses on both opportunities and obligations, in order to promote an understanding of the applicable ‘law in context’ and ultimately increase police effectiveness. The direction of my published work follows a series of not only influences, but also *confluences*, tributaries and deltas of change all flowing towards the same unequivocal destination: an original contribution to “*knowledge about the traditional elements of the law and also about the quickly changing societal, political, economic and technological ... aspects of relevance.*” (Langbroek).

Note regarding co-authored works and research carried out in collaboration with others

1. Fiona Kinnear was one of my research team working at the Police Authority when I arrived in 2008, responsible for maintaining the local crime mapping database and I encouraged her to begin to collate and publicise the details of the methodological approach being pioneered in West Yorkshire. She validated the technical accuracy of the article and provided the graphic; the remainder of the published work and the research on which it is based are my own.

8. Alison Lyle is a former colleague from CENTRIC who previously worked with me on European Commission funded projects in the West Yorkshire Police. The principal concept and message running through the chapter are my own, as are the practical policing elements and case law. Alison as one of the leads on the Project ATHENA team provided the data protection analysis and factual information from the project.

11. As part of the Steering Group I worked with the Scottish Universities Insight Institute to research the Principles. I was then tasked with researching and writing the Explanatory Guide which is entirely my own work.

Analysis of the Publications, their Contribution and Synthesis as a Coherent Body of Work

1. "Plotting Crimes: Too True to be Good? The rationale and risks behind crime mapping in the UK."

This preparatory work - diagnosing and action planning for the remainder of the published materials - began shortly after I was appointed as Chief Executive of the West Yorkshire Police Authority in 2008 when I worked on an emerging innovative criminological concept involving the tensions and competing legal considerations attending the compilation and accessibility of LEA datasets: that of crime mapping.

While community policing was firmly embedded in every police force in England & Wales, a model in which the participation of the citizen is a central tenet, the key data relating to types, times and locations of volume crime were being expressly *withheld* by the police from the very communities being exhorted to help tackle it. I was able to interview key policy leads such as Louise Casey, Home Office officials and researchers in specific police forces both domestically and in the US and, in so doing, identify the scale of the emergence of what was then a relatively narrow 'data dilemma' recognised by Heather Brooke: that of accurate and meaningful crime mapping. The principal reason given by the police for withholding these data from external examination was, paradoxically, their accuracy: specificity and reliability were equated with 'dangerousness' and even illegality. Building on the local ambitions of the Authority at that time I researched the data requirements and sentiments of our communities and then reviewed the realities of the legal framework within which any data sharing and analysis would take place. Researching work carried out in the US and Canada, and interviewing the lead US researcher around civic data access, analysing the risks of making meaningful crime datasets publicly available, I held meetings and discussions with LEA personnel, the Home Office, police technology and training organisations and local politicians. The postulated legal risks of withholding data and the failure to see how future expectations of citizens would become increasingly important to policing capability showed a lack of understanding by LEAs and represented a significant gap in knowledge. Both the legal framework and the dependency on citizen-created data (each of them being a key feature in the identified dilemma at the heart of my research) subsequently evolved significantly over the period of publication.

The fundamental challenge for LEAs at the point of publication was how to enhance their community policing capability in the digital age in a way that was legally compliant, met the expectations of our communities and remained consonant with wider police accountability. At the time of publication, only West Yorkshire Police Authority was publishing crime data to street/address level using 'dots-on-maps' as opposed to the generalised 'painting-by-numbers' choropleth model. In order to bring an innovative approach to the pooling of data and analytics emboldened by a better understanding of the digital *zeitgeist*, I published this article with the intention of increasing knowledge and understanding within the LEA community, setting out the issues in the context of the pioneering work that we were undertaking in West Yorkshire and contrasting the approach with that of the Civic Data Movement in the USA. I include the article here partly because it marks the starting point for my programme of work to alert the law enforcement community to the bigger dilemma arising from the developing data interface between them and their citizens, the differential purposes for data collation and deployment and most of all because, as a result of this work it became clear to me that, not only was there a growing demand for public access to crime data and a legitimate expectation that it would be provided by LEAs, but also that LEAs would increasingly come to *depend* on citizens' data captured on their own personal devices. The shift from a societal context in which citizens were vying to access the *metadata sets of their LEAs* to the endpoint where the emergence of social media and technological commoditisation has resulted in the creation of digital relationships between the LEAs and the citizen within which the police are increasingly dependent

upon the *metadata sets of the citizen* became a central feature of my research theme and sits at the centre of my final piece of work within the ATHENA project. The specific legal considerations connecting the two pieces of work represent, not only a new area of rapidly developing law for LEAs, but one to which my published work has made an original contribution.

2. “Cyberspace: the new frontier for policing?”

In the first training chapter of its kind to introduce LEA officers to the new technical realities of their digitized communities I examine two critical legal aspects of capability – scale and shape of challenge - in the specific context of cyber and cyber-enabled crime. At the time of publication of the UK’s 2011 Cyber Security Strategy, an estimated 2 billion people were ‘online’ with over 5 billion Internet-connected devices in existence. The response of LEAs in terms of the number of people being proceeded against in England and Wales for offences under the single specific piece of legislation (by then already over 20 years old) – the Computer Misuse Act 1990 - was just nine with no people at all being proceeded against for the two principal offences under s.1 (1) and s.1 (3). My research of records from the Police National Legal Database (PNLD) shows that, during two weeks (chosen at random) in 2013, officers across England and Wales accessed the text of the legislation and its accompanying guidance notes 907 times in one week and 750 times in another illustrating both an asymmetry in the scale of response to threat and an anomaly in the demand for legal knowledge and guidance.

Against this background I introduced the ‘shape’ of the digital challenge for LEAs, demonstrating how fundamental, taken-for-granted concepts of investigation need to be reconsidered in light of technological possibility and public expectation. Researching familiar, established concepts from standard criminal investigations (*mens rea*, *actus reus*, scene, suspect, etc.) I realised that even the most basic tenets of criminal investigation would need to be revisited by practitioners in the context of cyber and cyber-enabled criminality. Using the concept of jurisdiction and an established set of legal criteria (Cottim 2010) I set out to demonstrate how the existing theories and approaches of the courts could not necessarily be relied upon in the digital context. By working with senior policy leads in this area, analysing the statistical data from local and national LEA sources and assessing the knowledge, resources and ideas deployed within this developing area of policing, I put forward these propositions, testing them out at an international workshop of LEAs and research partners in Montpellier, France in 2015. Having interviewed visiting Advisory Board members from CENTRIC, along with the most senior police officer in the US and a former US Attorney-General, I researched the case authorities emanating from the United States to investigate the jurisdictional aspect, citing some (e.g. *United States of America v. Jay Cohen*; Docket No. 00-1574, 260 F.3d 68 (2d Cir., July 31, 2001); *Bavaria v Felix Somm* (unreported)) to illustrate a new approach within an appropriate format for LEAs, before going on to review UK case law and selecting some standing authorities that might no longer hold good in the new digital age of citizens’ data and cyber offending (e.g. *Klemis v Government of the United States of America* [2013] All ER (D) 287; *Bloy and Another v Motor Insurers’ Bureau* [2013] EWCA Civ 1543).

In terms of impact, this work is now used within the curriculum for specialist investigator training in LEAs in England and Wales and the areas of learning captured are also part of *organisational* learning within LEAs (the link between the two being a key feature of strategic knowledge management – Klein 1998). I go on to diagnose the nature, size, shape and scale of the challenge represented by cyber space within the context of the UK Cyber Security Strategy and the subsequent developments among public bodies to adapt accordingly. I conclude by raising the growing dilemma presented by the need to balance security of

citizens against the regulated conduct of state agencies in respect of their citizens' data (a central part of my research theme that runs through the publications that follow, to the final publications in which that dilemma is borne out within an EU funded research project in which the University was a key partner). This book is now a staple of cyber investigation training for LEAs both in the UK and internationally.

3. ***"The Legal Challenges of Big Data Application in Law Enforcement."***

"With so much data so readily available, on what basis would law enforcement agencies (LEAs) *not* seize it and run with it as far and as fast as possible, if doing so meant preventing terrorist attacks, disrupting serious organized crime, or preventing wide-scale child sexual exploitation, human trafficking, and so forth?"

This question was put to me during the course of my research for the previous article by an interviewee and I adopted it here as a rhetorical question against which to continue the research theme into the next piece of work. My posited answer to the question sets out the peculiar legal issues arising from the increased Big Data capabilities by LEAs and what I saw as their new relationship with the citizen. Setting out the overarching legal framework from the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Council of Europe Treaties 108 (01/1981) I introduce LEA practitioners to the legal issues arising from Big Data and then, by way of a further new contribution to the discussion, illustrate how the extraordinary capability of Big Data to identify general trends and macro-correlations can also be used directly to affect the individual, a feature which, I demonstrate, has specific implications for LEAs. Taking the research theme further I consider the technical legal framework components such as the Protection of Freedoms Act 2012 governing the retention and destruction of fingerprints, footwear impressions, and DNA samples taken in the course of a criminal investigation; the further regulation of closed circuit television, automatic number plate recognition, and other surveillance camera technology operated by the police and local authorities; the need for judicial approval before local authorities can use certain data-gathering techniques; data provision with respect to parking enforcement and counter-terrorism powers, the ECHR and the EU Charter of Fundamental Rights and the jurisprudence of the Court of Justice of the European Union (ECJ). Within the work I then introduce another novel argument: that the indiscriminate—or at least non-discriminating—nature of Big Data analytics and the automation of data processing (a *sine qua non* of Big Data's principal value) *extends* the research theme dilemma for LEAs because the greater the automation, the less scope there is for intervention by the controlling mind and the application of discretion, both critical considerations when demonstrating proportionate interference with the rights of the citizen which will always be subject to review by the Court (per *Coster v. United Kingdom*, 2001; 33 EHRR 479). Continuing the research theme I examine the human rights considerations and expand upon the challenges brought by the key legal concept of 'purpose limitation' and 'further processing', exploring the correlative need to address *societal acceptability* and issues of trust, confidence and legitimacy of the police, collating the seminal case law and legal actions against LEAs. For example, in terms of the former, *S & Marper v. United Kingdom* (2008) ECHR 1581 (a case arising at the time of the Crime Mapping evolution which held that the retention of DNA samples of individuals arrested but later acquitted or having the charges against them dropped was a violation of right to privacy); *R (on the application of GC & C) v. The Commissioner of Police of the Metropolis* (2011) UKSC 21 (successful challenge of policy allowing indefinite retention of biometric samples); *The Queen (on the application of Catt) v. The Association of Chief Police Officers of England, Wales and Northern Ireland and The Commissioner of Police for the Metropolis* (2013) EWCA Civ 192 (police monitoring of public protests). In terms of the latter my research into parliamentary and regulatory publications reveals stark and cogent criticism of the police handling of datasets (Report of the Public Administration Select Committee 13th

session 2013/14 HC 760, HMIC reports) which, as part of the research theme's dilemma have to be balanced with e.g. findings of the Bichard Inquiry in which I was instructed as a solicitor by the Police Federation of England & Wales. The work illustrates how the technical complexities of even the European Union's own legislative framework were unable to keep pace with the technological changes in law enforcement activity and I end the work with a specific consideration of how far generic Big Data practices such as "do not track" and "do not collect" are applicable in an LEA relationship with the citizen, concluding that the resolution of this strand of the research theme dilemma for LEAs (and, by extension, for the relationships of their partners in key areas such as safeguarding, fraud prevention, and the proper establishment of the rule of law in cyberspace)—will be as much a technical challenge for the law itself as for the data technology.

4. "Whatever You Say ...": The Case of the Boston College Tapes and How Confidentiality Agreements Cannot Put Relevant Data Beyond the Reach of Criminal Investigation in Policing."

In this journal article I take the 'legitimate purpose' theme further and introduce a situation whereby LEAs seek to *compel* the disclosure of private digital material produced for one legitimate non-investigatory purpose (academic research) for use in their legitimate investigation of crime and as evidence in the prosecution of offenders. This followed my interviews with investigators who wanted to understand the legal framework and principles of compellability further. My subsequent research of the legal interface between LEAs, the state and social media service providers in order to compel disclosure of data that may amount to evidence in a criminal investigation was highly topical, touching as it did upon the so-called crypto wars and wider data privacy disputes in the United States which engaged many of the accountability issues I had explored in the previous material. Having interviewed colleagues from LEAs and an academic researcher from the Republic of Ireland I researched a live dispute between the Police Service for Northern Ireland, an academic body in the US and the individual rights and interests of a private citizen and took it as a case study for further investigation. In the subsequent article I begin by adapting an established common law authority that sets out the challenge of proportionate intrusiveness facing police officers (*R v. Lewes Crown Court ex parte Hill* (1991) 93 Cr App R 60) in an 'analogue' context and extend/apply the principles to the arguments that were being contested in the Boston College Tapes case in which privately-processed datasets owned by an academic institution were being sought by detectives in a terrorism investigation into an undetected murder.

By reference to the approaches of the courts against the LEA in several jurisdictions (e.g. Re: Request from the UK Pursuant to the Treaty Between the Government of the USA and the Government of the UK on Mutual Assistance in Criminal Matters in the Matter of Dolours Price M.B.D. No. 11-MC-91078 US district court district of Massachusetts; *Rea's (Winston Churchill) Application* [2015] NICA 8) and by illustrating the engagement with the previously-discussed issues under the ECHR and associated case law (e.g. *Amann v. Switzerland* (2000) 30 EHRR 843; *R (OTAO Hafner and Another) v. City of Westminster Magistrates' Court* [2009] 1 WLR 1005), I illustrate the novel ways in which the LEAs and their respective governments were calling upon international law to challenge the local court rulings over data privacy considerations at the heart of my research theme, along with the equally novel grounds of resistance by private bodies/individuals.

Highlighting one of the further elements from the research theme - the public expectations of our LEAs (in this case to investigate murder and bring suspected offenders to justice) – I use the Boston College case to explore the competing legal and societal issues from my research theme and to show how the fundamental obligations of the police have ultimately prevailed in attempts to use public, private and international law

principles to put the data set beyond the reach of criminal investigation. I also introduce the novel argument of asserting journalistic material protection, an argument that was not pleaded by the respondents in these cases but which was deployable and which might be prayed in aid in future challenges to LEAs as they try to tap into the 'collective problem solving' of citizens and their data (Palen (2008); Palen et al. (2009) proposing that there remains an overriding presumption in favour of the operational requirements of the relevant LEA investigation, a presumption that cannot be rebutted or qualified by individual consensus or even perhaps inter-State agreements under International Law. The importance of this tension between operational imperatives and privacy for data processors arises later in items 6 and 7 in relation to the reluctance of the citizen to share their datasets with LEAs *even in the rarefied and neutral context of a research programme*.

5. "Intelligent evidence: Using open source intelligence (OSINT) in criminal proceedings."

6. "Following the Breadcrumbs: Using Open Source Intelligence as Evidence in Criminal Proceedings"

Through these publications I specifically progress and expand the element of the research theme that I had identified early on in my research. Moving from consideration of how LEAs might lawfully access and deploy data sets acquired by third parties for non-LEA purposes I consider the *reverse* situation which I proposed would assume greater significance for LEAs in the future, asking how the reverse might be addressed. In these works I look at the dilemma from the citizens' perspective by examining how far LEAs are coming to terms with the potency of social media and Internet-based communication as a phenomenological intelligence source, one feature of which I identify as the narrowing of 'traditional' boundaries between information directing lines of investigation (intelligence) and material connecting a chain of proof relied upon in criminal proceedings (evidence). In both publications I address a further strand within the research theme dilemma, that of social media and other open source material becoming freely available to the police in everyday policing matters and emanating from their new 'digital relationship' with the citizen. I use the journal article and a subsequent LEA textbook chapter to follow this central feature of my research theme into two elemental areas for LEAs: criminal intelligence and criminal evidence. Taking the proliferation in social media and Open Source Intelligence ('OSINT') in the first article, I consider the impact in a literature review and, as in previous articles, take an established definition for the digital sector (from Kaplan and Haenlein 2010) before applying it by revisiting the long-established legal principles for criminal evidence. For example I consider some carefully chosen key concepts such as admissibility, relevance to a fact in issue (*DPP v Kilbourne* [1973] AC 729; *R v Blastland* [1986] AC 41), weight and purpose, considering them all in the digital context of Twitter and other social media platforms – thereby illustrating the need to balance the first and second aspects of the research theme dilemma (possible vs permissible). I go on to extend this discussion by applying the established legal principles and the relevant legislation to a hypothetical case that I construct from research of the case law and statutory analysis. I create a fact pattern in order to lead the LEA reader to consider the relevant issues from my research theme, providing a detailed legal analysis of those issues in light of selected case authorities (e.g. *Bucknor v R* [2010] EWCA Crim 1152; *T v R* [2012] EWCA Crim 2358).

In terms of practical contribution to knowledge, I offer a list of new 'self-check questions' that I adapt from the CPS Guidelines on hearsay, suggesting that they be applied by LEA actors when considering *all* the legal issues highlighted in the article before going on to consider a second, more complex hypothetical case the fact pattern of which was produced by my further research of case law and statutory references in order to illustrate the ideas proposed. I produce a review of the relevant case law around the exclusion of

unlawfully or unfairly obtained materials in criminal trials and in particular consider the consequences for LEAs of failure to adhere to the legal requirements and the perils of being tempted into trickery using social media to catch suspects, once again extending and furthering the central research theme dilemma of how LEAs will have to balance the technically possible with the legally permissible.

Directly addressing the research theme I conclude that “in a world that relies so unquestioningly on information gathered from open sources it is all too easy to assume that such information will be accepted in every setting, including formal legal proceedings” and demonstrate how failure by LEAs to consider the issues elaborated upon may prove fatal to a prosecution or related proceedings. Finally I return to the novel legal concept arising from social media researchers treatment of some OSINT material as ‘citizen journalism’ and how such material might attract the statutory protection (see the Police & Criminal Evidence Act 1984, ss. 11 and 13) accorded to sensitive materials and presenting LEAs with a further challenge within the dilemma of the research theme.

The second publication was researched and produced specifically for a textbook written for all LEA actors in EU member states. In it I develop the elements of the research theme from the conjoined journal article by examining more closely the considerable power of social media to provide an extension of LEA capability in respect of intelligence through the jurisprudential lens of the European Convention on Human Rights (ECHR). Considering and analysing once again the *purposive* element of the applicable legal framework I examine the differences between community policing *intelligence* (wide ranging, almost undefined, and covering an array of activities from supplying information on which to base an arrest e.g. by giving rise to reasonable suspicion to the likely destination of a vulnerable person who has gone missing) and the *evidential* purposes within an investigation. I look at developments in socio-digital behaviour among citizens and propose a novel concept: that these have produced a new category of ‘community’ which can be seen as a virtual group created by coalescence around a particular theme or event. Such groups are evanescent in nature and probably unique in identity and, once the event/activity/interest that unites the members of the community diminishes, so does the digital community itself. This is a significant new concept for LEAs and one that directly engages considerations at the heart of the research theme. While the availability of data both *from and about* these digital communities creates a new potential capability for LEAs (the ‘possible’) - some of whom are increasingly inviting their citizenry to contribute digital material in the investigation crime (for example by ‘dashcam’ recordings) - the legal implications of LEAs accessing and relying on the datasets are of central importance to police effectiveness, legitimacy and accountability (the ‘permissible’ and ‘acceptable’). I consider in detail the extent and impact of the ECHR and of Art 6(1) (right to a fair criminal hearing) in particular, for all LEAs operating within EU jurisdictions. Once again I further the knowledge required by LEAs in order to be effective within the context of the research theme, providing an examination of the case law and encouraging LEA actors to consider these issues anew within their recently-enabled digital capabilities – for example the impact in new ‘OSINT’ circumstances of standing authorities on disclosure to defendants in criminal proceedings (*Rowe and Davis v. the United Kingdom* (2000) ECHR 91) and raising novel questions of how these will affect the entitlement to “facilities” that a defendant must enjoy when preparing his/her defence (*Huseyn and Others v. Azerbaijan* (application nos. 35485/05, 45553/05, 35680/05 and 36085/05); *OAO Neftyanaya Kompaniya Yukos v. Russia* (2014) ECHR 906.) or the opportunity to acquaint him or herself with the results of investigations carried out throughout the proceedings *Mayzit v. Russia* application no. 42502/06; *Moiseyev v. Russia* (2011) 53 EHRR 9).

I go on to demonstrate by reference to worked examples how, if digital or social media-obtained LEA intelligence is to be relied upon *evidentially* anywhere within the EU, it will need to meet the same forensic

standards and clear the same legal hurdles as any other form of evidence, thereby continuing the research theme in relation to technical possibility vs legal permissibility. My contribution to 'new knowledge' here is in the diagnosing of gaps between the expository, doctrinal research and the contextual realities of the LEA environment, increasing knowledge and understanding that flow from its posited answer: that the application of informatics within a law enforcement setting is qualitatively different from that of Big Data application in most non-LEA settings. I go on to explicate those reasons, found within the complex and dynamic legal framework for data protection and regulation across the European Community (black letter law) setting out the synchronic legal position against a diachronic review of the cases and events charting an unedifying history of LEAs' treatment of personal data. The chapter appears in *Application of Big Data for National Security* (Elsevier) which "provides users with state-of-the-art concepts, methods, and technologies for Big Data analytics in the fight against terrorism and crime, including a wide range of case studies and application scenarios". Opening the section specifically aimed at the legal and social challenges of Big Data I balance the central dilemma against the further perennial risk for LEAs of community condemnation for failing to use all 'available' data to prevent loss of life or to detect serious crime, illustrating how and why this makes law enforcement a peculiarly perilous context for Big Data application.

By combining the existing legal knowledge in the form of established laws of evidence and applying them within a wholly new and developing context of digitized citizen-generated and owned data sets, I make an original contribution to the professional knowledge of LEAs while, at the same time, adopting a simple established learning technique of taking the already 'known' and applying it to a new concept to introduce and improve understanding of the latter (Bransford *et al* 2000). Some of the specific risks picked up in this chapter were subsequently addressed directly by EU and domestic legislation while the wider principles and competing pressures remain. In terms of impact, the book is already becoming a standard text for LEAs nationally and internationally. Insofar as further and continuing impact is concerned, I went on to apply the research directly within a project undertaken by CENTRIC on behalf of Europol in the production of an 'app' to support LEA actors in understanding and managing data processing law and the specific provisions that they must take into account when balancing that which is technologically possible with the legally permissible. The 'app' was formally accepted by Europol in May 2020.

In the next two overlapping pieces I bring together the issues explored in the preceding works.

7. "The ATHENA Equation – Balancing the Efficacy of Citizens' Response to Emergency with the Reality of Citizens' Rights."

8. "Legal Considerations Relating to the Police Use of Social Media" (with Lyle, A).

Led by the LEA team that I established in West Yorkshire Police, Project ATHENA was a meta-project funded by European Commission H2020 grant involving, in addition to the University, the UN International Organisation for Migration, public authorities from Hungary, Turkey and Slovenia, the Supreme Court of Latvia, the University of Virginia (Critical Incident Analysis Group) and Harvard Medical School. Taking place over 3 years ATHENA set out to develop 'apps' for smart phones and mobile digital devices to capture real-time information from citizens during crisis situations and, as such, directly engaged my research theme. My specific contribution was formally published under the requirements of the Work Package in which I demonstrated how, at the very heart of the project's output, there lay the same issues elucidated in my research theme and developed throughout the preceding articles, issues of citizens' legitimate expectations

and entitlements, duties and responsibilities of emergency responders, complicated by abstruse and as yet unformed causes of action, restrictions, private and public data interests, possibilities and opportunities all arising within a complex and developing inter-jurisdictional legal framework engaging issues of informed consent, licensed ownership and overriding public and political interests. My bringing together these issues was elemental to the Project's efficacy (and that of any similar project) and the tangible product I contributed was a new praxis for emergency responders to adopt when using citizens' data within any EU LEA (which was subsequently used in a further ambitious research programme).

Taking the law at the time of writing and applying it to the specific societal contexts of ATHENA, my original contribution in these two linked publications was to bring together the many principles and legal considerations identified and analysed in the foregoing publications, with item 7 setting out the initial legal elements for LEAs in an article produced for policing decision makers, with item 8 forming the broader in-depth analysis for the relevant chapter in the full write-up under the rigorous terms of the EU project grant.

The goal of the ATHENA project was to deliver two major outputs enabling and encouraging users of 'new media' to contribute to the security of citizens in crisis situations. Based on the LEA learning from the terrorist attack on the Taj hotel, Mumbai in 2008, Project ATHENA proposed to achieve the outputs by *designing a set of best practice guidelines* for both LEAs and citizens to increase their *joint capability* by using new media and applying them lawfully, proportionately and accountably towards a common end: safety and security. The specific tensions and issues within my research theme were designed into the project and, in exploring how LEAs and other crisis responders might harness new communications media (particularly web-based social media such as Twitter and Facebook) and the prolific use of high-tech mobile devices to provide efficient and effective communication and enhanced situational awareness during a crisis, ATHENA was *aimed directly at the research theme's focus*, addressing the dilemma at the developing interface between Big Data, LEA capability and the citizen.

The 'narrow' contribution made by the two publications lies in my diagnosis of the novel competing legal considerations in a complex operational setting, followed by the action planning, implementation, evaluation and specification of the subsequent learning for the LEAs involved and those that follow. I begin by bringing together the components of the legal framework for the general protection, processing, sharing and retention of data in the UK and identifying how, for LEAs, this area is heavily regulated by a mixture of European and domestic law, some of which creates particular challenges and dilemmas for LEAs (as summarised at the time by the Supreme Court in the context of data access and journalism in *Kennedy v The Charity Commission* [2014] UKSC 20). Returning to the critical legal concept of purpose limitation and exploring the overarching legal framework for data processing in EU-wide jurisdictions, I apply the established jurisprudential principles to what I continue to identify as a novel concept of 'digital relationships'. In the setting of this major research project I examine how the proposed actions of the LEAs under the project will result in the creation, *de facto* and *de jure*, of digital relationships between citizens and the State. I then critically examine how the relevant legal instruments (e.g. Article 8 ECHR prohibiting interference with the right to privacy except where such interference is in accordance with the generally applicable departures from the Convention article necessary in a democratic society); Article 6(1)(b) of Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, 31) and the attendant case law (e.g. *Gillan and Quinton v The United Kingdom* (no 4158/05/2010)) might apply. Published contemporaneously with a period of intense international political, legislative and judicial activity around data protection and processing (see for example the judgment in Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* and the subsequent

legislation) this work - and the subsequent chapter published in order to promulgate the learning from Project ATHENA - highlights acutely the dilemma of possibility vs permissibility for LEAs. I also extend the argument around the anticipated assertion of a the status of 'journalistic material' as protected by the courts (*R (on the application of British Sky Broadcasting Ltd.) v The Commissioner of Police of the Metropolis* [2014] UKSC 17) to a new, expanded class of material incorporating citizen data.

My introduction of the concept of 'digital relationships' between the LEAs and their participating citizens represents a further original contribution to knowledge and I go on to identify how – following the arguments and issues from the previous publications - the legal issues arising within the relationships created at the interface between the data elements, the LEAs and the citizen required an *extension* to the project's 'best practice guidelines' (first article) and then expound further on the wider issues and risks arising within the ATHENA exploitation phase touching on LEAs' use of social media generally. While the original project brief for ATHENA included some mandatory legal and ethical principles (put forward by another ATHENA researcher, Alison Lyle of CENTRIC), I argued in the settings of workshops and programme reviews that there were fundamental legal considerations *beyond those originally identified*. I therefore proposed a governing legal protocol between ATHENA subscribers (citizens) and those LEAs (and other State agencies) that will ultimately be collecting, sharing, processing and retaining their data. In this way *the triptych of informatics, intelligence and innovation came together*, in a highly practical, multi-jurisdictional research project creating new understanding and capability in the legal and accountable digital frontiers for law enforcement. The specific contribution to knowledge and learning from the consolidating publication is set out in the form of a series of recommended 'rules of engagement' both for the Project and the wider activity for LEAs. The subsequent 12 rules all draw on the principles in the foregoing publications; all are concerned with Hermitage's (*op cit*) police 'knowledge requirement' and the legal framework I have established, identified and followed throughout; all are part of an original contribution to knowledge. That contribution is finalised in the second piece of work which rounds off, not only my own research work, but also the research findings of the ATHENA project itself. Taking the form of a technical manual that sits within a wider series of international authoritative texts in transactions in computational science and computational intelligence, my penultimate piece (co-authored with Lyle) brings together the overlapping elements from the ATHENA and OSINT work and synthesises all the previous publications. Building on the work at item 7, the final chapter analyses previously discussed legal and societal elements of the 'data dilemmas' within the research theme, addressing the expectations of privacy by the 'citizens' in ATHENA and the extent of citizen mistrust of the State with their data *even in the controlled circumstances of volunteers in a research project*. The chapter also considers other themes such as the recent recognition by the Police Foundation of 'intelligence and evidence' as a specific category of social media data deployment by LEAs, as well as going into greater depth on the legislative framework for data protection across the EU member states and the changes being introduced via the General Data Protection Regulation 2016.

The relevance of ATHENA to my research question can be seen most clearly in the project's feedback summarised in the book's concluding remarks thus: "*What is perhaps most notable of all about the feedback received ... is that, whilst 'members' of the police and public alike were generally impressed by the technological and communicative prowess of the ATHENA system, there was evidence of some concern among the latter with regard to certain legal or ethical issues. Respondents were evidently discomfited to learn that the app provided access to personal data, with some arguing that the ATHENA privacy policy needed to be far more explicit in saying that, by sending messages to the police, the individual was effectively surrendering their right to privacy. Similar feelings of alarm surrounded the fact that the police*

might use information volunteered by the public as ‘evidence’ in the process of crime detection.” (Akhgar et al).

This conclusion neatly synthesises the divergent tensions at the centre of my research theme that began many years earlier, underscoring the critical importance of LEAs being able to identify and address *all* the competing issues if they are legitimately and effectively to harness what is technologically possible and balance it with the legally permissible and societally acceptable in increasing their overall capability. The contribution to new knowledge comes principally from combining the detailed expository legal research with that of the ‘law in context’ (the context here being the ATHENA case studies) and the legitimate expectations of the citizen, together with my proposal for LEAs to develop a form of End User Agreement License. My contribution to the chapter addressed the application of the black letter law across a series of legal cases and constructs to the dilemma while Lyle had been on hand throughout the ATHENA workshops and focused primarily on the explication of the constitutional framework and the ethical challenges. The ATHENA editors went on to observe:

“The trick, as Lyle and Sampson rightly maintain, is to strike the right balance between respecting the personal privacy of the individual while doing as much as possible to guarantee the safety and security of the wider population. These authors quite reasonably insist that ATHENA and other SA platforms of this nature have a clear need to operate according to transparent sets of guidelines and protocols for the use of personal data, which should ideally incorporate an End User Agreement License. It is, they believe, only by resorting to such safeguarding mechanisms that the likes of ATHENA will be able to maintain the legitimacy and integrity it requires to guarantee the ideal levels of public consent and cooperation”.

This endorsement of my research theme – and the explicit reference to transparency and legitimacy - reflects the overarching consideration in enhancing LEA capability by digital development, and the object of my final piece of work: accountability.

9. The Principles for Accountable Policing ⁴

In 2016, as a Fellow of the Scottish Institute for Policing Research (SIPR), I was invited to be a member of a programme team to research and draft a set of Principles for Accountable Policing. Funded by the Scottish Universities Insight Institute the programme comprised two workshops bringing together practitioners from the police and oversight bodies across the UK, and academic experts to devise a set of principles *“intended to be of practical use to the police and the various oversight bodies, as well as the public”⁵*. This programme gave me the opportunity to make an original contribution to the product in the form of *direct incorporation of the research dilemma* within the Principles themselves, making the considerations and findings a component part of the Principles themselves. Within the preparatory scoping work, the workshops themselves and the post-workshop events, I jointly drafted the Principles; I then researched and wrote the Explanatory Guidance published in October 2019 which I submit as my final piece of work. In terms of impact and contribution, the Principles were formally accepted by the Police Foundation shortly before the Covid19 restrictions and will be offered via the Foundation to all LEAs in democratic societies across the world. In light of the civil unrest following the deaths of African Americans at the hands of the police, filmed by citizens and published contemporaneously as OSINT/evidence the Principles and the

⁴ <https://www.scottishinsight.ac.uk/Programmes/OpenCall201516/PrinciplesofAccountablePolicing.aspx>

⁵ *loc cit*

consonant elements of my published works have been proposed by the JAMS Foundation in California as the focus for an international law enforcement mediation project involving Senior Mediation Fellows in Pakistan, Nigeria, Croatia and the United States. No formal reference is yet available for this document but Professor Nick Fyfe, Dean of the School of Social Sciences at the University of Dundee can testify to its provenance and the fact that it has recently been requested by the City of Seattle to help them redesign their policing governance arrangements.

Published Works

Item 1

"Plotting Crimes: too true to be good? The rationale and risks behind crime mapping in the UK." in Policing: a Journal of Policy and Practice, Oxford University Press 2010 Vol 4 Issue 1 pp15-27
<https://doi.org/10.1093/police/pap015>
(with Kinnear, F)

Plotting Crimes: Too True to Be Good? The Rationale and Risks behind Crime Mapping in the UK

Fraser Sampson* and Fiona Kinnear**

* Fraser Sampson, Chief Executive of the West Yorkshire Police Authority, Wakefield, UK. E-mail: fs1@wypa.pnn.police.uk 

** Fiona Kinnear, Research Director at the Authority. E-mail: fk1@wypa.pnn.police.uk 

Fraser Sampson L.L.B., L.L.M., M.B.A., Solicitor, is Chief Executive of the West Yorkshire Police Authority, and Fiona Kinnear B.Sc. (Hons) is Research Director at the Authority. Working closely with the West Yorkshire Police, the West Yorkshire Police Authority has been leading the way in crime mapping in England and Wales since 2005. Beatcrime, their award-winning website, is unique in using dots-on-maps to show recorded crimes and trends down to street level and to make that information available to the public. While this approach has been recognized by bodies such as the National Policing Improvement Agency, the question of how much detail the public are entitled to expect from their criminal justice agencies and how much those agencies should withhold remains a contentious area in the UK. This article considers some of the competing arguments against the backdrop of increasing demands for public access to civic data.

If knowledge is power, information is the natural energy source on which it depends. In the context of public information generally, and criminal justice in particular, that energy source appears to be in short supply. As the clamour for more information gains both global momentum and political attention, policing organizations across the UK are under pressure to make their crime data available to their communities. How this has come about and what strategic challenges it brings with it are the subject of this article.

What follows is an analysis of the route by which crime mapping has taken hold within England and Wales, the key drivers behind its development and the strategic challenges for its future.

The route to crime mapping in England and Wales

The need to provide better public information on criminal justice matters has been recognized for some time within the UK and to that extent, the demand for maps illustrating where crimes have been committed is nothing new;

however, it is only in the last few years that the efforts to do so have come front and centre of policing policy, with the last 12 months having been particularly prominent. Now that the government has required all police forces to provide information around crime and criminality in their areas, the needs and benefits are becoming apparent; so too are some of the difficulties.

In what was reported as being the first fully accessible and interactive system in England and Wales to provide the public with local, up-to-date crime information on a map,¹ the West Yorkshire Police Authority launched a website called Beatcrime² in 2005. Originally created by the Police Authority,³ the website is supported by the West Yorkshire Police with whose data the site is populated and its title reflects both the objective of tackling crime and the illustration of recorded offences by local area (historically known as ‘beats’). By entering a postal code and selecting a crime type, people were able to view for the first time the crime picture of their local area, either as dots marking the approximate location of crimes reported in the previous month (often on maps going down to street level) or as bar charts, comparing crime levels for each month with those for the previous year. Since its launch, the site has

become established in the range of tools available both to the public and the Police Authority to hold the police to account. The site also raises the profile of the Police Authority and helps the public to associate it with the monitoring of police performance and crime and disorder reduction.⁴

This award-winning website attracted over 40,000 hits in its first year—by January 2009, it received almost the same number in a month. Among many innovative features the Beatcrime website has, two are of particular interest in the sphere of public information provision. The first is that, as noted *supra*, it was the first website of its kind among UK police organizations; the second is that it was, and remains at the time of writing, the only crime mapping system to use ‘dots-on-maps’ when displaying crime statistics. It is the latter of these features that has attracted interest recently—and that has also given rise to some cautiousness on the part of other policing bodies in the UK.

Before considering the implications of the various approaches to crime mapping by police forces in England and Wales, it is helpful to look at the backdrop against which these developments have taken place along with the developments relating to data access generally.



Civic data access

Beyond pure crime statistics, there is clear evidence of a growing mobilization of public pressure for greater access to official data *per se*, and not only within the UK but on a global basis, to the extent that the provision

of accurate and timely civic data is becoming a central component of the democratic process.⁵

Whether this truly world-wide phenomenon is born of greater concern for ensuring transparency and accountability in our public services or whether it is simply a discrete manifestation of an increasing but discerning appetite for what might be categorized as civic data access (CDA) is unclear. There are however many examples of what is almost a political movement with global ambitions towards accumulating and unmasking civic data to be found on many websites and search engines. Ranging from, for example, the Open Govt Data movement that claims to represent exponents of e-advocacy to the proponents of e-activism (such as DemocracyInAction.org) the presence, popularity and proliferation of these e-communities is illustrative of the public demand for more civic data.⁶

Just what qualifies as ‘civic data’ is uncertain; but the following is offered as a useful working definition, based on the communications from these organizations:

‘Civic data’ are those sets of information created and maintained by public organizations and paid for at the public's expense as part of the day-to-day activities of local or national government.

As such civic data can include things as diverse as crime data, the number of street lamps on a stretch of road, the sentences handed down by particular courts or the allowances paid to public officials. Though it is not always clear from some of the material available, the CDA argument appears to be based on the proposition that—to the extent that raw information can attract proprietary rights—such data are *owned* by the public and therefore ought to be made available to the public. There is force in this argument. Even if the jurisdiction of the country concerned fails to recognize the ownership of raw information, there is no gainsaying the fact that the creation, classification and cataloguing of these data (i.e. all the activities that give it its inherent value) are funded by the taxpayer. Plainly, this is not the same as accepting that *all* such data collated by the State on our behalf must therefore necessarily be disclosed (in full or at all) to the general population—otherwise information affecting defence, civil nuclear programmes, and vulnerabilities in the critical national infrastructure, etc. would present a significant strategic risk. But perhaps in the case of civic data, there should be a general presumption in favour of public disclosure, a presumption that will only be rebutted by a substantial, evidenced and proportionate case such as a real threat to national security. In any event, the call for access to civic data is a real and growing phenomenon and forms the background against which the more specific crime mapping activities of policing organizations are taking place.

► Crime mapping

It is within the broader context of this CDA *Zeitgeist* that police organizations have been coming under increasing pressure to divulge information about criminality in their area.

While the West Yorkshire Police Authority launched its seminal website in 2005, it was not until 2008 that crime mapping really took off in England and Wales. The reason was the coincidence of several key publications and events in the summer of that year that significantly raised the profile of crime maps, lending them the strategic lift and speed necessary to get the subject into the already crowded skies over UK policing governance. These events can thus be summarized as follows:

1 On 3 May, the charismatic media personality and Member of Parliament, Boris Johnson, successfully challenged Ken Livingstone for the office of Mayor of London.⁷ As the Chairman of the Metropolitan Police Authority (a position accompanying his mayoral appointment), Mr Johnson became a keen advocate of crime mapping almost as soon as he took up the role⁸ and has continued to promote the principles of making such information available to the public ever since.

2 On 18 June, Tony Blair's former advisor on anti-social behaviour, Louise Casey, reported her findings following her extensive research into public expectations of the criminal justice system at a neighbourhood level (*Engaging Communities in Fighting Crime, 2008*). Ms Casey recommended that police forces should be required to publish monthly crime information and to include what action is being taken to tackle crime, contact telephone numbers, e-mail addresses and how to complain if dissatisfied.⁹

3 On 17 July, the government published its Green Paper 'From the neighbourhood to the national: policing our communities together'.¹⁰ In this much-debated paper, the government set out its national proposals for the strategic reform of policing in England and Wales. Among the many themes and strands on which it drew, the paper identified the type of information that the public said they wanted from their police organizations and the role that policing organizations should play in providing it.

In the Green Paper, the government also accepted the findings of a national research project the same year, showing that victims' satisfaction correlates directly with the quality and responsiveness of their contact with the police and the information they receive.¹¹

4 And in December, the first national Policing Pledge was introduced as part of the government's wider agenda for policing reform. Taking the form of a national promise of service priority and delivery signed up by all 43 chief constables in England and Wales,¹² the thinking behind the Pledge is supported by other broader research that shows how public confidence improves when the police deal with local priorities (Tuffin *et al.*, 2006). Thus creating the Policing Pledge commits chief officers to a series of things ranging from response

times to call handling and also includes an undertaking to provide information and crime mapping as a specific clause.

At the same time as these events occurred, the need for reliable, accessible and meaningful information on crime and the criminal justice system clearly evidenced within the key reports was robustly corroborated in an independent report by [Giangrande et al. \(2008\)](#). Relying on its extensive review of the evidence on the subject, the researchers concluded that

Britons have become "passive bystanders", uninformed about crime and punishment and less likely to participate in maintaining justice than people in other countries.

The report went on to highlight the importance of providing information thus: Poor information is the key barrier to the active engagement of society in lawfulness. On the one hand, individuals do not understand the true level of crime in their area, increasing fear of crime. On the other, individuals are unaware of the activities of the criminal justice system, increasing their disassociation from it, and making them suspicious about whether perpetrators are dealt with.¹³

All these events and publications served to bring about two things: they drew greater public and political attention to crime mapping and made the link between information provision and public engagement, conspicuously and repeatedly. Once the attention had been caught and the link accepted, only a short step is required to connect information provision with what is becoming the supra-ordinate aim of public bodies in the UK: that of public confidence.

▶ **Linking information and confidence**

If we accept the premise that information is the natural energy source fuelling empowerment, it should follow that informing the public will give them greater power. It is reasonable to hypothesize that a degree of empowerment—or at least a reduction in feelings of impotence—increases confidence on a general human level (Baranski and Petrusic, [1995](#)). What then is the effect of the presence or absence of information on public confidence in the specific context of policing? The links between the provision of accurate crime data and greater confidence among the populace are probably borne out intuitively and empirically; but they are also made out on the more persuasive epistemological and practical levels too.

Taking first the general experience of CDA and the research cited above, it is clear that, without information, the public become too remote from the realities that influence and characterize policing and criminal justice in their area. Leaving aside the difficulties of identifying—let alone categorizing—‘the public’ (a term which appears to include everyone when not at work), the

link between provision of information to members of communities affected by criminal activity and the confidence within those communities is clearly made out, both within the Casey report and that of Giangrande. According to the former the public see the criminal justice system as a distant, sealed-off entity, unaccountable and unanswerable to them or to Government. In part this distance is created by the fact that little information about what happens to those who commit crime is placed in the public domain.

In a report commissioned by the government, Professor Adrian Smith argues that:

[At the local level] trust and confidence are closely related to perceived relevance, accord with experience and the local dialogue with law enforcement agencies, notably the police.¹⁴

As for the practical correlation between confidence and information, the authors of the Reform report go further. They are prepared to argue that, not only is there evidence to suggest that the traditional remoteness they found in our criminal justice sector goes unaddressed by some organizations, but that this is in fact the organisations' intention in doing so; denying the public information to create electoral advantage or avoid scrutiny. This second proposition is corroborated elsewhere, one example of which is the reporting of Heather Brooke who has said:

The police in Britain feel they "own" crime data and the public have no right to know what is happening.... In a void of ignorance, a politician or police chief can claim anything [they] like about crime: that binge drinking is endemic or under control, that muggings are increasing or falling, that policing is working or failing.

She goes on to allege that this withholding of data allows the police to 'hide their failings' citing Northumbria Police who, she maintains, claimed that only three crimes of note had occurred one weekend in May 2008, yet a freedom of information request revealed that there were more than 1,000 incidents, 161 of them being violent.¹⁵

Whether or not these accusations (which is, in truth, what they are) are a fair deduction from the research is a separate matter; what is important here is that the reports clearly evince the nexus between information, effective public engagement and confidence.

The provision of meaningful data however is not just a matter of data disclosure; it also requires a clear understanding and accommodation of the 'end user'. In this context, it is useful to note the findings of a government survey that showed that 47% of the UK population cannot understand 'straightforward, mathematical information' nor can they 'independently select relevant information from given numerical information'.¹⁶

Such shortcomings in data analysis notwithstanding, in the context of policing and criminal justice Louise Casey's research in 2008 also restated the

importance of informing communities about what is really happening in their area. Again, this may not always have a wholly positive effect in and of itself, and there is evidence to show the asymmetric way in which the release of information by decision makers can be received (White and Eiser, [2005](#)). In light of what we know, from the research of Casey and Giangrande and others, it is fair to conclude that the provision of relevant and meaningful information—good or bad—is at least essential to public *understanding* and *contribution*. As it is also important—either as a positive or negative influencing factor—to the wider issue of public confidence, there is an important practical and political element for policing in the UK, which is as follows.

The government intends to sweep away the morass of police performance targets, replacing them instead with a single measure—that of public confidence.¹⁷ Together with the introduction of the Policing Pledge, this will mean that it is more important than ever for policing bodies to make information available to the communities in which relevant criminal activity, and the corrective activity of our public services, takes place. The ‘single target’ of public confidence was put in place at the same time and for the same reasons as the Policing Pledge: to increase the local accountability of the police and to empower communities.¹⁸ While there is still consultation on some of the finer aspects of measurement and calibration, improving confidence rates will be of supra-strategic importance for all involved in policing governance and delivery in the years to come.

In this way, those responsible for the strategic direction of policing have not only accepted but also openly embraced the connection between the provision of timely and accurate information and the creation of public confidence. This marks an acceptance of a premise that has become embedded in jurisdictions such as the USA for years: that if people are either to consider doing anything about crime or, at least to frame the questions they ask of those whose job it is to do so—they need an accurate (as opposed to a purely apochryphal or anecdotal) picture of criminal activity in their neighbourhood. Of course, it could be argued that providing accurate crime data that reveal high levels of serious crime in a certain locality would *reduce* confidence in some areas on the basis that this would amount to official confirmation of people's worst suspicions and that things *are* in fact as bad as they seem—or perhaps worse. This argument may have some merit¹⁹ although there is little independent research available to make the case in the UK, but it is clear that there is a growing body of opposition to the publication of crime data that is *too* accurate or *too* specific. And therein lies the fundamental dilemma of the crime mapper, a dilemma that appears to be predicated on the regulatory arrangements for the publication of data.

► Too true to be good?

It is proposed that, in the context that concerns us here, data are either accurate or useless. For example, knowing that an area of several hundred kilometres² has no more than an ‘average’ (however computed or arrived at) number of robberies this year is perhaps of little value if someone is trying to get a picture of how violent the streets are around their child's school or the roads around their parents’ home. Similarly, is it any better knowing that there was some vague form of dishonesty offence (but not burglary) committed somewhere near X Street or the junction of Y Road at some unspecified point in the past 6 months?

When it comes to crime information, it is submitted that, other than to the ostrich population, the degree of confidence that can be derived from data is in direct proportion to their accuracy. For it to be of value to the police, crime information must be sufficiently specific to inform decision makers promptly, consistently and reliably about that which concerns them most. The same must be true of the rest of us. However, the framework regulating data protection and publication in the UK works in almost the opposite direction: the greater the degree of proposed specificity the greater the risk and therefore the greater the regulation militating against it.

Plainly there are certain crime types where the very nature of crime requires particular sensitivity, and this is recognized expressly in criminal statutes so far as the law of England and Wales is concerned.²⁰ But in terms of other more generic but sensitive data, it is the civil legal arrangements regulating publication and disclosure that present a barrier to organizations wishing to make information accessible to the public.

This tension became apparent in the early stages of development of crime mapping by police organizations and the Office of the Information Commissioner wrote to several police organizations urging great caution before moving towards what was being described as a ‘New York’ model of crime mapping. Boris Johnson's reported response for the Metropolitan Police was to amend their mapping website and make the data far less specific than had been originally planned.²¹ This was clearly a move away from what the Conservative party leader David Cameron had originally encouraged: he had exhorted every police force in the country to record every crime online, every month, in map form.²²

In addition, some organizations such as the Jill Dando Institute, have expressed real concerns around the publication of crime data that are too specific or insufficiently controlled and contextualized. In what they regard as ‘the worst cases’, they maintain that crime mapping

...may actually increase the public's fear of crime, prompt greater scepticism over crime statistics and generate more negative debate about the performance, accountability and transparency of police forces and [statutory crime reduction partnerships].²³

This response finds some support in wider research around the nexus between trust and the provision of information and, in the context of policing, it is not yet safe to assume that greater candour will always produce greater confidence (White and Eiser, [2007](#)). The general response from crime data providers has therefore, perhaps unsurprisingly, shown a similar degree of caution to that of the Metropolitan Police, with two approaches being adopted. The first approach is the ‘choropleth’ model,²⁴ used in one form or another by all other police organizations in England and Wales; the second is the West Yorkshire model showing dots-on- maps.

► Hotspots and averaging

If the primary purpose of providing crime data is to inform people who are interested in or intending to involve themselves with a location, the data need to have a degree of specificity that supports that aim.

As the US Department of Justice website explains, crime is not spread evenly across maps; rather it tends to congeal around some areas and is absent from others. People can (and do) use this knowledge in their daily activities, avoiding some places and seeking out others with their choices of neighbourhoods, schools and recreation areas being influenced by the knowledge that their chances of being a victim are increased or reduced accordingly. In short, crime is not evenly distributed and the risk of our being a victim of crime is not geographically constant. Therefore, to provide crime data in a way that highlights hotspots or averages out the areas of offending as though they were areas of equal atmospheric pressure joined by isobars is of limited utility to the literal and figurative ‘person in the street’. But this is what the vast majority of crime mapping sites in the UK do. Following an ellipse or choropleth methodology, these sites seek to join areas of similar criminal activity and illustrate them either with general hotspots or by delineating a large swath of a map and applying a colour to it (see Fig. [1](#)).



View larger version (89K):

[\[in this window\]](#)

[\[in a new window\]](#)

Figure 1: Extract from the Metropolitan Police crime mapping website

[\[Download PowerPoint slide\]](#)

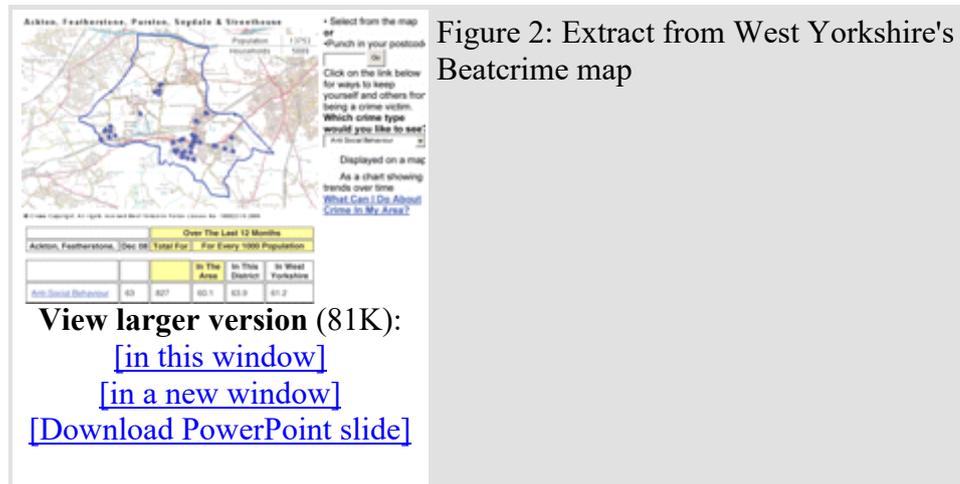


Figure 2: Extract from West Yorkshire's Beatcrime map

In this way the ellipse and choropleth maps imply that the designated areas share the same risk level, rendering specific streets or locations irrelevant. But their lack of relevance does not only relate to the methodology and its underlying assumptions: it is equally irrelevant to persons trying to access the data in order to inform decisions about their life and livelihood. This criticism finds support from Professor Adrian Smith who states that more and better crime information has to be available at a sufficiently local level and communicated in a form that relates to the individual member of the public's day-to-day experience of living or working in an area.²⁵

► Beatcrime

Whether or not the reticent approach of other police organizations and the attendant shrinking from full and frank disclosure provides evidence of what the outgoing Chief Inspector of Constabulary referred to as the inherent 'risk aversion' to be found throughout UK policing (Flanagan, 2008) is debatable. What it does demonstrate is the gap between ambition and delivery in crime mapping within England and Wales.

In contrast, the approach adopted in West Yorkshire has sought to reconcile the tensions between accessibility and sensitivity with a clear focus on the public interest and a bias towards accuracy.

Naturally, the West Yorkshire model recognizes that there are sensibilities around certain types of crime and criminality, as well as legal restrictions on publishing information from which victims might be identified. Similarly, although someone suitably motivated and having the right software could possibly extrapolate from the West Yorkshire data a specific address outside which a car had been stolen or a person robbed, but is this a reason to withhold or adulterate all the data all the time? An alternative approach that has been suggested involves ‘moving’ the locus of the offence a set distance in a random direction (say within a radius of 30 m). While this would certainly reduce the likelihood of identifying a particular person or place, the adulteration of the data would surely have a similar diluting effect on its utility and therefore its efficacy in informing and empowering the public. There is, it is proposed, an irreducible minimum beyond which data become so vague as to be at best unhelpful and at worst damaging to public confidence in that it dashes expectations and hints at disingenuousness.

For this reason, the West Yorkshire Beatcrime model plots reported crimes down to the street where they occurred and, although there are special considerations for isolated places (e.g. remote dwellings within farmland), the approach tries wherever possible to identify the true location of the crime.

Notwithstanding these efforts, Giogrande *et al.* remain critical of the lack of specificity in the information provided by those police authorities such as West Midlands and West Yorkshire who do make such information available (although they do describe a Metropolitan Police test site that provides burglary, robbery and vehicle offences per month and yearly trends as ‘promising’).

Though compared, these sites are not comparable because, at the time of writing at least, the degree of detail provided by police bodies in England and Wales is not simply variable but also binary: the only police force providing specific ‘dots-on-maps’ type information about specific geographical locations is the West Yorkshire Police. Nevertheless, bloggers and commentators from the CDA community go further than Giogrande and make the argument *supra* that averaging should be avoided altogether, and point data should be used instead, with all maps having overlays to explain crime spikes and day/night splits. On the other hand, the highly regulated environment of the UK places some real hurdles in the way of public bodies that wish to open their data banks to scrutiny, at the heart of which beats the European Convention on Human Rights which seeks constantly to balance the competing interests of the individual, the State and the wider public good. Beneath that framework there is the domestic legislation such as the Data Protection Act 1995 (which applies a series of principles that must be applied by all who keep personal data records) and the Freedom of Information Act 2000 that is designed to facilitate public access to data collated by public bodies. Responsibility for overseeing the operation of this legislative framework generally falls to the Office of the Information Commissioner (OIC) who wrote to a number of police organizations and the Home Office during the development of crime mapping identifying areas of potential

conflict between the rights of individuals and the wider public interest and seeking reassurances before their sites went ‘live’.

Since the enactment of the Human Rights Act 1998 in the UK, there have been some significant and substantial challenges to the State's collection and use of personal data for criminal justice purposes—most notably the challenge to the police practice in England and Wales of retaining DNA data on individuals even after they have been found not guilty of an offence or proceedings against them have been discontinued (*S & Marper v UK*, 2008). Interestingly, the OIC has itself recently required the government to abandon its practice of withholding details of parties to employment disputes and to reveal the names and addresses of organizations involved in proceedings before the employment tribunals.²⁶

Nevertheless, despite the provisions of the freedom of information regime and the decisions of the OIC, there remains something of a contrast between the UK and the much more open data culture elsewhere, for example the USA where, although there are similar federal and constitutional laws balancing privacy with publicity, practices are distinctly different and prosecution policies are openly discussed on weblogs and in public forums. Giogrande recognizes that the legal and cultural approach in countries such as the USA differs significantly from that of the UK and cites some very useful examples that evidence the position (Privacy Rights Clearinghouse, 2006; Kerr and Shelton, 2001).

► The future

The corollary to CDA is a reverse flow of information *from* communities back towards their public services. Indeed if the Policing Pledge in the UK is to take the form of a sort of contractual undertaking, then beyond the basic *consensus ad idem* there needs to be some ‘consideration’ flowing from the other contracting party: the citizen. This remains a largely unexplored benefit of crime mapping and is one that it will potentially allow a two-way exchange of information between the police and the policed. Though yet to mature, it is easy to see how this two-way interaction using crime mapping might work. By choosing to visit the site, individuals are indicating their interest in the work of the relevant policing organization. As such these visitors form a self-selecting group who might be interested in helping the police in other consultation programmes or in wider participative activities that address the issues underlying the published statistics, from crime detection to preventing violent extremism. Not only would this fit within the generic statutory obligation on police authorities in England and Wales to consult with their communities; it would also be consonant with the strategy, for example, of the West Yorkshire WaYs to meaningful engagement.²⁷ Interactive mapping will help the Police Authority to show what has been done and indicate where the

improvement is to be found, before beginning the consultation cycle once more.

The crime mapping system can also have benefits in terms of performance monitoring, testing the effect of policing initiatives and the visibility of information provision down to a neighbourhood level, with the nature, frequency or content of visits to the site revealing something about the user or usage. Postal or zip code trawls will allow the site host to group the areas of search and therefore see, for example, if there has been any increased activity in enquiries around an area where there has been targeted action or communication. But then this activity itself raises questions of data monitoring and privacy. Then there is the larger consideration of expense; maintaining up-to-date sites is an expensive endeavour—which might be why most examples of crime mapping sites in the USA are not maintained by the police at all but by external bodies to whom the crime data are given by the relevant criminal justice agency.²⁸ Providers of UK crime maps will need to consider these practicalities as the expectations of their communities become increasingly sophisticated in their demands. An alternative to outsourcing control of the sites might be some form of commercial sponsorship (for example with an insurer) or at least partnership with other public sector organizations.²⁹

► Conclusion

However they map out, the activities of the 43 police forces of England and Wales will carry some risk in the future. The first risk is that they are challenged under the regulatory framework for maintaining individual privacy. Another is that they might be challenged by business interests such as estate agents claiming that the publication has adversely affected already falling house prices.³⁰ The answer to such challenges surely lies in the fact that it is not the *publication* of the data that ought to concern us but rather the fact that the crimes have occurred. In addressing the situation complained of, it is interesting to ask the question "which of the following is preferable: galvanization of joint efforts to prevent the reality of criminal activity in a particular area or suppression of the truth in order to create a more favourable but inaccurate perception?" Is this really what public confidence requires? But there are, it is submitted, far greater risks. One, highlighted by Giogrande, is that the crime mapping sites fail to go beyond mere presentation of a criminal activity and avoid stating what was done about it. In his view, merely presenting detail of the crime without the correction gives a very unbalanced view of UK criminal justice to the public.³¹ In this light, there must be a strong argument in favour of, for example, sentence mapping showing how cases are disposed of at each court within a locality for the same reasons as crime mapping: to provide clear and reliable evidence of the relevant activity being undertaken by the criminal justice system and also to address any perception that the courts are being unduly lenient with those they convict.³²

Whatever the manner and form that criminal justice ‘mapping’ takes in the future, in mitigating or closing out the relevant risks, the challenge for public authorities will be to balance accuracy with sensitivity and privacy. While in technological terms ‘the use of statistical devices of various kinds on maps is limited only by the analyst's imagination’ (Harries, 1999); the reality for those policing organizations seeking to produce accurate and useful crime maps in the UK is ‘far harder than it appears’ and—as the Home Office has been warned—‘does not rely only on geographical information’³³ though, at the request of the Home Office, Pitney Bowes MapInfo has at least released a white paper on best practice³⁴ to help them. The paper itself envisages fundamental problems because ‘a significant amount of crime goes unrecorded, location may be uncertain, and time of day, seasons and even the activities of the police will make figures vary’³⁵ and suggests a wide amount of consultation with local authorities, social, health and emergency services, MPs, community groups as well as ‘crime pattern influencers’, business groups and others—including presumably the e-advocacy and e-activists referred to above.

Further risk resides in the outsourcing options and the possibility of data sets being given to or taken over by the daunting array of professionals (lawyers, copyright experts, librarians, archivists, cartographers, engineers, communications activists, open source programmers and new media designers) prepared to offer their services in helping to make civic data and information ‘available to citizens without restrictions, at no cost, in usable open formats’.³⁶ This would potentially lead to loss of control, consistency or (ironically) confidence.

But perhaps one of the greatest strategic risks is that all 43 organizations will continue plotting their own crimes in their own way and proliferating a maze of systems that not only prevent public access to accurate data but also preclude any meaningful comparison across what are, in the end, entirely artificial boundaries.

Whatever the future direction of crime mapping, former crime reporter Heather Brooke says³⁷ that we cannot afford to ignore the issues set out here.

When the deadline for all police forces to make crime mapping information available expired at midnight 31 December 2008, those organizations still faced something of a dilemma but ultimately the response to the growing expectation of civic data provision will call for the exercise of mature judgment.

From a starting point that, as it has been collated and processed and analysed at the public's expense, the public have substantial intellectual property rights in the data sets, if people in communities are seriously expected to make a meaningful contribution to the debate around their public services, let alone assist in shaping their delivery, those in charge of the services must make sure that they are able to access the relevant information needed to make sense of the challenges. The biggest risk is, it seems, that public bodies are not yet fully willing or able to do so.

Notes

- ¹ *Police Professional*, 31 July 2008. 
- ² www.Beatcrime.info. 
- ³ In England and Wales, the police authority is the legal body corporate that employs staff and provides governance to the relevant police force whose resources and officers are under the direction and control of the chief constable/commissioner (see the Police Act 1996). 
- ⁴ *Police Professional*, *ibid.* 
- ⁵ For example, see <http://icicp.blogspot.com/>;
<http://www.projectcensored.org/>;
<http://www.opendemocracy.net/article/china-democracy-in-action>. 
- ⁶ See also Citizens for Open Access to Civic Information and Data that describes itself as a ‘loose grouping of academics, activists, and citizens concerned with promoting data liberation in Canada’. 
- ⁷ *The Guardian*, 3 May 2008. 
- ⁸ *The Register*, 23 June 2008. 
- ⁹ *The Times*, 18 June 2008. 
- ¹⁰ Cm 7448. 
- ¹¹ *Closing the Gap*, MORI 2008. 
- ¹² www.direct.gov.uk/policingpledge. 
- ¹³ *Ibid.* 
- ¹⁴ *Crime Statistics: An Independent Review Carried Out for the Secretary of State for the Home Department*, November 2006. 
- ¹⁵ *The Times*, June 26, 2008. 
- ¹⁶ Skills for Life Survey 2003, DFES research report 490. 
- ¹⁷ Home Office Press Release, 5 March 2009. 

- ¹⁸ See comments of the Policing Minister Vernon Coaker, MP, *The Daily Telegraph*, 7 January 2009. [↑](#)
- ¹⁹ See, for example, observations of the Police Federation of England and Wales, *The Daily Telegraph*, 7 January 2009. [↑](#)
- ²⁰ See, for example, the Sexual Offences Act 2003. [↑](#)
- ²¹ *The Register*, 25 June 2008. [↑](#)
- ²² <http://www.freeourdata.org.uk/blog/?p=194>. [↑](#)
- ²³ http://www.jdi.ucl.ac.uk/crime_mapping/web%20statistics.php. [↑](#)
- ²⁴ A technique used in Europe from the early 19th century but a term generally attributed to a geographer, J. K. Wright, with the American Geographical Society (AGS) in New York City in 1938. [↑](#)
- ²⁵ *Ibid.* [↑](#)
- ²⁶ OIC, 14 October 2008. [↑](#)
- ²⁷ This follows a cycle of *We asked, You said, We acted, You saw*. [↑](#)
- ²⁸ For example, U.S.: Crime Reports: ‘Crimereports.com is a US site built to help citizens get more information about the locations and frequencies of crime incidents in their cities.’ [↑](#)
- ²⁹ For a good UK example, see the LASOS system operated within South Yorkshire with the support of the local government of Yorkshire and Humber—www.lasos.org.uk. [↑](#)
- ³⁰ See the comments of the Royal Institute of Chartered Surveyors, *The Daily Telegraph*, 7 January 2009. [↑](#)
- ³¹ *Ibid.*, p. 9. [↑](#)
- ³² This, according to Casey (*ibid.*), is the single biggest contributor to public confidence in the criminal justice system. [↑](#)
- ³³ *The Guardian*, 11 December 2008. [↑](#)
- ³⁴ Pitney Bowes MapInfo Press Release, ‘Crime in Focus’, 2 December 2008. [↑](#)
- ³⁵ *The Guardian supra.* [↑](#)
- ³⁶ Citizens for Open Access to Civic Information and Data. [↑](#)
- ³⁷ *Ibid.* [↑](#)

References

Baranski J. V., Petrusic W. M. On the Calibration of Knowledge and Perception. *Canadian Journal of Experimental Psychology* (1995) 49:397–407. [\[CrossRef\]](#)[\[Medline\]](#)

Casey L. *Engaging Communities in Fighting Crime*. (2008) London: Cabinet Office.

Flanagan R. Sir. *The Review of Policing* (2008) HMCIC, February 2008.

Giangrande R., Haldenby A., Lundy L., Parsons L., Thornton D., Truss E. *The Lawful Society*. (2008) Reform.

Harries K. *Mapping Crime: Principle and Practice* (1999) December 1999 NCJ 178919, National Institute of Justice.

Kerr T., Shelton R. (2001) *Privacy and the Development of Online Criminal Databases*.

Privacy Rights Clearinghouse. *Public Records on the Internet: The Privacy Dilemma*. (2006).

S & Marper v UK. (2008) ECtHR, 4 December.

Tuffin R., Morris J., Poole A. *An Evaluation of the National Reassurance Policing Programme*. (2006) Home Office Research Study 296.

White M. P., Eiser J. R. Information Specificity and Hazard Risk Potential as Moderators of Trust Asymmetry. *Risk Analysis* (2005) 25:1187–1198. [\[CrossRef\]](#)[\[Web of Science\]](#)[\[Medline\]](#)

White M. P., Eiser J. R. A Social Judgement Analysis of Trust: People as Intuitive Detection Theorists. In: *Trust in Cooperative Risk Management: Uncertainty and Scepticism in the Public Mind—* Siegrist M., Earle T., Gutscher H., eds. (2007) London: Earthscan. 95–116.

Item 2

“Cyberspace: the new frontier for policing?” 2015, Chapter 1 pp 1-10 in
“Cyber Crime and Cyber Terrorism Investigators’ Handbook
Akhgar, B., Staniforth, A., Bosco, F. (Eds) Elsevier

eBook ISBN: 9780128008119

Paperback ISBN: 9780128007433

Cyberspace: The new frontier for policing?

Fraser Sampson

Published in 2011, the UK Cyber Security Strategy states that:

“Our vision is for the UK in 2015 to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society.”

That the United Kingdom even has a cyber security strategy is telling. Governments and their agencies—not only in the United Kingdom but worldwide—have struggled to distinguish criminality that specifically relies on the use of the hyper-connectivity of global information technology from “ordinary” crime that is simply enabled by using information and communication technology. Despite legislative interventions such as the Council of Europe Convention on Cybercrime (for an analysis of which see Vatis, 2010, p. 207) in 2001, cyberspace remains a largely unregulated jurisdictional outpost.

The first piece of criminal legislation to address the use—or rather the misuse—of computers in the United Kingdom was enacted in 1990. The recital to the Computer Misuse Act 1990 states that it was an act “to make provision for securing computer material against unauthorized access or modification; and for connected purposes.” This narrow, pre-Internet focus was very much predicated on the concept of a computer as a functional box (or network of boxes) containing “material” that required protection (Sampson 1991a, p. 211). Although the Act addressed unauthorized access, the concept of causing a computer to perform a function in furtherance of other crimes was also a central part of the new legislation (Sampson, 1991b, p. 58) which, for the first time in the United Kingdom, sought to catch up with computer technology that was becoming part of people’s everyday lives—a race in which the legislative process did not stand a chance.

While the legislation was amended in 2006 with the introduction of a new criminal offence of unauthorized acts to impair the operation of a computer or program, etc., looking back through

today's digital prism, the legislation has a decidedly analog look to it. When the legislation came into force we had little idea of the impact the "information super-highway" would have on our everyday lives, still less the *engrenage* effect of social media. According to the UK's 2011 Cyber Security Strategy, at the time of its publication 2 billion people were online and there were over 5 billion Internet-connected devices in existence. During that same year, the number of people being proceeded against for offences under the Computer Misuse Act 1991 in England and Wales, according to a document from the Ministry of Justice, was nine (Canham, 2012) with no people being proceeded against for the two offences under s.1(1) and s.1(3). Perhaps as surprisingly, the records from the Police National Legal Database (PNLD) used by all police forces in England and Wales for offence wordings, charging codes, and legal research show that during two weeks (chosen at random) in 2013 the Computer Misuse Act 1990 and its constituent parts were accessed as follows:

Between 4th and 10th March—907 times
Between 10th and 16th
November—750 times.

Reconciling these two data sets is difficult. While it is clear from the PNLD access data that law enforcement officials in England and Wales are still interrogating the 1990 legislation frequently (on average, around 825 times per week or 118 times per day or annually 42,900 times), the number of prosecutions for the correlative offences is vanishingly small. One of the many challenges with cybercrime and cyber-enabled criminality is establishing its size and shape.

THE SHAPE OF THE CHALLENGE

Just as the shape of our technology has changed beyond all recognition since 1990, so too has the shape of the challenge. The almost unconstrained development of Internet-based connectivity can be seen, on one hand, as a phenomenological emancipation of the masses, an extension of the Civil Data Movement and the citizens' entitlement to publicly held data (see (Sampson and Kinnear, 2010)). On the other hand, the empowerment it has given

others (particularly sovereign states) to abuse cyberspace has been cast as representing the “end of privacy” prompting a petition to the United Nations for a “bill of digital rights.”

Steering a predictably middle course, the UK strategy sets out the key—and, it is submitted, most elusive—concept within the document: that of a “vibrant, resilient, and secure cyberspace.” The aspiration must surely be right but how can resilience and security be achieved within a vibrant space run by computers? In terms of both computers and our reliance upon them, we have moved so far from the original notion of boxes, functions, commands and programs, along with the consequences that can be brought about by their use, that a fundamental re-think is needed.

So what—and where—is cyberspace? Much has been written recently on the threat, risk and harm posed by “cybercrime,” “e-crime,” “cyber-enabled” criminality but the legislation has been left a long way behind. The EU has a substantial number of workstreams around its “Cybersecurity Strategy” and its own working definition of “cyberspace” though its own proposed Directive has no legal definition but rather one for Network and Information Security to match the agency established in

2004 with the same name. In the United Kingdom, a parliamentary question in 2012 asked the Secretary of State for Justice how many prosecutions there had been for “e-crime” in the past 5 years. In response, the Parliamentary Under Secretary of State gave statistics for ss 1(4), 2 and 3(5) of the Computer Misuse Act while the correlative Hansard entry uses the expression “cybercrime” in its heading.

Wherever it is, constitutional lawyers around the world have wrestled with the applicability of their countries’ legislation with the borderlessness of the virtual world of the Internet; the application of “analog” territorial laws to the indeterminable digital boundaries of the infinite global communications network is, it seems, proving to be too much for our conventional legal systems. Here is why.

When it comes to interpreting and applying law across our own administrative jurisdictional boundaries, an established body of internationally agreed principles, behavior, and jurisprudence has developed over time. Some attempts have been made to apply these legal norms to cyberspace. For example, the International Covenant on Civil

and Political Rights sets out some key obligations of signatory states. In addition, activities executed within or via cyberspace should not be beyond the reach of other community protections such as those enshrined in the European Convention of Human Rights or the EU Charter of Fundamental Rights, particularly where issues such as online child sexual exploitation are involved. The first basic challenge that this brings however, is that of jurisdiction.

Cottim has identified five jurisdictional theories and approaches in this context, namely (Cottim A. 2010):

1. *Territoriality theory*: The theory that jurisdiction is determined by the place where the offence is committed, in whole or in part. This “territoriality theory” has its roots in the Westphalian Peace model of state sovereignty that has been in place since 1684 (see Beaulac, 2004, p. 181). This approach has at its heart the presumption that the State has sovereignty over the territory under discussion, a presumption that is manifestly and easily rebuttable in most “cyberspace” cases.
2. *Nationality (or active personality) theory*: Based primarily on the nationality of the person who committed the offence (see *United States of America v. Jay Cohen*; Docket No. 00-1574, 260 F.3d 68 (2d Cir., July 31, 2001) where World Sports Exchange, together with its President, were defendants in an FBI prosecution for conspiracy to use communications facilities to transmit wagers in interstate or foreign commerce. The defendants were charged with targeting customers in the United States inviting them to place bets with the company by toll-free telephone call or over the Internet). While the Antiguan Company was beyond the jurisdiction of the court, the President was a US citizen and could, therefore, be arraigned before an American criminal court.
3. *Passive personality theory*: While the “nationality theory” deals with the nationality of the offender, the “passive personality theory” is concerned with the nationality of the victim.

In what Cottim calls “the field of cybercriminology,” a good example of this jurisdiction assumption can be seen in a case where a Russian citizen who lived in Chelyabinsk, Russia

was sentenced by a court in Hartford Connecticut for hacking into computers in the United States.

4. *Protective theory*: Cottim’s “protective theory” (also called “security principle” and “injured forum theory”) deals with the national or international interest injured, assigning jurisdiction to the State that sees its interest—whether national or international—in jeopardy because of an offensive action. Cottim sees this rarely used theory as applying principally to crimes like counterfeiting of money and securities.

5. *Universality theory*: In his final theory, Cottim identifies the approach of universality based on the international character of the offence allowing (unlike the others) every State to claim of jurisdiction over offences, even if those offences have no direct effect on the asserting State. While this theory seems to have the most potential for applicability to cyberspace, there are two key constraints in the way it has been developed thus far. The first constraint is that the State assuming jurisdiction must have the defendant in custody; the second is that the crime is “particularly offensive to the international community.” While this approach has, Cottim advises, been used for piracy and slave trafficking there is considerable practical difficulty in defining the parameters of the universality approach even in a conventional context and the possibility of extending it to cover cyberspace offending and activity is as yet unexplored.

When it comes to conventional extra-territorial challenges, the device of focusing on key elements such as the nationality of the offender and the geographical location of the causal conduct or consequent harm has produced some successful prosecutions for (and perhaps thereby deterred) some conventional cyber-enabled offending. For example, Cottim cites a case where the Managing Director of CompuServe Information Services GmbH, a Swiss national, was charged in Germany with being responsible for the access—in Germany—to violent, child, and animal pornographic representations stored on the CompuServe’s server in the United States. The German court considered it had jurisdiction over the defendant, although he was Swiss, he lived in Germany at the time. The Amtsgericht court’s approach has been criticized as not only unduly harsh but as unsustainable and it is difficult to argue with Bender who says “it must be noted that the ‘law-free zones’ on the Internet cannot be filled by a ruling like this, but need a new self-regulatory approach” (Bender, 1998).

In some cases litigants also use the jurisdictional differences to argue down the gravity of the sanction or the extent of their liability, particularly where the perpetrator from one jurisdiction brings about consequence in another. A good recent example is *Klemis v Government of the United States of America* [2013] All ER (D) 287 where the UK defendant allegedly sold heroin to two men in Illinois, USA. One of the men subsequently died and raised questions at the point of sentencing as to how the different legislatures in the two jurisdictions had set the requirements for the relevant *actus reus* (criminal act) and the *mens rea* (culpable state of mind) differently. Another recent example of trans-jurisdictional friction is *Bloy and Another v Motor Insurers' Bureau* [2013] EWCA Civ 1543. In that case a road traffic collision in the United Kingdom had been caused by a Lithuanian national who had been uninsured at the time. The Motor Insurers' Bureau is the UK compensation body for the purposes of the relevant EU Directive and was obliged to pay compensation where a UK resident had been injured in a collision in another Member State caused by an uninsured driver. In such cases, the Directive enabled the Bureau to claim reimbursement from the respective compensatory body in the other Member State. However, under the domestic law of Lithuania the liability of the compensatory body was capped at €500k. The Bureau argued that its liability to pay the victim should be capped by Lithuanian domestic law even though the collision happened on an English road.

Clearly the challenges of unauthorized access and use of data obtain; so too do the jurisdictional challenges of locus of initiators and consequences. However, these have to be understood in the context of the much more pernicious and truly viral threats such as denial of service attacks, malware, data espionage and what Cottim calls the scareword of “cyber-terrorism” which has now become formally adopted by many law enforcement agencies, politicians and commentators. The reality is that, with the requisite knowledge and motivation, a teen with a laptop can alter the “use by” dates on food products in a packing plant on the other side of the world, or command the central heating system of a neighbor's Internet-connected home to overheat, or send the traffic lights in a far away city into a frenzy. The further reality is that the wattle-and-daub constructs of conventional law making in common law countries, along with their correlative law enforcement practices, will not provide the answer to these threats and risks and even staples such as “crime scenes” and “perpetrators” are no longer adequate within the new frontier of cyberspace.

However, it is not just the domination and manipulation of cyberspace by criminals that has caused public concern. The aftermath of the Edward Snowden revelations about intrusive governmental espionage demonstrated that cyberspace is regarded as a potentially perilous place by private users not just in fear of becoming victims of remote criminality. There is also a real fear that the technological environment allows state agencies to operate in highly intrusive yet anonymous and unaccountable ways, prompting the CEOs of some of the world's leading IT companies to write an open letter to the President of the United States demanding reform of cyberspace surveillance based on a series of overarching principles that guarantee the free flow of information yet limit governmental authority and impose a substantial degree of oversight (Armstrong et al., 2013).

What then is the size of the challenge presented by this amorphous construct of cyberspace?

THE SIZE OF THE CHALLENGE

The population of cyberspace is estimated by the UK government to be >2 billion. While we do not accurately know the frequency or longevity, this means that one-third of Earth's population visit cyberspace and billions more are anticipated to join them over the next decade, exchanging over \$8 trillion in online commerce.

According to the Commissioner of the City of London Police, "cyber" fraud (broadly offences of dishonesty committed by use of computer networks) costs the UK £27 billion per year while "cyber breaches" (presumably involving the unauthorized infiltration of a private or public computer network) have been recorded by 93% of small and medium businesses in the United Kingdom in 2013, an increase of 87% on the previous year.

Aside from some of the peculiar criminological features unique to crime committed in cyberspace (such as the absence of any real motive for anyone—individual or corporate victims or their Internet Service Providers—to report crimes involving fraud) the basic challenge facing us now seems to be how to get to grips with the concept of cyberspace—vibrant, resilient, secure or otherwise. Having separated cybercrime from cyber-enabled

crime in the same way we might separate crime within a transport network from crime where the transport network is merely an enabler, surely we need to begin to treat cyberspace for what it is: a separate socio-spatial dimension in which people choose not only to communicate, but also to dwell, trade, socialize and cultivate; to create intellectual property, generate economic wealth, to begin and end relationships; to forage, feud and thrive; to heal and harm. Viewed in this way cyberspace is another continent, vast, viable and virtual, a distinct jurisdiction requiring its own constitution and legal system, its own law enforcement agents and practices. The Director of Operational Policing Support for Interpol's General Secretariat, Michael O'Connell, has compared the movement across cyberspace with "the 2 billion passenger movements across the world." The reality is that cyber travellers move around the borderless virtual globe with almost immeasurable speed, almost zero cost and almost total anonymity.

The challenge of tackling cyber security stretches way beyond simply standardizing our legal frameworks. The UK Government has also recognized that "Without effective cyber security, we place our ability to do business and to protect valuable assets such as our intellectual property at unacceptable risk." In the report commissioned by the UK Government, Price Waterhouse Coopers estimate that there are over 1000 different global publications setting out cyber standards. Moreover, their assessment of the standards situation across organizations looked patchy and incomplete.

While the awareness of cyber security threats and the importance placed on them was generally found to be high, the efforts to mitigate cyber security risk differ significantly with the size of the organization and its sector. The report found that only 48% of organizations implemented new policies to mitigate cyber security risks and only 43% conducted cyber security risk assessments and impact analysis to quantify these risks. The report also found that 34% of organizations who purchased certified products or services did so purely to achieve compliance as an outcome. Although the authors are clear in pointing out that the online survey reached an audience of ~30,000 organizations, it produced around 500 responses, not all of them complete. Nevertheless, the picture that emerges from the report is one of a fragmented and nonstandardized response to a global threat.

THE RESPONSE

Aside from stretching and reworking legal principles such as jurisdiction and issuing strategies, there have been several key responses to the challenges of cybercrime and cyber-enabled criminality. For example, the Metropolitan Police Service was recently reported as having substantially expanded its E-crime unit to a reported 500 officers in response to the threat of “cybercrime” having become a Tier One National Security threat. This is consistent with the responses having effect across the UK law enforcement community. The Police Reform and Social Responsibility Act 2011—the legislation that created elected police and crime commissioners— also introduced the concept of the Strategic Policing Requirement (SPR). The SPR is published by the Home Secretary and sets out those national threats that require a coordinated or aggregated response in which resources are brought together from a number of police forces; it applies to all police forces in England and Wales and is referred to by other law enforcement agencies throughout the United Kingdom.

The SPR identifies how police forces and their governance bodies often need to work collaboratively inter se, and with other partners, national agencies or national arrangements, to ensure such threats are tackled efficiently and effectively.

The SPR contains five areas of activity and threat that are, if at a Tier One or Tier Two risk level in the National Security Risk Assessment, covered. These are:

- Terrorism (Tier One)
- Other civil emergencies requiring an aggregated response across police force boundaries
- Organized crime (Tier Two)
- Threats to public order or public safety that cannot be managed by a single police force acting alone
- A large-scale cyber incident (Tier One) including the risk of a hostile attack upon cyberspace by other states

The SPR recognizes that there may be considerable overlap between these areas. For example, there may be a substantial organized crime element involved in a cyber incident and vice versa. All elected police and crime commissioners and their respective chief police officers must have regard to the SPR in their planning and operational arrangements. This is an important legal obligation for reasons that are discussed below.

Having set out these key risks to national security, the SPR requires policing bodies to have adequate arrangements in place to ensure that their local resources can deliver the requisite: Capacity Capability Consistency Connectivity and Contribution to the national effort (the five “Cs”).

Given the legal and practical difficulties that are explored *infra*, the extent to which local policing bodies are in a position to meet these criteria in a meaningful way in relation to “cyber incidents” — whether “upon” or within cyberspace is questionable. For example, while it is a relatively simple task to assess the capacity and capability of a group of local police force (even a large one such as the Metropolitan Police) to tackle large-scale public disorder, and to measure the connectivity of their resources in preparing for such an event, it is far harder to demonstrate that the same forces meet the five C requirements (capability, connectivity, and so on) required to understand and respond to even a highly localized cyber incident, still less a cyber attack sponsored by another state. This too is important because the courts in the United Kingdom have interpreted the expression “have regard to” a government policy as meaning that public bodies fixed with such a duty must above all properly understand that policy. If a government policy to which a public body must have regard is not properly understood by that body this has the same legal effect as if that body had paid no regard to it at all. Further, if a public body is going to depart from a government policy to which it must “have regard,” that body has to give clear reasons for doing so, such that people know why and on what grounds it is being departed from. While the EU might have a series of arrangements in place which require Member States to notify them of “incidents” that “seem to relate to cyber espionage or a state-sponsored attack” and invoke the relevant parts of the EU Solidarity Clause, there is little evidence that most police areas would be in a position confidently to make that assertion, promptly or at all.

Quaere: how well are all affected police agencies in England and Wales able to demonstrate that they have properly understood the threat of a cyber attack in the context of the SPR? If the answer to this is anything other than an unqualified “yes,” then they might do well to issue a notification to that effect to their respective communities and stakeholders.

CONCLUSION

Tackling computer-enabled criminality has generally focused on the physical presence of those controlling, benefiting, or suffering from the remote activity—it has been concerned with input and output. The European Union has a proposed Directive to require Member States to ensure they have minimum levels of capability in place, along with Computer Emergency Response Teams (CERTs) and arrangements for effective coordination of “network and information systems.” At the same time the Budapest Convention has been in force for almost a decade to provide a model for the many signatory nations (including the United States) to draft their domestic “cybercrime” legislation and the correlative cyber security industry is vast and burgeoning. But is there not a pressing need to tackle what is taking place in cyberspace itself? Using existing jurisdictional theories is arguably not enough; what is needed is not a partial application of some extra-cyberspace laws adapted to suit some extra-cyberspace consequences. Continuing to apply the traditional criminological approaches to technological innovation in the context of cyberspace is, it is submitted, rather like separating criminality that takes place within an underground transport network from that where the offender uses the London Underground to facilitate their offending. In the first situation the setting is a key component of the offending while, in the second, it is a chosen part of the wider modus operandi and the offender might just as easily have chosen to take the bus, a taxi or to walk to and from the locus of their crime. This is the fundamental difference between cyber-enabled offending and offending within cyberspace. Policing the exits and entrances is never going to be a complete or even satisfactory answer to the latter. Aside from the practical and jurisprudential reasons, there are also important political imperatives beginning to emerge. For example India’s Telecom and IT Minister

Kapil Sibal asserted recently that there should be “accountability and responsibility” in the cyberspace in the same way as in diplomatic relations:

“If there is a cyberspace violation and the subject matter is India because it impacts India, then India should have jurisdiction. For example, if I have an embassy in New York, then anything that happens in that embassy is Indian territory and there applies Indian Law.”

For this approach to go beyond the conventional jurisdictional approaches considered supra would require a whole new set of processes, procedures and skills; it would take more than the publication of a set of agreed standards or an agreed recipe for domestic legislation. There needs, it is submitted, to be a new presence in cyberspace, a dedicated cyber force to tackle what the Director-General of the National Crime Agency, Keith Bristow, calls “digital criminality.” Perhaps what is needed is not a new way of overlaying our conventional law enforcement assets and techniques on cyberspace or a new way of extending our two-dimensional constructs of jurisdiction to fit a multi-dimensional world, but a new wave of cyber assets—“cyber constables” as it were—to patrol and police the cyber communities of the future. However, given our global experience of the ways in which some state agencies have operated within cyberspace, in the post-Snowden era that perennial question of democratic law enforcement “quis cusodiet” sits just as fixedly above cyber policing as it has in every analog setting to date.

REFERENCES

Armstrong, T., Zuckerberg, M., Page, L., Rottenberg, E., Smith, B., Costelo, D., 2013. An Open Letter to Washington. 9 (December 2013).

Beaulac, S., 2004. The Westphalian model in defining international law: challenging the myth. *Austral. J. Legal History* 7, 181–213.

Bender, G., 1998. *Bavaria v. Felix Somm: the pornography conviction of the former CompuServe manager*. *Int. J. Commun. Law Policy Web-Doc* 14-1-1998.

- Canham, D., 2012. Freedom of Information Request to Secretary of State for Justice. (accessed 24.10.2012). https://www.whatdotheyknow.com/request/computer_misuse_act_2.
- Cottim, A., 2010. Cybercrime, cyberterrorism and jurisdiction: an analysis of article 22 of the COE convention on cybercrime. *Eur. J. Leg. Stud.* 2 (3), European University Institute, San Domenico de Fiesole, Italy.
- Sampson, F., 1991a. Criminal Acts and Computer Users Justice of the Peace. *Chichester* 155 (14), 211.
- Sampson, F., 1991b. Criminal Acts and Computers. March 1991, Police Requirements Support Unit Bulletin 39, 58, Home Office Science & Technology Group, London.
- Sampson, F., Kinnear, F., 2010. Plotting criminal activity: too true to be good crime mapping in the UK. *Oxford J. Policing* 4 (1), 2–3.
- Vatis, M.A., 2010. Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. National Research Council, The National Academies Press, Washington, DC, pp. 207–223.

Item 3

“The Legal Challenges of Big Data Application in Law Enforcement” 2015,
Chapter 15 pp 229 – 237 in *“Application of Big Data for National Security –
A Practitioner’s Guide to Emerging Technologies.”*
Akhgar, B., Saathoff, G., Arabiana, H., Hill, R., Staniforth, A., Bayerl, S. (Eds)
Elsevier

eBook ISBN: 9780128019733

Paperback ISBN: 9780128019672

THE LEGAL CHALLENGES OF BIG DATA APPLICATION IN LAW ENFORCEMENT

Fraser Sampson

INTRODUCTION

Big Data “calls for momentous choices to be made between weighty policy concerns” (Polonetsky and Tene, 2013). The weighty policy concerns also have to weigh in the balance the most efficient and effective use of available resources with the fundamental rights and freedoms of individuals. One of the weightiest policy concerns is that of law enforcement. The setting of law enforcement raises several dilemmas for Big Data; because Big Data represents such an expansive, dynamic, and complex subject, this chapter is necessarily selective and succinct.

In the opinion of the European Union Data Protection Working Party,⁶ “Big Data” refers to exponential growth in both the availability and the automated use of information. Big Data refers to “gigantic digital datasets held by corporations, governments and other large organisations, which are then extensively analysed using computer algorithms.”

ATTRACTIONS OF BIG DATA

One of the principal attractions—if not *the* principal attraction—of Big Data is its enabling of analytics, the almost limitless power that attends the super-synthesis of information. Offering what perhaps are the obverse attractions of nano-technology, Big Data’s giga-analytics can produce macro-level pictures of trends, pathways, and patterns that might reveal pictures hitherto unseen even by the data owners. Such tele-analytics allow not only a better understanding of what may be happening here and now, but a reliable basis for predictions of what is to come.

⁶Article 29 Data Protection Working Party 00,569/13/EN WP 203 Opinion 03/13, p. 35.

Aside from the obvious attraction for commercial suppliers trying to understand, predict, and influence consumer behavior, Big Data analytics also holds out a phenomenological capability for law enforcement agencies in trying to understand, predict, and influence behaviors of offenders and potential offenders.

As Professor Akghar from CENTRIC⁷ puts it, “When we look at ways to advance the use of data and analytics for public security and safety, the potential has never been greater. We now have the computing power to not only understand past events, but also to create new knowledge from billions of data points—quickly. In minutes, we can run analyses that used to take days” (Akhgar, 2014).

DILEMMAS OF BIG DATA

With so much data so readily available, one might ask on what basis would law enforcement agencies (LEAs) not seize it and run with it as far and as fast as possible, if doing so meant preventing terrorist attacks, disrupting serious organized crime, or preventing wide-scale child sexual exploitation, human trafficking, and so forth?

Take, for example, successful work in Greater Manchester⁸ that has shown the power of having a range of agencies literally in the same room. Why not have the totality of their data virtually present in the same place, too? Because Big Data can be applied to mass datasets to reveal high-level trends and patterns, it might be thought that the extent to which it can assist in preventing and detecting criminality is limited. Not necessarily. As the Article 29 Working Party⁹ noted, not only can the awesome capability offered by Big Data be used to identify general trends and macro-correlations, it can also be processed—rapidly and almost effortlessly—to directly affect the individual.¹⁰

⁷The Centre for Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research at Sheffield Hallam University, UK

⁸ See “Greater Manchester against crime: A complete system for partnership working,” available at: <https://www.ucl.ac.uk/jdi/events/mapping-conf/conf-2005/conf2005-downloads/dave-flitcroft.pdf>.

⁹ This Working Party is made up of EU member state national data protection authorities and is an independent advisory body on data protection and privacy. Established under Article 29 of the Data Protection Directive (95/46/EC), its role is to contribute to the uniform application of the Directive across member states.

¹⁰ Data Protection Working Party loc. cit

From a practical operation perspective, then, there is a vast potential for Big Data in law enforcement. From a legal perspective, the point at which Big Data focuses this astonishing power on individuality can become highly contentious. One such point is where it is used for law enforcement, whether that is in the context of criminological extrapolation or criminal suspect extradition.

The challenging question from a pragmatic law enforcement perspective is: If information is law- fully held within the databases of willing and socially responsible organizations that might help prevent people becoming victims of crime or bring perpetrators to justice, why would LEAs not only feel justified in accessing those data but obliged to do so?

Part of the answer is that the application of informatics within a law enforcement environment is arguably different from that of Big Data application in most other settings. There are several strands to the answer, first among which is the high level of legal regulation of this area. Yes, there are substantial and significant exceptions within most legal data frameworks to allow access by LEAs to data held by others, particularly when their principal purpose is to prevent or investigate crime or pursue the interests of national security, but they are not always that clear and seldom amount to a blank check. Before looking more closely at some of the components of the law enforcement dilemma, it is necessary to look at the broad components of the legal framework within which the pragmatic law enforcement activity takes place.

LEGAL FRAMEWORK

The legal framework regulating the Big Data challenges for law enforcement in the United Kingdom (UK) is dominated by that throughout all European Union (EU) member states. Primary law components (but by no means all) of that framework are to found in:

- The European Convention on Human Rights
- The European Charter of Fundamental Rights

- of
- The EU Data Protection Directive 95/46–8
 - The Council of Europe Convention 108¹¹—providing the main point of reference for the directive applying to data protection in policing and criminal justice
 - The Data Protection Act 1998 (based on the central principles of the Directive)
 - The Freedom of Information Act 2000, which created rights of access to information, superseding the Code of Practice on Access to Government Information and amending the Data Protection Act 1998 and the Public Records Act 1958
 - The Protection of Freedoms Act 2012, a very wide-ranging act making provision with respect to the retention and destruction of fingerprints, footwear impressions, and DNA samples and profiles taken in the course of a criminal investigation; requirements of schools and further education colleges to obtain the consent of parents of children under 18 years of age attending the school or college before the school or college can process a child’s biometric information; the further regulation of closed circuit television, automatic number plate recognition, and other surveillance camera technology operated by the police and local authorities; the need for judicial approval before local authorities can use certain data-gathering techniques; data provision with respect to parking enforcement and counter-terrorism powers.

These are supported, extended, and elaborated upon in various other instruments too numerous to list here¹² (for a guide, see [Bignami, 2007](#); [Holzacker and Luif, 2013](#)).

¹¹ Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Council of Europe Treaties 108 (01/1981).

¹² See also, for example, Framework Decision 2008/977/JHA for the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (Data Protection Framework Decision) and the Council Decision 2008/615/JHA of June 23, 2008 on the stepping up of

Article 13 of the EU Directive provides that “member states may adopt legislative measures to restrict the scope of the obligations and rights provided for in Article 6 (1)...when such a restriction constitutes a necessary measure to safeguard...national security; defence; public security; the prevention, investigation, detection and prosecution of criminal offences.” However, a qualified test must be applied to any restriction to ensure that the legislative measure meets the criteria that allow derogating from a fundamental right. There are two limbs to this test: First, the measure must be sufficiently clear and precise to be foreseeable; second, it must be necessary and proportionate, consistent with the requirements developed by the European Court of Human Rights.

HUMAN RIGHTS

Much of the legislation and jurisprudence relating to data protection across the EU derives from human rights and fundamental freedoms. Clearly, there is not the space here to review the legal and political provenance of this subject. However, it is worth pausing at this stage to note and distinguish the two “distinct but related systems to ensure the protection of fundamental and human rights in Europe” (Kokott and Sobotta, 2013). The first, the European Convention on Human Rights, is probably known and understood by law enforcement personnel in the UK better than the second. The Convention is an international agreement between the States of the Council of Europe of which all member states are part, as are external states such as Switzerland, Russia, and Turkey. Matters engaging the Convention are ultimately justiciable in the European Court of Human Rights, which has jurisdiction over actions brought by individuals against member states for alleged breaches of human rights, and a substantial body of jurisprudence has been built up around this area.

cross-border cooperation, particularly in combating terrorism and cross-border crime (the Prum Decision).

The second, less familiar system arises from the jurisprudence of the Court of Justice of the European Union (ECJ), which guarantees the protection of fundamental human rights within the EU. Respect of these rights is part of the core constitutional principles of the EU. Both systems are engaged by some activities around data capture, retention, and analysis, but a key distinction in relation to Big Data is that for most purposes, human rights protections treat the protection of personal data as a form of extension of the right to privacy.¹³ (Article 8 of the European Convention on Human Rights incorporates this in the respect for an individual's private and family life, home, and correspondence.) Article 8 prohibits interference with the right to privacy, except where such interference is in accordance with the generally applicable departures from the Convention article necessary in a democratic society.¹⁴ The EU Charter of Fundamental Rights, however, specifically enshrines data protection as a fundamental right in itself (somewhat unhelpfully under Article 8). This is distinct from the protection of respect for private and family life (Article 7). The Charter also establishes the principle of purpose limitation, requiring personal data to be processed "fairly for specified purposes" and stipulating the need for a legitimate basis for any processing of such data.

Even the EU's own legal framework for enshrining rights and freedoms for data subjects is not immune from challenge. For example, the ECJ found that the Data Retention Directive¹⁵ allowed the data retained under its aegis to be kept in a manner so as to allow the identity of the person with whom a subscriber or a registered user had communicated to be revealed as well as identify the time of the communication and the place in which that communication occurred.¹⁶ The Directive sought to ensure that data were available to prevent, investigate, detect, and prosecute serious crimes, and that providers of publicly available electronic communications services or of

¹³ For an unusual police-related case, see ECtHR June 25, 1997, *Halford v. The United Kingdom* (no. 20605/92, 1997-III).

¹⁴ See, for example, *Copland v. The United Kingdom* (no. 62617/00 Reports of Judgments and Decisions 2007-1); ECtHR January, 12, 2010, *Gillan and Quinton v. The United Kingdom* (no. 4158/05, Reports of Judgments and Decisions, 2010).

¹⁵ EU Data Retention Directive 2006/24/EC.

¹⁶ Judgment in Joined Cases C-293/12 and C-594/12 *Ireland and Seitlinger and Others*.

public communications networks were obliged to reveal the relevant data. The ECJ held that those data might permit “very precise conclusions to be drawn concerning the private lives of the persons, whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.” The ECJ also held that the retention of data might have a chilling effect on the use of electronic communication covered by the Directive on the exercise of freedom of expression guaranteed by Article 11 of the Charter of Fundamental Rights.¹⁷

Then there is the indiscriminate—or at least non-discriminating—nature of Big Data analytics. The automation of processing is not just a strength; it is almost a sine qua non of Big Data use. The dilemma for agencies tasked with the exercise of discretionary powers is that the greater the automation, the less scope arguably there is for intervention by the controlling mind and the application of discretion (which, as once described by Lord Scarman,¹⁸ is the police officer’s daily task). Much has been written and said of the use of “non fault” or “without cause” powers by the police and the absence of Scarman’s “safe-guard of reasonable suspicion” (see, e.g., [Staniforth, 2013](#)), and the general trend for law enforcement in the UK has been to move away from the blanket applications of powers.

Interference by a member state with an individual’s rights under the European Convention must be “necessary in a democratic society” and have a legitimate aim to answer a “pressing social need,” but even then an identified interference must be proportionate and remains subject to review by the Court (*Coster v. United Kingdom*, 2001; 33 EHRR 479).¹⁹ Whereas the relationship between accuracy and reliability is clearly important in any form of data analysis, when the analysis is used at the level of the individual, biometrics, demographics, and social epidemiology take on a different legal quality.

¹⁷ For a fuller explanation, see Boehm and Cole (2014).

¹⁸ Report on the Brixton Disorders, April 10–12, 1981 (Cmnd. 8247), February 4, 1984

¹⁹ See also Article 40 of the UN Convention on the Rights of the Child of 1989, which states that it is the right of every child alleged to have infringed a penal law to be treated in a manner consistent with the promotion of the child’s dignity and worth, reinforcing the respect for the child’s human rights and fundamental freedoms.

Almost by definition, Big Data deals with the supra-personal, the yotta-aggregation of data that is unconcerned with the binary constructs of personal identity and individuality. However, the Working Party puts it thus: “The type of analytics application used can lead to results that are inaccurate, discriminatory or otherwise illegitimate. In particular, an algorithm might spot a correlation, and then draw a statistical inference that is, when applied to inform marketing or other decisions, unfair and discriminatory. This may perpetuate existing prejudices and stereotypes, and aggravate the problems of social exclusion and stratification.”²⁰

Just how little information Big Data needs to pinpoint an individual can be seen in [Tene’s \(2010\)](#) graphic citing of research that has shown how “a mere three pieces of information—ZIP code, birth date, and gender—are sufficient to uniquely identify 87 per cent of the US population.”

PURPOSE LIMITATION AND FURTHER PROCESSING

Within the legal framework protecting human rights are several key and interlinking concepts. The first such concept is purpose limitation. Purpose limitation is a key legal data protection principle²¹ that appears (as discussed above) in both limbs of the European framework engaging with data protection: the Convention on Human Rights and the European Charter on Fundamental Freedoms. Through this framework the law seeks to protect data subjects (in crude shorthand, those individuals to whom the relevant data relate) by setting limits, albeit flexible, on how the data controllers (equally crudely, those who are able to manage and direct the manner in which the data are used) are able to use their data.

Purpose limitation, which has parallels in other jurisdictions (such as Article 6 of Law n. 121/1981 in Italy; see Chapter 16 for more information), has two components. First is purpose specification, which means that the collection of

¹⁵ *Loc. cit.* at p. 45.

²¹ Article 6 (1)(b) of Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, November 23, 1995, p. 31).

certain types of data such as “personal data”²² must be for a “specified, explicit, and legitimate” purpose. The second element of purpose specification is “compatible use.” This means that the data must not be further processed (see below) in a way that is incompatible with those purposes.

Arguably, the whole concept of Big Data analytics is predicated on some further perhaps even ulterior processing of data collected as a separate set or for a different, more specific purpose. The subsequent use of data represents a key barrier to lawful processing because of the requirement for compatibility. That is not to say that there can be no further processing, but such processing as there is will generally need to be compatible with the original lawful purpose or be exempt from that compatibility requirement. Even the recycling of personal data that has already been made publicly available remains subject to the relevant data protection laws.

An important aspect of the further processing issue is the nature of the relationship between the controller and the data subject; in general terms, compatibility assessments should be more stringent if the data subject has not been given sufficient—or any—freedom of choice.

Exemptions for processing personal data within the UK are widely drafted and include purposes such as the administration of justice, statutory functions, and public interest provisions, which cover the work of a whole range of public bodies. However, the number of community outcomes for which the police alone are responsible is vanishingly small and (certainly in the UK) almost every activity that keeps people safe and thriving is the product of collaborative enterprise and partnership. This level of *engrenage* is not specifically reflected by the law regarding data protection and processing. There are restrictions on data sharing, particularly when the organizations involved are in different jurisdictions. Then there are limitations on the aggregation and analysis of huge datasets generally, which can present barriers to the proper activities of LEAs and problems regarding reliability of extrapolation, interpolation, and identification. Public bodies such as police

²² Personal data in England and Wales means data relating to an identified/identifiable living individual (Data Protection Act, 1998).

forces have no general power to share data and must do so only when they are able to indicate a power (expressed or implied) that permits them to do so.²³

A key challenge of Big Data for law enforcement therefore arises from the almost total reliance on partnerships within the British neighborhood policing model, which makes sectoral and functional separation (i.e., separation into public health, education, research) all but impossible. The best one can hope for is to identify the legitimate outcomes toward which the law enforcement partnership is working, understand the key elements of the relevant data protection framework applicable to that setting, and aim for compliance.

The relevant legislative frameworks, however, presuppose a “neat dichotomy” (Tene, 2010), whereas the increasingly collaborative manner in which businesses operate precludes a neat dichotomy between controllers and processors. Many decisions involving personal data have become a joint exercise between customers and layers upon layers of service providers. With the rise of cloud computing and the proliferation of online and mobile apps, not only the identity but also the location of data controllers have become indeterminate (Tene, 2010).

This is challenging enough when the LEAs and partners are within EU member states. When non-member states are involved—as occurs in many cases particularly involving serious organized crime—there is an additional requirement of “adequacy of protection.” It is a key principle of the relevant legislation in member states that personal data must not be transferred outside the European Economic Area (EU member states and Norway, Iceland, and Lichtenstein) unless there is an ensured adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

PUBLIC TRUST AND CONFIDENCE

²³ For instance, the Ant-iTerrorism, Crime and Security Act, 2001, s. 17

Finally, and perhaps most important, there is public trust. The consensual model of policing in the UK entirely depends on the support of the communities within which the police operate. The principal factor keeping relative order on the streets of the UK is not so much the presence of 140,000 police officers; rather, it is the legitimacy (Stanko, 2011) they enjoy among the 60 million people who tolerate and support them.

Some key features of Big Data, such as behavioral targeting, have a different cachet in LEA settings, and the history of data processing within UK policing has not been without its difficulties. There have been various legal challenges to the use and retention of personal data by the police: for example, *S & Marper v. United Kingdom* (2008) ECHR 1581 (police retention of DNA samples of individuals arrested, but who are later acquitted or have the charges against them dropped, was a violation of right to privacy) and *R (on the application of GC & C) v. The Commissioner of Police of the Metropolis* (2011) UKSC 21 (successful challenge of a policy of the Association of Chief Police Officers allowing indefinite retention of biometric samples, DNA and fingerprints for an indefinite period save in exceptional circumstances).

Police monitoring of public protests has produced a series of legal challenges for which LEAs have not always managed to achieve the fine balance between the obligations of the state to ensure the security and safety of its citizens and its duty to ensure the protection of their human rights and fundamental freedoms (see *The Queen (on the application of Catt) v. The Association of Chief Police Officers of England, Wales and Northern Ireland* and *The Commissioner of Police for the Metropolis* (2013) EWCA Civ 192). The *Catt* case involved a lawful demonstration and the indefinite retention of data about the applicant on the National Domestic Extremism Database. The case shows that even where the relevant event takes place in public, the recording and retention of personal data about individuals involved can be an unlawful interference with the right to respect for private life under Article 8 of the European Convention of Human Rights.

Aside from the litigious challenges over operational retention and use of personal data, the police have also experienced the ignominy of having their official recognition removed by the Office for National Statistics because their data processing approaches for recording crime were found to be unreliable. The police found themselves the subject of a Parliamentary report called “*Caught red handed: Why we cannot count on police recorded crime statistics*,” published by the Public Administration Select Committee,²⁴ whose chair, Bernard Jenkin, MP, said in the press release accompanying the report: “Poor data integrity reflects the poor quality of leadership within the police. Their compliance with the core values of policing, including accountability, honesty and integrity, will determine whether the proper quality of Police Recorded Crime data can be restored.”²⁵ Shortcomings in data quality and reliability in the LEA context are not just about compliance and can have real and immediate detrimental impacts on and within the criminal justice process.²⁶

The Public Administration Committee’s report was followed by a report of HM Inspector of Constabulary on the reliability of crime recording data created and maintained by the police forces of England and Wales.²⁷ The interim report published on May 1, 2014, which drew upon several previous reports, referred to the Inspectorate’s “serious concerns” in the integrity of police crime recording data.

Conversely, the failings of the police in England and Wales to retain relevant data in a searchable and shareable way, so as to enable the tracking of dangerous offenders such as Ian Huntley,²⁸ were widely reported and criticized in the *Bichard Report*,²⁹ which led to wholesale changes in the police approach to operational information technology capabilities.

²⁴ Report of the Public Administration Select Committee 13th session 2013/14 HC 760, The Stationery Office, London.

²⁵ See <http://www.parliament.uk/business/committees/committees-a-z/commons-select/public-administration-select-committee/news/crime-stats-substantive/>.

²⁶ See <http://www.telegraph.co.uk/news/uknews/crime/11117598/Criminals-could-appeal-after-Home-Office-admits-potentially-misleading-DNA-evidence-presented-to-juries.html>.

²⁷ See <http://www.justiceinspectores.gov.uk/hmic/programmes/crime-data-integrity/>.

²⁸ Convicted on December 17, 2003 of the murder of 10-year-old schoolgirls Holly Wells and Jessica Chapman.

²⁹ Report of the Bichard Inquiry HC 653 June 22, 2004, The Stationery Office, London.

The corrosive effect of such cases and the media’s reporting of them can be expected to damage public trust and confidence in the police and to affect the legitimacy they need to operate. When taken against the wider international context of “data-gate” and the Snowden revelations³⁰ of how governments have been using Big Data analytics and high-tech information and communications technology monitoring capabilities, this reduced trust and confidence represents a serious impediment to even the lawful and compliant use of Big Data by LEAs in the future.

CONCLUSIONS

Although the attractions of Big Data for LEAs are immediate and obvious, so, too, are the dilemmas it creates. The benefits of a capability of the scale offered by Big Data are readily apparent in every aspect of law enforcement, particularly where technology is used by perpetrators. For example, where the proscribed activities take place within the galactic setting of social media communications, such as in radicalization activities in terrorism and the online grooming of children and vulnerable victims in sexual offending, influencing behaviors and searching out prospects, the *modus operandi* almost invites a Big Data approach to both detection and prevention.

It is one thing to get private organizations from the retail sector or business-to-business suppliers working to certain data protocols, but what about LEAs? Staples such as individual consent and the right to be forgotten become much more difficult to apply, whereas exceptions such as the investigation, detection, and prevention of crime or—even broader—the public interest are much more readily applicable.

HOW FAR SHOULD BIG DATA PRINCIPLES SUCH AS “DO NOT TRACK” AND “DO NOT COLLECT” BE APPLICABLE TO LEAS, EITHER IN QUALIFIED FORMAT OR AT ALL?

Can the developing legal framework around human rights and concepts such as privacy and identity offer sufficient protection, engender legitimacy, and

³⁰ See <http://www.theguardian.com/world/the-nsa-files>

foster public trust? At this point the proposed Data Protection Regulation (Article 6 (4)) contains a broad exception from the compatibility requirement and if enacted, will allow a great deal of latitude for the further processing of personal data including a subsequent change of contractual terms. This potentially allows a data controller not just to move the goal posts, but to wait and see where the ball lands and then erect the goal around it. How will such relaxation of the rules be viewed by citizens, and what safeguards can they legitimately expect from their states?

When it comes to Big Data, the higher the stakes, the greater the challenges for LEAs that risk being condemned for not using all available data to prevent terrorist atrocities or cyber-enabled criminality and damned if they do so to the detriment of individual rights and freedoms.

As Polonetsky and Tene (2013) put it: “The NSA revelations crystallized privacy advocates’ concerns of sleepwalking into a surveillance society’ even as decision-makers remain loath to curb government powers for fear of terrorist or cybersecurity attacks.”

One thing seems certain: The continued expansion of Big Data capability will inflate the correlative dilemmas it presents to our LEAs.

²⁵ See <http://www.theguardian.com/world/the-nsa-files>.

The resolution of the dilemmas of Big Data for LEAs—and by extension, for their partners in key areas such as safeguarding, fraud prevention, and the proper establishment of the rule of law in cyberspace—will be as much a challenge for the law as the technology. The dilemmas for LEAs are but one example of how our legal systems and principles need to catch up with the practices of their citizens’ lives. It will need a new breed, a form of *lex veneficus*,³¹ perhaps, to work alongside the technical wizards who have set the height of the Big Data bar.

³¹ Literally a *legal magician*.

REFERENCES

- Akhgar, B., 2014. Big Data and public security. *Intelligence Quarterly Journal of Advanced Analytics* 2Q, 17–19.
- Blackman, J., 2008. Omniveillance, Google, privacy in public, and the right to your digital identity: a tort for recording and disseminating an individual's image over the Internet. *Santa Clara Law Review* 49, 313–392.
- Bignami, F.E., 2007. Privacy and law enforcement in the European Union: the data retention directive. *Chicago Journal of International Law* 8, 233–255.
- Boehm, F., Cole, M.D., 2014. Data Retention after the Judgment of the Court of Justice of the European Union. (Munster/Luxembourg).
- Costanzo, P., D'Onofrio, F., Friedl, J., 2014. Big Data and the Italian legal framework: opportunities for police forces. In: Akhgar, B. (Ed.), *Big Data and National Security*. Elsevier. (To be published).
- Holzacker, R.L., Luif, P., 2013. *Freedom, Security and Justice in the European Union: Internal and External Dimensions of Increased Cooperation after the Lisbon Treaty*. Springer Science+Business Media, New York.
- Kokott, J., Sobotta, C., 2013. The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law* 3 (4), 222–228.
- Polonetsky, J., Tene, O., 2013. Privacy and Big Data: making ends meet. *Stanford Law Review* 66, 25 Online.
- Richards, N.M., King, J.H., 2013. Three Paradoxes of big data. *Stanford Law Review* 66, 41 Online.
- Stanko, B., 2011. Observations from a decade inside: policing cultures and evidence based policing. In: 5th SIPR Annual Lecture. Scottish Police College. Delivered 20 October 2011.
- Staniforth, A., 2013. In: Sampson, F. (Ed.), *The Routledge Companion to UK Counter-Terrorism*. Routledge, London.
- Tene, O., 2010. Privacy—the new generations. *International Data Privacy Law* 1–13.

Item 4

“Whatever You Say...The Case of the Boston College Tapes and How Confidentiality Agreements Cannot Put Relevant Data Beyond the Reach of Criminal Investigation.” in Policing: A Journal of Policy and Practice, Oxford University Press, 2016 Vol 10 Issue 3 pp 222-231

<https://doi.org/10.1093/police/pav034>

‘Whatever You Say...’: The Case of the Boston College Tapes and How Confidentiality Agreements Cannot Put Relevant Data Beyond the Reach of Criminal Investigation

Fraser Sampson LL.B., LL.M., MBA., Solicitor

Abstract A review of the legal issues arising in the litigation between Boston College and law enforcement agencies over data files containing evidence of terrorism in the troubles in Northern Ireland and an analysis of the wider legal principles for policing.

Introduction

The retention of data by law enforcement agencies (LEA) is a highly topical and controversial area for both practitioners and academics (Sampson, 2013). The case of the ‘Boston College Tapes’ provides a salutary lesson in how the two differing purposes— criminal investigation and criminological re- search—for the generation and storage of data files can come into conflict; and also how the use of confidentiality agreements are unlikely to be effective in putting material beyond the reach of criminal investigation.

The dilemma

While still very much a ‘live’ matter¹ the Boston College Tapes case illustrates what has been a fundamental dilemma for LEAs and citizens for decades. Recognised and summarized over 20 years ago, in a different, barely digital age, and before the challenges of data processing and protection had become a feature of the investigative landscape, the dilemma was summed up thus:

There is, first of all, a public interest in the effective investigation and prosecution of crime. Secondly, there is a public interest in protecting the personal and property rights of citizens against infringement and invasion. There is an obvious tension between these two public interests

because crime could be most effectively investigated and prosecuted if the personal and property rights of citizens could be freely overridden and total protection of the personal and property rights of citizens would make investigation and prosecution of many crimes impossible or virtually so.²

The tapes

The case of the Boston College Tapes, arising out of historical criminal investigation into the Troubles in Northern Ireland³, neatly demonstrates how, when it comes to competing interests and claims over data, the machinery of investigation is almost irresistible irrespective of any consensual efforts of the data owners and processors to put the data beyond its reach either in advance of the data being created or in the course of subsequent legal challenge. This case—and the substantial litigation that arose from it—started with a project by Boston College in Massachusetts (the so-called ‘Belfast Project’) in 2001 to create an oral history of the Troubles in Northern Ireland.³ In brief, the Belfast Project involved former paramilitaries agreeing to take part in a series of interviews during the course of which they made inculpatory admissions about their involvement in various activities to be recorded and retained.

The interviews took place under the terms of an express agreement between data processors (the researchers) and the data subjects (former terrorists) to the effect that the latter would provide candid detail of their experiences and activities confidentially and that the content of the interviews would not be disclosed until after the death of the relevant interviewee. The data files recorded during the interviews were retained in the Boston College library.

The information provided by some—such as David Ervine of the Progressive Unionist Party and Brendan Hughes, a former IRA

² R v. Lewes Crown Court ex parte Hill (1991) 93 Cr App R 60, per Bingham LJ at 65–66.

³ <http://www.bbc.co.uk/news/uk-northern-ireland-27238797>.

commander, was published after their deaths (Maloney, 2011) in accordance with the confidentiality agreement. However, the Police Service for Northern Ireland (PSNI) took the view that some of the material in the tapes was directly relevant to their ongoing criminal investigations into a number of unsolved crimes within Northern Ireland stretching back over four decades.⁴ Unsurprisingly, perhaps the PSNI attempted to obtain disclosure of the material. When this was denied, the subsequent attempts by the police to gain access to the data initiated a protracted and highly controversial stream of litigation on both sides of the Atlantic.

The litigation—USA

In the USA, the relevant judicial activity began by the issuing of a subpoena in response to a request by the UK government seeking the assistance of the American administration in securing access to the tapes.⁵

Subpoenas were issued to Boston College in May and August of 2011 by a commissioner appointed under the mutual legal assistance treaty between the USA and the UK.⁶ The subpoenas were specifically part of an investigation by the PSNI into the abduction and death of Jean McConville 1972. Mrs. McConville was thought by the Provisional IRA to have acted as an informer for the British authorities on the activities of republicans in Northern Ireland.⁷ As is not uncommon in such sensitive matters as the activities of informers (since categorized as covert human intelligence sources⁸) no evidence has been produced—then or since—to confirm this belief. However, a woman convicted of the bombing of the Central Criminal Court in London in 1973, Dolours Price, had made several public claims that the Provisional IRA had been responsible for this and

⁴ The admissibility of any material so obtained is not examined here but any application to have the material excluded is likely to face some substantial hurdles.

⁵ Case 1:11-mc-91078-RGS Re: Request from the UK Pursuant to the Treaty Between the Government of the USA and the Government of the UK on Mutual Assistance in Criminal Matters in the Matter of Dolours Price M.B.D. No. 11-MC-91078 US district court district of Massachusetts.

⁶ 18 USC § 3512 and the 'US-UK MLAT'

⁷ <http://caselaw.findlaw.com/us-1st-circuit/1605342.html#sthash.XRHGrVDt.dpuf>.

⁸ See the Regulation of Investigatory Powers Act 2000 Part II.

other abductions and murders,⁹ claims that she was believed to have made on tape to the Boston College researchers.

Because Hughes had died since his interview and the material had been made available for publication, the data held by Boston College was disclosed to the authorities on the basis that Hughes 'had no confidentiality interests at stake'. However, Boston College sought to quash¹⁰ other subpoenas relating to data provided by interviewees who were still alive. The District Court of Massachusetts denied the motions to quash¹⁰ and, after undertaking a review in camera of the subpoenaed material, it ordered production of the data.¹¹

The author of the Hughes and Irvine book, Ed Moloney together with a fellow writer/academic and former IRA prisoner, Anthony McIntyre who had been the lead researcher on the Boston project and who had conducted the interviews with Republican interviewees sought unsuccessfully to intervene in both sets of subpoenas. The applicants sought declarations that the US Attorney General's compliance with the UK's request violated the US- UK Mutual Legal Assistance Treaties (MLATs). The applicants sought injunctive relief compelling the US Attorney General to comply with the terms of that treaty. The effect of the relief sought would have been to prevent disclosure of the data sought under the subpoenas.

Having lost on intervention, Moloney and McIntyre then filed their own complaint which made largely the same claims and they too were dismissed by the District Court for the reasons it gave in its reported decision for denial of Boston College's claims.¹²

⁹ See The Daily Telegraph 2 May 2014

¹⁰ 831 F.Supp.2d 435 (D.Mass.2011)

¹² See Order of Dismissal, Moloney v. Holder, No. 11-12331 (D.Mass. 25 January 2012), ECF No. 15; Tr. of Mot. Hr'g, Moloney v. Holder, No. 11-12331 (D.Mass. 24 January 2012), ECF No. 18.

The case then proceeded to the US Court of Appeals, First Circuit.¹³ The Court of Appeals determined that both MLATs were self-executing treaties. Specifically, the Court noted that Article 1 of the US–UK MLAT provides that the parties to the agreement shall assist one another in: ... taking testimony of persons; providing documents, records, and evidence; serving documents; locating or identifying persons; transferring persons in custody for testimony or other purposes; executing requests for searches and seizures; identifying, tracing, freezing, seizing, and forfeiting the proceeds and instrumentalities of crime; and providing other assistance the parties’ representatives may agree upon.

Article 1 further states: ‘This treaty is intended solely for mutual legal assistance between the Parties. The provisions of this Treaty shall not give rise to a right on the part of any private person to obtain, suppress, or exclude any evidence, or to impede the execution of a request.’¹⁴

The Court noted that this treaty expressly prohibits the creation of private rights of action and upheld the ‘background presumption’ (that ‘[i]nternational agreements, even those directly benefitting private persons, generally do not create rights or provide for a private cause of action in domestic courts.’¹⁵ The Court noted how its own decisions and those of other courts of appeals¹⁶ have held that ‘treaties do not generally create rights that are privately enforceable in the federal courts’ and

¹³ Nos. 11–2511, 12–1159.

¹⁴ US–UK MLAT, art. 1, para 3

¹⁵ *Medellín v. Texas*, 552 US 491, 128 SCt 1346, 1357 No. 3, 170 L.Ed.2d 190 (2008) (alteration in original) (quoting 2 Restatement (Third) of Foreign Relations Law of the USA § 907 cmt. a, at 395 (1986)).

¹⁶ *United States v. Li*, 206 F.3d 56, 60 (1st Cir. 2000) (en banc); see also *Mora v. New York*, 524 F.3d 183, 201 & n. 25 (2d Cir. 2008).

reaffirming that there is a presumption that treaties do not create privately enforceable rights in the absence of express language to the contrary). This prohibition by its terms encompasses all private persons, not just criminal defendants.

Perhaps inevitably, the Court upheld the decisions of the lower courts and also held that any constitutional claims had been properly dismissed.

Interestingly, the Court also took notice of an earlier authority that the fact that disclosure of the materials sought by a subpoena in the criminal proceedings would result in the breaking of a promise of confidentiality by reporters was not by itself a legally cognizable First Amendment or common law injury.¹⁷ In *Branzburg*, the Court ‘flatly rejected any notion of a general-purpose reporter’s privilege for confidential sources, whether by virtue of the First Amendment or of a newly hewn common law privilege.’¹⁸

The litigation—UK

Following the failure of the US litigation to prevent disclosure of the data, an applicant began proceedings in Northern Ireland.¹⁹ This particular application was brought by Winston ‘Winkie’

Rea, former leader of the loyalist paramilitary organization Red Hand Commando. The applicant sought leave to apply for judicial review of a decision by the Director of Public Prosecutions (DPP) to issue an International Letter of Request (ILOR) ⁴⁰ to the Central Authority of the USA in accordance with the provisions of section 7(5) of the Crime (International Co-Operation) Act 2003 (the 2003 Act) seeking mutual assistance from the Central Authority in respect of the data held by Boston College.

His initial application for leave having failed on 9 February 2015 the applicant made a fresh application for leave to the Court of Appeal

¹⁷ *Branzburg v. Hayes*, 408 US 665, 92 SCt 2646, 33 L.Ed.2d 626 (1972).

¹⁸ *Loc cit.*

¹⁹ Rea’s (Winston Churchill) Application [2015] NICA 8.

Northern Ireland the next day seeking the assistance of the court as a matter of urgency since it had been learned that, subsequent to the hearing at first instance, officers from the PSNI had travelled to Boston for the purpose of taking possession of the relevant materials. The issue in this case was that, in⁵⁵ furtherance of an investigation into serious criminal offences, on 11 September 2014, the DPP had issued an ILOR pursuant to the Treaty between the Government of the UK of Great Britain and Northern Ireland and the Government of the USA 1996 on mutual legal assistance in criminal matters in accordance with the provisions of section 7(5) of the 2003 Act. For the purposes of that Act, the DPP is a designated prosecuting authority and it was the decision to issue that request for assistance that the applicant Rea was challenging. The applicant argued that his Article 8 rights²⁰ had been infringed and that his donation of material to the Boston College archive clearly engaged his Article 8 right to privacy. In such circumstances, to obtain access to the material the respondent would have to show that any interference was in accordance with the law and necessary in a democratic society for one of the purposes specified in Article 8.2.²¹ It had already been established that public authorities which obtained documents by compulsion engage the right to respect for the private life and correspondence in respect of each step of such measures (i.e. obtaining, storage, and subsequent use of the material).²²

After hearing detailed initial argument the Court of Appeal granted leave to the applicant in relation to the sole—and narrow—procedural ground namely:

²⁰ Art 8 of the ECHR provides the 'Right to Respect for Private and Family Life'.

²¹ National security, public safety, or the economic well-being of the country for the prevention of disorder or crime, for the protection of health or morals, or for the protection of rights and freedoms of others.

²² *Amann v. Switzerland* (2000) 30 EHRR 843 followed in *R (Hafner and Another) v. City of Westminster Magistrates' Court* [2009] 1 WLR 1005.

That on a proper interpretation of Section 7(5) of the 2003 Act there is a requirement to demonstrate the relevance of the requested material.

Perhaps this very narrow permission on what seems to be an easily provable point signalled to both the applicant and the PSNI officers in Boston the likely fate of this application. In any event, the applicant was given leave to file an amended Statement of Grounds and the respondent was given leave to file an affidavit; the application then proceeded as a rolled up hearing by way of appeal.

Again, the applicant in this case sought to rely on confidentiality and the express and limited purpose behind the data. He argued thus:

My clear understanding was that my testimony was recorded, conveyed, and deposited at the Burns Library, Boston College under the strictest conditions of confidentiality and would be retained there under the same duty of confidentiality which Boston College had promised me in return for my testimony. I gifted the contents of my recordings to Boston College for preservation and access to my testimony was to be restricted until after my death unless I provided prior written authority for their use, which authority has never been provided.²³

Giving the judgment of the Court Coughlin LJ said that:

“..even on the assumption that the issue of the ILOR may have infringed the applicant’s right to privacy we are entirely satisfied that any such interference was in accordance with law and necessary in the interests of the prevention of crime in accordance with Article 8(2) of the European Convention for the Protection of Human Rights and

²³ Applicant’s affidavit, para 5.

Fundamental Freedoms.”²⁴

Accordingly, this application failed as well.

The analysis

The UK litigation in this case is very different from previous cases involving data challenges against the police which have generally involved the creation, processing, and retention practices of enforcement bodies themselves.²⁵ In the Boston College Tapes case, the focus was the compulsion of disclosure of data files created by third parties. To that extent this was not a dispute about data access as such and the key principles could have applied equally to other material required for evidential purposes (such as items required for forensic analysis such as a fire- arm or piece of clothing). However, the growth in Big Data analytics (Akhgar et al., 2013) and the reliance of law enforcement agencies on data files such as CCTV, communications, and social media data (Bayerl, 2014) makes the Boston College Tapes case of particular importance to data specialists. The rapid expansion of social media and policing has been well documented.²⁶ The sensitivities around utilization of these data by LEAs—particularly in settings where material has originally been gathered by individuals for other purposes such as political protest (Russell, 2007; Kavanaugh et al., 2011; Papic and Noonan, 2011; Xiguang and Jing, 2010; Kotronaki and Seferiades, 2012) mean that the field of citizens’ social media data is one already prepared for battle.

It is perhaps worth noting here that the regulation of data capture, retention, and processing by LEAs is a developing area of law and has

²⁴ Loc cit.

²⁵ E.g. *S & Marper v. United Kingdom* [2008] ECHR 1581—police retention of DNA samples of individuals arrested and later acquitted or charges dropped held to be a violation of the data subject’s right to privacy); *R (on the application of GC & C) v. The Commissioner of Police of the Metropolis* [2011] UKSC 21) data subjects successfully challenged national policing policy allowing indefinite retention of biometric samples, DNA and fingerprints).

²⁶ See e.g. Casilli and Tubaro (2012); Howard et al. (2011); McSeveny and Waddington (2011); Deneff et al. (2013); Procter et al. (2013).

specific implications for law enforcement that are peculiar to the setting in which they operate (Sampson, 2015).

In more conventional data access cases applicants usually turn to the twin jurisdictional tracks of protection afforded by EU and domestic law²⁷ but in this case these did not prove sufficiently persuasive²⁸ (these instruments are elaborated upon in other detailed regulatory provisions²⁹ (Bignami, 2007; Holzacker and Luif, 2013)).

A critical—and often determinative—issue that arises in personal data disputes within EU Member States is that of purpose limitation. Purpose limitation is a core principle³⁰ in both elements of the European framework engaging with data protection: the European Convention on Human Rights and the European Charter on Fundamental Freedoms. Purpose limitation has parallels in other jurisdictions (such as Article 6 of Law no. 121/1981 in Italy; see Costanzo, D’Onofrio & Friedl) and means that certain types of data such as ‘personal data’³¹ must only be collected for a ‘specified, explicit and legitimate’ purpose (purpose specification) must not be further processed in a way that is incompatible with the specified purpose(s) (compatible use). Where personal data have been gathered for the express purpose, say, of assisting emergency service responders deal with a civil emergency such as severe weather conditions, any subsequent processing of the data for entirely different purposes—such as criminal intelligence gathering—will create a real risk for the LEA involved in that processing.

²⁷ For an analysis of the relationship between the two principal areas of jurisprudence—EU and domestic in the context of data access and journalism see *Kennedy v. The Charity Commission* [2014] UKSC 20.

²⁸ See also *Osborn v. Parole Board* [2013] UKSC 61; *R (Buckinghamshire County Council) v. Secretary of State for Transport* [2014] UKSC 3; *R v. Secretary of State for Transport ex p Factortame (No. 2)* [1991] AC 601.

²⁹ E.g. Framework Decision (2008/977/JHA) for the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (Data Protection Framework Decision) and the Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (the Prum Decision).

³⁰ Art 6(1)(b) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23 November 1995, p. 31).

³¹ Personal data in England and Wales means data relating to an identified/identifiable living individual (Data Protection Act 1998).

However, while the different and conflicting purposes of the police and the Boston College researchers was at the heart of this litigation, the usual issues around purpose limitation were not engaged.

Interestingly, an important consideration in the area of further processing is the nature of the relationship between the controller and the data subject; generally a compatibility assessment should be more stringent if the data subject has not been given sufficient—or any—freedom of choice. If the subject had expressly entered into an agreement to share or provide the data solely on the basis of a confidentiality agreement, this could be expected to have considerable weight in any later dispute about sharing that material. Not only did the purpose issue not arise in the facts of the Boston College Tapes, but also there are widely drafted exemptions for processing personal data within the UK which include purposes such as the administration of justice, statutory functions, and public interest provisions.³² The material being pursued in the Boston College Tapes case was principally for evidential purposes and one might have expected a fairly rigid test of admissibility and weight to be applied. However, the Court held in *Rea* that there was an inevitable flexibility in the whole concept of ‘evidence’. The Court held that, when speaking of ‘evidence’ in the course of a criminal investigation, the ‘permissible area of search’ must inevitably be wider than it would be once that investigation was complete and the prosecution’s concern is to prove an already investigated and ‘instituted’ offence.³³

It is worthy of note that, even where Member States are empowered to adopt legislative measures to restrict the scope of the obligations and rights of individuals to safeguard. . . national security, defence, public security, the prevention, investigation, detection, and prosecution of

³² Although, note that public bodies such as police forces have no general power to share data and must only do so where they are able to indicate a power (express or implied) that permits them to do so.

³³ per *R v. Secretary of State ex p Fininvest Spa* [1997] 1 WLR 743, at 752.

criminal offences,³⁴ a qualified test must be applied to any restriction to ensure that the legislative measure meets the criteria that allow derogation from a fundamental right. The two limbs to this test are that first, the measure must be sufficiently clear and precise to be foreseeable, and secondly, it must be necessary and proportionate, consistent with the requirements developed by the European Court of Human Rights. Even then the EU's own legal framework itself has not been immune from individual challenge. The Court of Justice of the European Union (ECJ) found that the Data Retention Directive³⁵ provided insufficient protection.³⁶ The controversial Directive sought to ensure the availability of data to prevent, investigate, detect, and prosecute [emphasis added] serious crimes. The ECJ held that, because this might permit 'very precise conclusions to be drawn concerning the private lives of [those] persons . . . such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them'. For this reason, it followed that the 'close, effective and certain regulation' was of fundamental importance to the protection of the individual.³⁷ However, the nature of the way in which the material was created in the Boston College Tapes case (i.e. voluntarily and consensually between two parties neither of which was a state agency) would have made this a difficult point to pursue in seeking to deny LEA access to relevant inculpatory material in the course of a serious criminal investigation).

Journalistic material

While the point was not argued in the Boston or Rea litigation, the issue of whether the contested material qualifies as journalistic material could well have arisen, particularly if the arguments had been more focused

³⁴ E.g. under art 13 of the EU Directive.

³⁵ EU Data Retention Directive 2006/24/EC.

³⁶ Judgment in Joined Cases C-293/12 and C-594/12 Ireland and Seitlinger and Others.

³⁷ Loc cit.

around the unexpurgated re- porting of the Troubles rather than the creation of an academic criminological archive.

Had the material been used for journalistic purposes, it would attract special statutory treatment in England and Wales ([Sampson, 2015](#)). Material created by responsible citizens qua citizens would probably not attract the protections enjoyed by journalists in the UK,³⁸ but material that they have shared with news agencies might. It is becoming increasingly common for journalists to source their material from citizens and ‘lay’ contributors—and the so-called ‘open source’ data.³⁹ Were the contested material to qualify as journalistic, the issues of compulsory disclosure to LEAs and prosecuting agencies would assume a different importance and would engage the fine balancing act required of the courts in weighing the investigative needs of the LEA against the potential impact of disclosure on the responsible reporting of highly sensitive matters of substantial public interest⁴⁰.

Conclusion

There are several generic lessons for data holders and processors to be learned from the case of the Boston College Tapes. First is that, where the data are required as evidence in the investigation of serious criminality, not only is it unlikely to be protected by any express agreement between the data owner and the data subject, but also it is arguably incapable of such protection either by a confidentiality agreement or general measures such as intellectual property rights.⁴¹

In more conventional data management settings, a key question arising from the data interface between wider contributors such as academics, researchers, even journalists, and law enforcement agencies is what [Searls \(2012\)](#) calls making the ‘customer’ a fully empowered actor in the

³⁸ See the Police & Criminal Evidence Act 1984 ss. 11 and 13.

³⁹ See e.g. Reynolds & Seeger (2012); Gillmor (2008); Greer (2010); Poell & Borra (2011); Russell (2007).

⁴⁰ R (on the application of British Sky Broadcasting Ltd.) v. The Commissioner of Police of the Metropolis [2014] UKSC 17.

⁴¹ The copyright in the material contained in the Maloney book was owned by the Boston College.

market place. But where the data are shown to be relevant in the context of the criminal investigation, the non-LEA entity or individual appears to be far from empowered; rather they are in a position where any exercisable power is entirely dependent on their exclusive and involuntary relationship with the state. Accordingly, the ability of the end user to exert any control over data that they have created within the parameters of relationships with others is vanishingly small. The nature of the investigative interaction between LEAs and citizens means that there will be circumstances where any data relationship between them arises from a form of coerced assent rather than free and informed agreement, and one that is capable of 'trumping' any other consensual relationship the citizen has established with a third party. This is a long way from the general data market principles being promoted in the context of commercial data exchange transactions such as the notion of a 'bidirectional' relationship between service provider and customer ([per Lanier, 2013](#)) or the development of an 'intention economy' (Searls *op cit*).

Secondly, when assessing the evidential nature of the contested material the courts are likely to take a wider view of the 'permissible area of search' than they would once an investigation is complete. This reduces still further the scope for argument by individual citizens or non-LEA bodies that their extant agreements limiting or preventing the sharing of data will be operative in the context of criminal investigation.

Thirdly, where the data have been shared across national jurisdictions the relevant legal instruments governing cooperation between sovereign states are highly unlikely to be treated as having created individual rights capable of private enforcement by the individual in any civil or criminal proceedings. Individuals and academic bodies facing challenge from another jurisdiction to disclose data files containing evidence of criminality under the aegis of a confidentiality agreement would do well to take specific advice on the extent to which any domestic agreement

can be overruled within either jurisdiction. To that end the trial judge in *Rea* indicated the importance of guidelines and encouraged ‘the creation and publication of appropriate guidelines for this type of application. . .’ on the basis that it might well assist designated authorities, practitioners, and individuals likely to be affected by material for investigative and prosecutorial processes can be expected to increase.

Fourthly, as LEAs increasingly try to tap into the ‘collective problem solving’ of citizens and their data,⁴² the legal and ethical questions of access to material for investigative and prosecutorial processes can be expected to increase. Public interest and policy means that, once they are able to establish relevance in the course of a criminal investigation, LEAs are very likely to have a supervening purpose that they can pray in aid over and above any limited or contingent purpose identified by the data owner/processor. Provided that purpose is not wholly speculative or fanciful, any application for disclosure made under the authority of international mutual assistance treaties will be very difficult to resist.

And finally, while the interviews in the Boston case were plainly not formal investigative interviews by an LEA for the purposes of criminal investigation, it might be wise for data collectors to highlight to participants the risks of voluntarily making inculpatory statements about criminality for whatever primary purpose they embark upon. Such a warning might operate in the same way as the criminal caution⁴³ in the UK or the *Miranda*⁴⁴ in the USA, putting the individual on notice that anything they say may be used in evidence. This evidential question has been raised in the context of a proposed ‘Commission for Information Retrieval’ put forward in the so-called Haas Report⁴⁵ aimed at

⁴² Palen (2008); Palen et al. (2009); Vieweg et al. (2008).

⁴³ Codes of Practice to the Police and Criminal Evidence Act 1984, Code C, para 10.

⁴⁴ *Miranda v. State of Arizona* 384 US 346.

⁴⁵ ‘An Agreement among the parties of the Northern Ireland Executive on Parades, Select Commemorations, and Related Protests; Flags and Emblems; and Contending with the Past.’ 31 December 2013.

encouraging former participants in unlawful activities during the Troubles to give inculpatory information about those activities and it might be that those considering doing so take careful note of the Boston College Tapes litigation.

Truth and reconciliation aspirations notwithstanding, wherever this particular data wrangle ends it will be hard for lawyers reading it not to find themselves reflecting on the line from the Seamus Heaney poem that found its way onto many murals during the Troubles in Northern Ireland—‘Whatever you say, say nothing.’

References

Akhgar, B., Saathoff, G., Arabnia, H., Hill, R., Staniforth, A., and Bayerl, P. S. (2013). *Application of Big Data for National Security: A Practitioner’s Guide to Emerging Technologies*. Waltham, MA: Elsevier.

Bayerl, P. S., Horton, K., Jacobs, G., and Akhgar, B. (2014). Who wants police on social media? *Proceedings of the 1st European Conference on Social Media*, Brighton, UK, 42–49.

Bignami, F. E. (2007). ‘Privacy and Law Enforcement in the European Union: The Data Retention Directive.’ *Chicago Journal of International Law* 8, 233–255.

Holzacker, R. L. and Luif, P. (2013). *Freedom, Security and Justice in the European Union: Internal and External Dimensions of Increased Cooperation after the Lisbon Treaty*. New York, NY: Springer Science & Business Media.

Kavanaugh, A., Yang, S., Li, L., Sheetz, S., and Fox, E. (2011). 'Microblogging in Crisis Situations: Mass Protests in Iran, Tunisia, Egypt' CHI2011, Vancouver, Canada, May 7-12 2011.

Kotronaki, L. and Seferiades, S. (2012). 'Along the Pathways of Rage: The Space-time of an Uprising.' In Seferiades, S. and Johnston, H. (eds), *Violent Protest, Contentious Politics, and the Neoliberal State*. Surrey: Ashgate, pp. 159–170.

Lanier, J. (2013). *Who Owns the Future?* NY: Simon and Schuster.

Maloney, E. (2011). *Voices from the Grave: Two Men's War in Ireland*. London: Faber and Faber.

Papic, M. and Noonan, S. (2011). 'Social Media as a Tool for Protest.' *Security Weekly*, Thursday 3rd February 2011.
<http://www.stratfor.com/weekly/20110202-social-media-tool-protest#axzz3LWjMNk4d> (accessed 10 December 2014).

Russell, A. (2007). 'Digital Communication Networks and the Journalistic Field: The 2005 French Riots.' *Critical Studies in Media Communication* 24, 285–302,.

Sampson, F. (2013). 'Big Data-Big Dilemmas: The Legal Challenges of Big Data Analytics / Big Data Application in Law Enforcement.' In Akhgar, B., Saathoff, G., Arabnia, H., Hill, R., Staniforth, A., and Bayerl, P. S. (eds), *Application of Big Data for National Security: A Practitioner's Guide to Emerging Technologies*. Waltham, MA: Elsevier.

Sampson, F.(2015). Cybercrime presentation Project Courage and CAMINO Cyber Security Workshop, Montpellier, France, 9 April.

Searls, D. (2012). *The Intention Economy: When Customers Take Charge*. Cambridge, MA: Harvard University Press.

Xiguang, L. and Jing, W. (2010). 'Web-based Public Diplomacy: The Role of Social Media in the Iranian and Xinjiang Riots.' *The Journal of International Communication* 16, 7-22.

Item 5

"Intelligent Evidence: Using Open Source Intelligence (OSINT) in Criminal Proceedings"
in *The Police Journal: Theory, Practice and Principles* 2016 pp 1-15

Sage Publications

<https://doi.org/10.1177/0032258X16671031>

Article

Intelligent evidence: Using open source intelligence (OSINT) in criminal proceedings

Fraser Sampson

The Police Journal: Theory, Practice and Principles 1–15 a The Author(s) 2016 Reprints and permission: sagepub.co.uk/journalsPermissions.nav DOI: 10.1177/0032258X16671031 px.sagepub.com

Chief Executive & Solicitor, Office of the Police & Crime Commissioner,
West Yorkshire, Wakefield, UK

Abstract

Law Enforcement Agencies (LEAs) are coming to terms with the potency of social media and Internet-based communication, not solely as an extension of mass communication but as a phenomenological source of intelligence. One feature of the expansion of material – particularly that which is openly available to investigators – is the narrowing of traditional boundaries between information to support lines of activity (intelligence) and material to be relied on during a criminal trial (evidence). This article addresses the legal considerations facing LEAs when this concatenation of two different categories of material occurs and matters of how to reconcile them.

Keywords

OSINT, evidence, social media, intelligence

Introduction

Law Enforcement Agencies (LEAs) around the world are rapidly coming to terms with the potency of social media and Internet-based communication, not solely as an extension of their own mass communication (Bruns and Burgess, 2012; Coptich and Fox, 2010; Crump, 2011) but as a phenomenological source of intelligence that for centuries has been the lifeblood of criminal investigation. One feature of the truly exponential expansion of accessible material – particularly that material which is openly available to investigators (Akhgar et al., 2015; Staniforth and Akhgar, 2015) – appears to be the narrowing of the

traditional boundaries between information to support lines of inquiry and activity (intelligence) and material to be deployed and relied on

Corresponding author:

Fraser Sampson, Office of the Police & Crime Commissioner, West Yorkshire, Ploughland House, George St, Wakefield WF1 1DL, UK.

Email: fraser_ospre@hotmail.com

during a criminal trial (evidence). The question that this article addresses is: what are the legal considerations facing LEAs when this concatenation of two very different categories of material occurs and how might they be reconciled?

What is OSINT?

The concept of open source intelligence (OSINT) is relatively new for LEAs and is loosely defined as intelligence collected from publicly available sources that does not require covert or clandestine methods of collection (Brunet and Claudon, 2015; Price, 2011). The potential of so-called 'Big Data' and the analytical tools being developed alongside it is, for LEAs, phenomenal (Armstrong et al., 2013; Blackman, 2008).

Principal among the many accessible 'open sources' used by LEAs are the Internet and the more popular elements of 'social media'. There is not space here to rehearse even the fundamental elements of this area of data processing but for the purposes of illustration in this article it suffices to adopt Kaplan and Haenlein's (2010) main varieties of social media:

1. collaborative projects (e.g. Wikipedia);
2. blogs and microblogs (e.g. Twitter);
3. content communities (e.g. YouTube);
4. social networking sites (e.g. Facebook);
5. virtual game worlds (e.g. World of Warcraft); and
6. virtual social worlds (e.g. Second Life).

Of these, the sources at 2, 3 and 4 have particular relevance in terms of both their intelligence value and their evidential potential for criminal trials. In addition, the Big Data capability of LEAs to access data showing, for example, the location of a device when a photograph was taken or a text sent (Lin, 1998; Seretan et al., 2003; Smadja, 1993) or the temporary and evanescent existence of a digital 'community coalescing around a one-off event such as a political rally or pop concert (Beguirisse-D'iaz et

al., 2014) opens up a source of potential evidence that was almost unimaginable at the time most of our laws of evidence were formulated. This article focuses on the law and procedure in England and Wales but, while each jurisdiction will be governed by its own domestic laws, there are nevertheless some common elements around evidence; there are also some significant overarching provisions within the European Convention on Human Rights (ECHR)¹ that will apply to relevant proceedings in each of the 47 signatory States.² In the discussion that follows, the generic principles of evidence and the jurisdiction-specific aspects are considered along with some examples to illustrate the evidential and procedural issues and the likely approach of the courts.

OSINT as evidence

Consider the following scenario. A teenage girl makes a complaint to the police that she has been raped by a friend. Investigators trawling OSINT sources find entries on the suspect's Facebook wall posted by the complainant (Kaplan and Haenlein's (2010) fourth variety of social media). Others in their respective Facebook groups can see these messages, some of which appear to show that the complainant had previously expressed a liking for the friend and were posted around Valentine's Day. There are no replies from him.

The suspect – a 15-year-old boy – is arrested and subsequently charged with rape. Investigators also find a photo of the complainant in her underwear saved on the suspect's Facebook account. Which if any of the OSINT material will be admissible as evidence at trial? The answer, of course, depends on a number of variables including which party wishes to rely on it and for what purpose(s). Before highlighting those variables and assessing how they might be applied by a court, it is necessary to take a brief look at some basic evidential principles.

Intelligence and evidence are, if not mutually exclusive, then at least substantively and purposively different. Open Source Intelligence may be

gathered for a variety of purposes, including tracing a suspect, locating a vulnerable missing person or preventing a planned crime. While LEAs will gather intelligence from a wide variety of sources, open and closed, there is no requirement – or often even a likelihood – that the product will be adduced in criminal proceedings.³ If and when it is, the use of such material as evidence will be open to challenge.⁴

So, can intelligence ever be relied on as evidence? The answer is simple: yes, provided the intelligence meets the relevant requirements for evidence of that type. Aside from the very specific statutory exclusions, such as the intercept intelligence referred to above, there is no specific reason why intelligence material ought not to be adduced as evidence. There are however further considerations that need to be addressed by investigators before relying on such material.

Principles of evidence

In mature legal systems with a developed observance of the rule of law, the rules of evidence themselves form a substantial body of jurisprudence. Wherever the jurisdiction, legal proceedings properly conducted will essentially involve the presentation of evidence by the respective parties, either tending to support their case and/or undermine that of the other(s) during the course of a fair (and usually public) hearing. And it is the fairness of the proceedings during which that evidence is presented (or prevented) that is often at the heart of decisions – and appeals – about the evidence. A defendant in criminal proceedings in democratically developed jurisdictions will generally enjoy a right to a fair hearing and certain basic entitlements. These would include the right to confront or challenge any witnesses giving evidence against him or her⁵ together with some form of qualified protection against self-incrimination.⁶

In criminal prosecutions the proceedings include the State who will prefer the charge(s) against an accused. The subsequent testing of the evidence relied upon by the parties against the charge(s) will call for decisions to be taken on the facts in issue. We will revisit this concept

with some worked examples below, after considering some other key features of evidence.

Facts in issue, admissibility and weight

In very broad terms two principal questions arise with any material that is going to be used as evidence: admissibility and weight. Plainly not all potential evidence is admissible,⁷ not all admissible evidence will be admitted in the hearing and not all admitted evidence carries the same weight. This is not as complicated as it might appear and the following illustrations help to clarify the concepts.

In order to be admissible, evidence must be relevant to a fact in issue. The burden of demonstrating relevance generally falls on the party seeking to rely on it. This can often be agreed in advance by the parties but will sometimes require a specific ruling by the judge or tribunal. 'Relevant evidence' is essentially material which makes the matter requiring proof more or less probable (see, for example, *DPP v Kilbourne* [1973] AC 729). If a fact is not in issue (for example, the consent of a complainant in a sexual offence) evidence of it is irrelevant and is highly unlikely to be admissible at all (see, for example, *R v Blastland* [1986] AC 41).

Therefore if an investigator intends to rely on any evidence – whether intelligence or otherwise – they will need to identify its 'materiality', that is the material must have some aetiological connection to a fact in issue. This could be the defendant's motive, the alleged actions of a witness or the provenance of a document, etc. The need to demonstrate materiality is particularly prominent in criminal matters where it is not unusual to have 'trials within trials',⁸ which involve the presentation of argument in the absence of a jury to obtain a specific legal ruling by the trial judge on whether a particular piece of evidence can be admitted. The facts in issue in a criminal trial will be established by the ingredients of the offence(s) with which the defendant is charged and their defence to those charges. Some evidence will be directly probative of the facts in issue (such as the defendant's state of mind in an offence requiring dishonesty) while other

evidence may be circumstantial, that is, evidence of relevant facts from which the existence of matters in issue may properly be inferred. For example, in a murder trial, the fact that the defendant delivered a kick to the victim's head may be a fact in issue; similarly any preceding demonstrations of enmity from the defendant towards the deceased may also be key to questions of motive and likelihood that the assailant was the defendant. Matters of identification or alibi may also be facts in issue and all of these can be particularly relevant where social media data are available.

Once evidence has been determined to be admissible, the finder of fact (a jury if there is one, judge/tribunal if not) will have to decide how persuasive it is. Just because it is relevant does not mean it will be determinative of the whole case. If, for example, the evidence comes from an unreliable source or if the witness providing it is less than convincing, these will clearly affect the weight to be ascribed to it. Before moving on to consider our example, it is necessary to consider a further key principle: that of purpose.

Purpose

If a party wishes to adduce evidence it will need to be for a clear relevant purpose. It is not unusual for the scope of evidence to be quite narrow. For example, in both England and Wales and the United States, a statement made in the presence and hearing of the accused before they were arrested has historically been admissible, not as evidence of the truth of the statement itself but as evidence of their reaction to it.⁹ This 'purposive' approach to items of evidence is critical in understanding the uses to which OSINT material may be put and the limitations or conditions that a court/tribunal may impose before it is admitted. Evidence might be admissible for more than one purpose. In the hypothetical murder case referred to above, a recording made by a witness on their mobile phone and posted on YouTube may, for example, be put forward for the purposes of proving both the identity of the

defendant and the fact that they kicked the victim – and perhaps that they did so more than once and that there was no other person immediately present. Alternatively, social media data may be adduced by a defendant to support evidence of alibi.

For some criminal offences (such as the making of threats or insulting comments,¹⁰ or fraud) the ‘open source’ material such as Twitter (Kaplan and Haenlein’s (2010) second variety of social media) may itself be prima facie evidence of the offence; the purpose in admitting the material would be to prove the ingredients of that offence. In a trial for assault one fact in issue might be whether the defendant had had any prior communication with a victim and either the prosecution or the defence may want to rely on social media (such as Facebook entries or Twitter exchanges) for the purpose of proving/disproving that fact in issue. Other foreseeable circumstances might include cases where the prosecution want to rely on social media entries made by a defendant to show the defendant’s mannerisms, style of writing or other idiosyncrasy (Ormerod, 2016). Alternatively the defence may wish to rely on OSINT to prove, for example in a homicide, that someone else had been present at the time¹¹ and that they had the same motive as the defendant. In sum, if investigators intend to rely on any OSINT material as evidence it is important for them to be very clear about its relevance, intended purpose, how it relates to any facts in issue in the case and what weight can fairly be given to it. And the concept of fairness is central to an understanding of the procedural issues that will arise. Here is why.

Fairness, disclosure and a word about hearsay

In those countries that are signatories to the ECHR, the admissibility of evidence is primarily a matter for regulation under national law;¹² however Article 6(1) requires that the prosecution authorities disclose to the defence all material evidence in their possession for or against the accused.¹³ This duty of disclosure (often strengthened by domestic legislation such as the Criminal Procedure and Investigations Act 1996 in

England and Wales) is an important element in the evidential use of OSINT and while the rules of evidence can differ significantly between common law jurisdictions (such as the UK) and 'civil law' jurisdictions (such as those countries whose legal systems evolved from the Napoleonic Code)¹⁴ the overriding requirements of a fair hearing will usually impose an irreducible minimum level of disclosure. Both fairness and disclosure will need to be considered if OSINT is to be relied upon in criminal proceedings.

Many, if not all, jurisdictions will also have specific rules about so-called hearsay evidence and its admissibility. The definition used in England and Wales is that hearsay evidence is 'a statement not made in oral evidence in the proceedings that is evidence of any matter stated'.¹⁵ While this definition is jurisdiction-specific, the principle is followed in other jurisdictions, such as the USA, Canada and Australia.

The rules against admitting hearsay evidence in criminal proceedings have been substantially relaxed in England and Wales¹⁶ and there are a number of statutory 'gateways' through which hearsay evidence may be introduced. In a case before the Court of Appeal¹⁷ the elements of a hearsay statement were summarised as:

any representation of fact or opinion made by a person by whatever means; [including] a representation made in a sketch, photofit or other pictorial form, [;if] the purpose, or one of the purposes, of the person making the statement appears to the court to have been—

1. (a) to cause another person to believe the matter, or
2. (b) to cause another person to act . . . on the basis that the matter is as stated.¹⁸

It can be seen immediately that documents obtained from open sources tendered in evidence as proof of any matter stated within them will generally meet this definition and the proposed use of OSINT material arguments as evidence in criminal trials can be expected to generate argument about hearsay admissibility. In an OSINT context the rules of

hearsay in England and Wales can be seen in two cases where text messages on a phone were relied upon as both admissible hearsay (R v Leonard [2009] EWCA Crim 1251) and non-hearsay material (R v Twist [2011] EWCA Crim 1143). There is neither space nor scope here for a trans-jurisdictional comparative analysis of the rules of hearsay. Suffice it to say that each jurisdiction will have its own rules for the admissibility of hearsay evidence, which, it should be remembered, is not solely a matter for the prosecution.¹⁹ Any admissibility considerations surrounding OSINT material should be approached by reference to the statutory language and provisions and with the express view of the prosecutor.

Applying the evidential principles

Returning to our working example of the teenage girl making a complaint of rape by a friend. Essentially the hypothetical facts in the question are the same as those arising in a prosecution involving an allegation of rape of a 13-year-old girl by a boy known to her.²⁰ There was – perhaps inevitably given the ages of the parties – an amount of open source information available to the prosecution and the defence. In particular, the defendant wanted to put the Facebook messages before the jury; he also wanted to show a photograph of the girl that the defendant said she emailed to him. In his defence statement²¹ the defendant denied that he had ever had sexual intercourse with the girl. The defence also sought²² to adduce evidence of a previous complaint by the girl in relation to a different incident but there was no reference to matters subsequently raised at trial. After the girl's evidence via video interview, the defence sought leave to introduce in cross-examination the photograph that the defendant alleged she had sent to him around about Valentine's Day in 2010. The photograph had been taken by the complainant and showed a 'selfie' image in a mirror of her dressed in a bikini or underwear and described as being 'quite graphic'. The principal questions here in relying on the material as described above will be that of relevance, purpose and weight. In T the defence sought to introduce

the photograph in order to prove motive for the complainant's making of a false complaint of rape against the defendant. However no emails enclosing the photograph were produced. The defence also sought to introduce a number of Facebook messages that they alleged had passed between the girl and the defendant. The first message had been sent some 18 months before the alleged incident and recorded that the girl had added the defendant as a 'friend' on Facebook. There followed a number of 'chat' messages on Facebook but none was shown to have had any response from the defendant and all showed communication in one direction.

On hearing the defendant's appeal against conviction the Court of Appeal said that, in the absence of any evidence of an email accompanying the photograph, the prosecution had been rightly sceptical as to its provenance as it could so easily have been obtained by means other than a direct email posting to the defendant (emphasis added). The question of provenance of OSINT materials – where, when and how they were created, by whom, for what purpose, who knew about them, how easily they might have been altered and so on – will be crucial to a determination of their admissibility and weight. There had been no explanation as to why the photograph had been adduced so late or as to why there had been no reference in the defence statement to a hostile motive or to the factual basis upon which such a motive was to be alleged.

Moving on to the specific relevance of the social media material, the question was whether the photograph had gone to a fact in issue. As the defendant denied that he had had sexual intercourse at all with the complainant, consent at the time was not in issue²³ (and the material had no relevance to it in any event). However, the material could potentially have gone to the issue of whether the complainant had been 'interested' in the defendant. This very much was a fact in issue and the defendant had claimed not to have been 'interested' in the complainant at all. His defence was that her motive for making a false allegation had been her

affront at his lack of interest. The court held that, once that relevance had been established, the judge should have allowed the matter to be put to the complainant and the defendant to give evidence about it.²⁴ The court also held that the material being raised so late in the day went to the weight to be attached to the photograph rather than its admissibility, illustrating neatly how the various elements of evidence summarised above can come together in criminal proceedings involving

OSINT material.

The court held that the fact that the complainant denied having sent the photograph to the defendant had not resolved the issue and that the court should have heard from the defendant too. He had wanted to say that he had been sent that photograph by the complainant and that was a conflict of testimony that the jury would have had to resolve. If, as was believed by the court, the photograph and questions about it related to a relevant issue [emphasis added], then it had not been open to the judge to refuse to allow it merely because the complainant said that she had not sent it. Once it had been established that the photograph and questions about it related to a fact in issue – namely a motive for lying – then the judge should have allowed the defence to cross-examine about the photograph and adduce evidence about it.

The court went on to point out how easily the photograph might have been obtained from another source, particularly bearing in mind the defendant's explanation for the late disclosure of the photograph and the Facebook entries: some defect in the hard drive of the computer used by him. On that matter, the court held that further evidence and consideration had been required. Again this illustrates a crucial practical area for those gathering OSINT material if it is to be relied on as evidence in legal proceedings.

To summarise, this case illustrates the key evidential considerations of the OSINT material, namely: where it came from, who made it, the purposes for which the party wished to rely on it, the fairness of allowing

them to do so, its relevance/materiality to any fact in issue (including those raised in the defence) and the context in which it should be considered, the reliability of the witnesses, the weight to be attached to any evidence once admitted and the technical functioning of the computer on which some of the material had been processed. All in all this represents a pretty comprehensive illustration of the issues discussed above.

Some practical guidance

Although they relate specifically to hearsay evidence (as discussed above) the Crown Prosecution Service guidelines are instructive in underscoring some of the wider evidential considerations that will concern a court when faced with OSINT materials. These have been adapted for the purposes of the discussion here and investigators should ask themselves:

- How much probative value does the material have in relation to a matter in issue, or how valuable it is to an understanding of other evidence in the case?
- What other evidence has been, or can be, given on the matter or evidence mentioned above?
- How important is the matter or evidence mentioned in the context of the case as a whole?
- How difficult will it be to challenge the material?
- To what extent is that difficulty likely to prejudice the party facing it?
- How reliable does the maker appear to be?
- How reliable does the evidence of the making of the material appear to be?
- In what circumstances was the material made or obtained?

The last three points will affect the weight attributed to any evidence and some- times its admissibility generally. Whether it be a percipient witness, an admission by a defendant, a document, a photograph,

scientific data or a social media feed, the provenance of material relied upon and the integrity of the process by which it has reached the court will be highly significant – and often determinative – of the material’s admissibility and weight. The greater the likelihood that the material might have been easily altered or interfered with, the less likely it is to have any substantial weight attributed to it. Similarly, where information is orphaned, anonymous or has no individual willing to testify to its provenance, the less helpful it will be to a court or tribunal in testing the facts of a case and arguably the less fair it would be to admit it against one party. Having considered the evidential principles, applied them to a specific set of facts and adapted some published guidance for prosecutors, we can move to consider another set of circumstances.

Applying the principles again

Following a fatal shooting in a suspected gang-related attack, a police officer conducts an Internet search and finds a number of photographs of a suspect on a BEBO page. The suspect (who had been arrested very near the scene some 10 minutes after the attack) appears to have taken the pictures of himself after he had left prison fairly recently and they have been digitally placed on the page in a way that suggest he is bragging as a member of the relevant gang, members of which engage in serious criminal violence. He is referred to in the material by his ‘street name’ Hustla and there are a few pieces of text about his coming out of prison. The BEBO page includes a hypertext link to a YouTube page portraying the gang as violent, although there is no picture of the suspect on the YouTube page.

What evidential use can be made of this OSINT material in the subsequent criminal proceedings against the suspect for assisting in the murder?

These were some of the evidential issues that arose in another English case²⁵ and again they are helpful in understanding how courts will approach some of the evidential challenges of relying on OSINT material in criminal trials. In this case the defendant said he had taken the

photographs of himself after he had left prison. Someone had placed the photographs on BEBO portraying him as belonging to the 'OC gang', the members of which engaged in serious criminal violence. The material referred to the defendant as 'Hustla' and associated him with the text 'Soon touch road' and the digit '3'. Although the prosecution had no evidence of the IP address from which the material had been uploaded, the entirety of the BEBO material (comprising some 46 separate 'pages') was copied for the jury, including a hypertext link to a YouTube page portraying the 'OC gang' as violent. There had been no picture of the defendant on the YouTube page but it had been downloaded and saved onto a DVD and shown to the jury.

The trial judge ruled on the admissibility of the material and directed the jury about (inter alia) its weight. The judge considered the relevant law²⁶ allowing the exclusion of evidence. Following his conviction the defendant appealed on the basis of both the ruling that evidence from the BEBO 'page' and the YouTube 'page' had been admissible and concerns about the judge's direction to the jury about that material. The Court of Appeal held that the material had been inadmissible and that the judge's direction had not cured the problems that arose from admitting it.

In the ruling on the BEBO material, the judge had said that, if the defendant had been the author of all or some of the material on that website then it was plainly admissible. If, however, the jury concluded that the defendant may not have been involved in the compilation of that website, they had still been entitled to receive that evidence as part of the general background to the case [emphasis added].

The defendant had denied any involvement in, or knowledge of, the material, both on the voir dire and in his evidence before the jury. In his testimony he had said that he did not feature in the YouTube video and had not been involved in the making of it. The BEBO material had not come from his website and he had not been involved in its creation. The defendant asserted that he had not known of the website before his arrest, he had not accessed it and had not had a password to access it. In

fact the first time the defendant had been aware of the material had been when it appeared in the paperwork of the prosecution. The photographs had shown him at his grandmother's house and had been taken shortly after his release from prison several years earlier. He had taken them with his cousin's telephone. No one else had been involved in taking them and he had explained that the word '3' meant 'free' from prison, while 'Soon touch road' meant that he would soon be coming home. He had testified that he spelled his street name 'Hustlar' with an 'AR', not as appeared in the material, and he had taken the jury through other initials that appeared on the website. He claimed he had not been responsible for what appeared on the website.

The defendant's lawyers also argued that both the BEBO and YouTube material were hearsay evidence and could not be admitted otherwise than through one of the statutory 'gateways' (as discussed above). The court held that it seemed likely that the account holder was representing as fact or opinion that the defendant was at the time a member of the OC gang. In order for the material to be admissible the judge had to be satisfied that it was in the interests of justice to admit it. Similar considerations applied to the YouTube page and there were several technical submissions about the manner in which the judge had approached the issue of admissibility.

The court held that, given that the central fact in issue in the case had been whether the defendant had been innocently at the scene of the shooting, the BEBO material was potentially very damaging to his case. The court went on to say that, among other things, the judge had to consider how reliable the maker of the statement had been but had not identified the maker of the material. Without having an identification of the maker of the material it was unclear how many different levels of hearsay had been involved.

The trial judge had not considered the reliability of the maker of the statement that the appellant was a member of the OC gang, and the court cited a previous authority:²⁷

. . . If it appears to the judge that the maker of the statement is unreliable that is a powerful indication that the statement should not be admitted in the interests of justice. The court held that, on the facts of the case, the judge should have considered how reliable the statement had been, that he should also have asked whether the prosecution could have called the maker of the statement and, if not, why not. There were also obiter remarks about whether claims ('bragging') could amount to evidence of confession (which would attract its own specific rules for exclusion.)²⁸

While much of this case turned on the specific application of the relevant statutory provisions of the hearsay laws in England and Wales and on the judge's directions to the jury, the approach of the Court of Appeal helps to illustrate further the evidential considerations of OSINT material used in criminal proceedings, mainly around relevance to a fact in issue, purpose, reliability and the issue of fairness.

Before leaving the principles of evidence, there is one final elemental consideration for LEAs when relying on intelligence and that is the manner in which it has been obtained.

Obtaining evidence, illegality and breach of process

A core issue regarding the admissibility of material obtained by an LEA in a prosecution will be the means by which it has been obtained. As has been seen, there is a general principle of evidence that the interests of justice are paramount: if it would be 'gravely prejudicial' to the defendant to admit the material then, even though technically admissible, that evidence may be excluded.²⁹ In some cases (for instance where evidence has been obtained as a result of a violation of Article 3 ECHR – the prohibition against torture, or inhuman or degrading treatment) the violation will render the proceedings as a whole automatically unfair.³⁰ If the material relied upon has been obtained unlawfully by the LEA then

there are substantial and significant barriers to its being deployed in proceedings, particularly in criminal trials. The definition and parameters of what amounts to the 'unlawful' obtaining of material are themselves often the source of considerable dispute and have arisen many times in cases where the material in question has been obtained in breach of a defendant's rights under Article 8 of the European Convention on Human Rights (ECHR).³¹ If, for example, the LEA obtained OSINT containing personal data in breach of the appropriate statutory procedure for doing so, the breach allows the admissibility of the material to be challenged (for example as a potential breach of Article 8 of the ECHR – *Perry v UK* (2004) 39 EHRR 76.)

The key element here is the fair administration of justice which, in the view of the European Court of Human Rights, 'holds so prominent a place in a democratic society...it cannot be sacrificed for the sake of expedience', and the actions of LEAs in gathering evidence must not, for example, amount to encouragement or incitement of offences.³² Even where other jurisdictions are involved in the proceedings, if there has been a deliberate breach of official process by the LEA, there is a substantial risk of the evidence being excluded.³³ Examples of this area of exclusion include cases where an undercover police informant encourages or induces the defendant to commit an offence and provides him or her with the means to do so,³⁴ and it makes no difference whether that encouragement or inducement takes place via the use of social media. While an LEA can present a defendant with an unexceptional opportunity to break the law of which s/he freely takes advantage,³⁵ great care will need to be taken by LEAs engaging in online or social media exchanges with potential suspects if the material is to be relied on in subsequent proceedings against them. Law Enforcement Agencies must not incite, instigate, persuade or pressurise the defendant into an offence.³⁶ Intelligence gathering that involves trickery, deception or oppression will be liable to exclusion if the product of it is going to be relied on as evidence.³⁷ Investigators must also be careful to avoid breaching statutory regulations protecting communications³⁸ and

committing specific offences relating to communications and data³⁹ during the course of their investigation. However, some material obtained by non-LEA personnel – such as covert filming⁴⁰ and material created by investigative journalists⁴¹ or even complainants⁴² – may be admissible. The methods used to capture OSINT will therefore need careful consideration and documentation (Liberty, 2011) and practices such as ‘mass data capture’ tactics (such as the use of web crawler software) may render the material open to challenge. Infringements (such as unlawful surveillance and interference with a defendant’s communications) may also amount to a breach of Article 8 ECHR, the entitlement to a private life.⁴³

Finally, if the OSINT material has been used for journalistic purposes (as is not uncommon (see, for example, Poell and Borra, 2011; Russell, 2007)) it may attract special statutory treatment. While material created by citizens acting alone in that capacity would probably not be protected by the usual statutory provisions enjoyed in England and Wales by journalists⁴⁴ and is unlikely to abide by the strictures of journalists’ rules for gathering and contributing material⁴⁵, material that has been provided to journalists might. If so, the issues of compulsory disclosure to LEAs and prosecuting agencies become highly sensitive and are likely to involve questions of the journalist’s substantive rights.⁴⁶

Conclusion

Intelligence has a different function and purpose from evidence. Both function and purpose can dictate how the intelligence is gathered, recorded and utilised. While overlapping, concepts such as ‘reliability’ are also different in the different context of investigation and prosecution. The ‘end user’ of intelligence is generally the LEA itself while the recipient of evidence is a court or tribunal. If intelligence is to be relied on in any form of legal proceedings it will need to meet the same requirements that the court or tribunal will demand of evidence in any other form. To improve the prospect of OSINT being admissible and

admitted in criminal proceedings the intelligence gatherer should ask themselves: what fact(s) will the material be used to prove? How far is it capable of proving that? Who was the 'maker' of the material, in what circumstances did they create the material and for what purpose? How reliable is the maker of the material and how reliable would evidence of any necessary supporting statement from them be? How does the material connect the defendant(s) with a key fact in issue? What contrary open- source evidence is available to the defendant and how will it be dealt with? How did the LEA come by the material and what processes did they use to get it? The earlier the gatherer can address the question of likely evidential use the better the prospects of identifying and remedying weaknesses and finding alternatives, although it is recognised that, until an indictment is presented and a defence position put forward to the court, it will be difficult to know what some of the fact-specific issues of that particular prosecution will be. However, LEAs should at least consider the issues from the perspective of a court and at least ask themselves questions about the basic fairness of admitting the particular material in evidence, questions such as how difficult it may be to challenge the OSINT and the extent to which that difficulty might prejudice the fairness of the proceedings against the party facing it.

In a world that relies so unquestioningly on information gathered from open sources it is all too easy to assume that such information will be accepted in every setting, including formal legal proceedings. While some open sources of information are clearly more dependable than others, the evidential gateways for courts and tribunals are well established and jealously guarded – failure to consider them may prove fatal to a prosecution or related proceedings.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship and/or publication of this article.

Notes

1. Unaffected by the result of the recent referendum on Great Britain's continued membership of the European Union.
2. <http://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/chartSignature/3> (accessed 15 April 2016).
3. In the case of covert intelligence obtained via an interception warrant in the UK, not only is its use in proceedings proscribed by law, but revealing its existence can amount to a criminal offence: Regulation of Investigatory Powers Act 2000, s.19. See also *The Use of Intercept Evidence in Terrorism Cases*, 24 November 2011 House of Commons Library SN/HA/5249.
4. See, for example, *Texeira v Portugal* (application 44/1997/828/1034).
5. See, for example, Art. 6(1) ECHR.
6. *Funke v France*, 44/1997/828/1034; see also *O'Halloran and Francis v the United Kingdom* [2007] ECHR 545 – the application of Art. 6 in the context of a right against self-incrimination will depend on the circumstance of each case; *Saunders v the United Kingdom* [1997] 23 EHRR 313.
7. Despite recent evolution in the rules permitting, for example, hearsay evidence, as seen in the courts of England and Wales.
8. In England and Wales these are referred to as *voire dire*.
9. See dicta in *R v Hayter* [2005] UKHL 6 at 28; also *Gaynor* (1957–1958).
10. See, for example, www.theguardian.com/uk/2012/may/22/muamba-twitter-abuse-student-sorry (accessed 16 April 2016).
11. In a case with facts similar to *R v Greenwood* [2005] 1 Cr App R 99.
12. *Schenk v Switzerland* [1988] ECHR 17; *Heglas v the Czech Republic* [2007] ECHR 5564.
13. *Rowe and Davis v the United Kingdom* [2000] ECHR 91.
14. See *Law Society Gazette* 11 April 2016: 13–15.
15. For England and Wales per *Criminal Justice Act 2003*, s. 114(1).
16. Principally by the *Criminal Justice Act 2003*.
17. *Bucknor v R* [2010] EWCA Crim 1152.
18. Per the *Criminal Justice Act 2003*, s. 115.
19. *Thomas v United Kingdom* [2014] ECHR 1195.
20. *T v R* [2012] EWCA Crim 2358.
21. A mandatory document in which defendants must set out the basis of their defence to the indictment brought by the Crown – see *Criminal Procedure and Investigations Act 1996*, ss 5– 6; *Criminal Procedure and Investigations Act 1996* (Defence Disclosure Time Limits) Regulations 2011; *Criminal Procedure Rules*, rule 22.4.
22. Pursuant to *Youth Justice and Criminal Evidence Act 1999*, s. 41.
23. A principal element of the offence of rape (*Sexual Offences Act 2003*, ss. 1, 74).
24. Following *R v F* [2005] Cr App R 13.

25. Bucknor, above n. 17.
26. Police and Criminal Evidence Act 1984, s. 78, the general statutory provision allowing the exclusion of evidence in criminal proceedings.
27. R v Musone [2007] EWCA Crim 1237.
28. Police and Criminal Evidence Act 1986, s. 176.
29. See Noor-Mohamed v R [1949] AC 182.
30. El Haski v Belgium (Application no. 649/08) Ga'fgen v Germany [2010] ECHR 759.
31. For a detailed analysis of the relevant law relating to EU member states, see 'Opinion on the status of illegally obtained evidence in criminal procedures in the Member States of the European Union' 30 Nov 2003. Reference: CFR-CDF.opinion3-2003.
32. Khudobin v Russia (application no. 59696/00); Teixeira v Portugal (application 44/1997/828/1034).
33. See R v Quinn [1990] Crim LR 58.
34. Khudobin, above n. 32.
35. Nottingham City Council v Amin [2000] 2 All ER 946.
36. R v Loosely [2001] 4 All ER 897.
37. See e.g. R v Fox [1986] AC 281; R v Alladice (1988) 87 Cr App R 380.
38. See Khan v UK (2001) 31 EHRR 1016.
39. For example, under the Computer Misuse Act 1990, s. 1(1) in England and Wales, when accessing data in a way that is unauthorised by either the relevant account holder or service provider (see for example DPP v Bignell [1998] 1 Cr App R 1 and R v Bow Street Metro- politan Stipendiary Magistrate ex parte United States (No. 2) [2000] 2 AC 216) and also (2013) Social media and criminal justice. Criminal Bar Quarterly 4, The Criminal Bar Association.
40. R v Loveridge (200) 2 Cr App R 591.
41. R v Marriner [2002] EWCA Crim 2855.
42. R v Rosenberg [2006] EWCA Crim 6.
43. El Haski, above n. 30.
44. See the Police & Criminal Evidence Act 1984, ss. 11 and 13.
45. See the Journalists' Code, published by the National Union of Journalists. Available at: www.nuj.org.uk/about/nuj-code/; see also Clause 47 of the Deregulation Bill.
46. R (on the application of British Sky Broadcasting Ltd.) v The Commissioner of Police of the Metropolis [2014] UKSC 17.

References

- Akhgar B, Saathoff G, Arabnia H, Hill R, Staniforth A and Bayerl PS (eds) (2015) Application of Big Data for National Security: A Practitioner's Guide to Emerging Technologies. Waltham, MA: Elsevier.
- Armstrong T, Zuckerberg M, Page L, Rottenberg E, Smith B and Costelo D (2013) An Open Letter to Washington. 9 December.
- Beguerisse-D'iaz M, Garduno-Hernandez G, Vangelov B, Yaliraki S and Barahona M (2014) Interest communities and flow roles in directed networks: the Twitter network of the UK riots.

Cornell University Library. Available at: <http://arxiv.org/abs/1311.6785> (accessed 12 September 2016).

Blackman J (2008) Omniveillance, Google, privacy in public, and the right to your digital identity: A tort for recording and disseminating an individual's image over the Internet. *Santa Clara Law Review* 49: 313

Brunet J and Claudon N (2015) Military and big data revolution. In Akhgar B, Saathoff G, Arabnia H, Hill R, Staniforth A and Bayerl PS (eds) *Application of Big Data for National Security: A Practitioner's Guide to Emerging Technologies*. Waltham, MA: Elsevier, ch. 7.

Bruns A and Burgess J (2012) #qldfloods and @QPSMedia: Crisis Communication on Twitter in the 2011 South-East Queensland Floods. Brisbane: ARC Centre of Excellence for Creative Industries and Innovation, Queensland University of Technology.

Copitch G and Fox C (2010) Using social media as a means of improving public confidence. *Safer Communities* 9(2): 42–48.

Crump J (2011) What are the police doing on Twitter? Social media, the police and the public. *Policy and Internet* 3(4): article 7.

Gaynor M (1957–1958) Admission in evidence of statements made in the presence of the defendant. *Journal of Criminal Law, Criminology and Police Science* 48: 193

Kaplan A and Haenlein M (2010) Users of the world, unite! The challenges and opportunities of social media. *Business Horizons* 53(1): 59–68.

Liberty (2011) Liberty's Report on Legal Observing at the TUC March for the Alternative. Available at: www.liberty-human-rights.org.uk/sites/default/files/libertys-report-on-legal-observing-at-the-tuc-march-for-the-alternative.pdf (accessed 22 November 2014).

Item 6

“Following the Breadcrumbs: Using Open Source Intelligence as Evidence in Criminal Proceedings” Chapter 18 in
“Open Source Intelligence Investigation – From Strategy to Implementation.”
Akhgar, B., Bayerl, S., Sampson, F (Eds)
Springer 2016

ISBN 978-3-319-47671-1

Chapter 18

Following the Breadcrumbs: Using Open Source Intelligence as Evidence in Criminal Proceedings

Fraser Sampson

Abstract Intelligence and evidence are fundamentally different and while evidence can always provide some degree of intelligence the reverse is not the case. If intelligence is to be relied on evidentially it will need to meet the same forensic standards and clear the same legal hurdles as any other form of evidence. Therefore LEAs need to be aware of these standards and hurdles at the outset and to ensure— so far as practicable—that they are in a position to address them. This chapter addresses some of the legal issues that arise if OSINT material is to be used in legal proceedings, particularly within countries that are signatories to the European Convention on Human Rights (ECHR).

*Breadcrumbs*¹[noun]

1. a series of connected pieces of information or evidence
2. a type of secondary navigation scheme that reveals the user's location in a website or Web application.

18.1 Introduction

The provenance, collation, interpretation, analysis and deployment of open source intelligence (OSINT) is becoming a highly topical and relevant area of policing. As has been considered in detail in earlier chapters OSINT can be considered as an element of a 'new age' in policing and as an adjunct to the 'longer arm of the law' (Chap. 3). In this chapter we are concerned with addressing some of the legal issues that arise if OSINT material is to be used in legal proceedings, particularly

¹ <https://www.google.co.uk/#q=breadcrumbs+web+design> (Accessed 12 June 2016).

within countries that are signatories to the European Convention on Human Rights (ECHR). While each jurisdiction will be governed by its own domestic laws there are some common elements around evidence and some overarching provisions within the ECHR that will apply to relevant proceedings in each of the 47 signatory States.² Both the generic principles of evidence and the ECHR are considered below.

The expansion of social media and Internet-based communication, together with its relevance for criminal investigation and national security, have been explored and discussed in the previous chapters. It is clear from the foregoing just how far Law Enforcement Agencies (LEA) have come to understand the power of these tools, not just as an adjunct to their own communications (Coptich and Fox 2010) but as a game-changing source of intelligence and investigation. The contribution of OSINT to inductive investigation has yet to be fully understood, still less harnessed, but the 'breadcrumbs' left by electronic data interactions by suspects, victims, witnesses and other persons of interests represent a phenomenological change in the intelligence world. Following those breadcrumbs—in both senses defined above—in order to find people, patterns, propensities or property is one thing; relying on the material to support a prosecution is another matter altogether. This chapter will consider some of the key elements in utilising OSINT material as evidence. The developments in socio-digital behaviour have produced a whole new category of 'community' which can be seen as a virtual group which coalesces around a particular theme or event, groups which are evanescent in nature and probably unique in identity. Once the event/activity/interest that unites the members of the community diminishes, so does the digital community itself (for examples see Beguerisse-Díaz et al. 2014). Law Enforcement Agencies are increasingly requesting contributions from these digital communities and seeking material from citizens to investigate crime (see for example the request

² <http://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/chartSignature/3>—accessed 15 April 2016.

by police for ‘dashcam’ material in connection with the suspected attempt to abduct an RAF serviceman³).

18.2 What Is the Difference Between Intelligence and Evidence?

At its heart the principal difference between intelligence and evidence is purposive. The purpose of intelligence is wide ranging, almost undefined, and can cover an array of activities from supplying information on which to base an arrest (e.g. by giving rise to reasonable suspicion under the Police and Criminal Evidence Act 1984, s. 24) to the likely destination of a vulnerable person who has run away from home or understanding the lifestyle of someone suspected of benefiting from the proceeds of crime. Evidence, on the other hand, has one function: to assist a court or finder of fact to determine a matter that has come before it. Of course, if the matter coming before a court arose out the use of intelligence (for example a civil action against the police for wrongful arrest based on flawed information) then the two might overlap. Taking Staniforth’s second category of intelligence (see Chaps. 2 and 3), the end user of OSINT material is essentially the organization producing or collating it while with evidential material the recipient will be the relevant tribunal.

Generally a court will not be concerned with intelligence and in some cases in England and Wales will be prevented from considering it at all.⁴ However, in some cases OSINT will potentially be helpful to parties either in a criminal prosecution or in some civil proceedings such as employment litigation, defamation or infringement of intellectual property. If OSINT is to be deployed and relied upon in criminal proceedings by LEAs there are some important practical considerations

³ <http://www.bbc.co.uk/news/uk-england-norfolk-36853106>. Accessed 26 July 2016.

⁴ See for example ss. 17–19 of the Regulation of Investigatory Powers Act 2000.

that need to be borne in mind—and the earlier in the process of acquisition the better.

To illustrate those considerations consider a situation where investigators are inquiring into a robbery. Conducting OSINT research they find a photograph on a Facebook page that appears to have been taken at the time and in the location of the alleged offence. The photograph shows two people, one of whom is the registered user of the Facebook page. The photograph shows the two people, both male, standing in a park laughing and one of the males is holding up what looks like a handgun. Plainly this OSINT would be potentially relevant to the robbery inquiry for a whole range of reasons. In and of itself the material might be sufficient to put the two men at the scene of the offence and substantiate the grounds for their arrest. It might also be relevant in terms of search activity for a weapon and stolen property, for identification of suspects, associates, witnesses, clothing etc. But how far would the material be accepted by a court in a subsequent criminal trial? A good starting point in addressing that question would be the material's relevance and what purpose it would serve. The court would need, for example, to establish the facts in issue in the case and how far the Facebook material helped to prove any of those facts. If the men in the photograph admitted to having been present in that place and at that time but simply denied having been involved in the robbery, it would be of limited relevance. If, on the other hand, they denied having been present or even knowing each other, the material would be of greater relevance. If there was dispute about their whereabouts at the time and location it might be possible to show not only the content of the image but, if it had been created on a mobile device, where and when the image was made and transmitted. There might be a description of the offenders' clothing or other matters of their appearance, words used during the offence etc., some of which could be corroborated (or indeed contradicted) by the Facebook entry and any accompanying text. But

unless the party relying on it can demonstrate the material's relevance to an issue in the proceedings it is likely to be inadmissible.⁵

18.3 Practical Issues

The requirement to demonstrate relevance to a fact in issue is a critical element in the rules of evidence within England and Wales and, as we shall see below, any other state that is a signatory to the ECHR. Then there will be issues of reliability. While a key concept in intelligence gathering, reliability has a very specific legal meaning when it comes to the rules of evidence. Before admitting the Facebook material the court would also want to know where the material came from, who made the photograph, who posted it on the page, how reliable the maker (if identified) is, how easily someone else could have made and posted the material, what the defendant has had to say about it and the integrity of the process by which it has reached the court. These considerations will not just affect the admissibility of the material but also the weight to be attached to it. The greater the likelihood that the material could have been altered or interfered with, the less weight it will carry even if it is held to be relevant.

A further and overriding consideration in a criminal trial will be the fairness of allowing the material to be adduced as evidence. In trials involving a jury it is often necessary for the judge to give specific directions about the evidence admitted, for what purpose(s) it can be considered (e.g. motive, identity, alibi etc.) and the limits of any inference that can be made from it. Generally material that has appeared in some open source with no reliable antecedents, with ready opportunities to interfere with/alter it and without anyone willing to testify to its provenance such material is unlikely to be of much use in criminal proceedings. And a significant consideration where the material is being relied upon by an LEA will be the means by which it has been obtained. If

⁵ See e.g. *R v Blastland* (1986) AC 41.

the material has been obtained illegally or in breach of process (particularly if it has been obtained in breach of a defendant's rights under Art. 8 of the ECHR⁶) there will be further impediments to its being deployed as evidence.

18.4 Legal Framework

In most jurisdictions with developed legal systems the legal framework governing criminal proceedings will provide a defendant basic entitlements such as the right to a fair hearing before an impartial tribunal, a (qualified) right not to incriminate him/herself⁷ and the right to challenge any witnesses testifying against him or her. In countries that are signatories to the ECHR these fundamental entitlements are set out in Art 6(1) and are likely to have parallels in other jurisdictions observing the rule of law. The legal framework is considered below.

The legal framework governing the acquisition and use of OSINT by LEAs in the UK is a mixture of European and domestic law, some of which creates particular challenges and dilemmas for LEAs (see Sampson 2015). As discussed above, the ECHR—and art 6(1) in particular—plays a central part in this framework; other jurisdictions beyond the 47 signatory states will have their own primary and secondary sources of protection for defendants in criminal proceedings.

18.5 European Convention on Human Rights

Article 6(1) of the European Convention on Human Rights provides that

Article 6—Right to a fair hearing

⁶ see “Opinion on the status of illegally obtained evidence in criminal procedures in the Member States of the European Union’ 30 Nov 2003—Reference: CFR-CDF. opinion 3-2003.

⁷ Funke v. France, 44/1997/828/1034; see also O'Halloran and Francis v. the United Kingdom (2007) ECHR 545; Saunders v. the United Kingdom (1997) 23 EHRR 313.

1. In the determination of ... any criminal charge⁸ against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. ...
2. Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law
3. Everyone charged with a criminal offence has the following minimum rights
 - (a) to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him;
 - (b) to have adequate time and facilities for the preparation of his defence;
 - (c) to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require;
 - (d) to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;
 - (e) ...

The admissibility of evidence is primarily a matter for regulation under national law⁹ but Art. 6(1) requires that prosecuting authorities disclose all material evidence in their possession for or against the accused.¹⁰ This duty of disclosure is strengthened by domestic legislation¹¹ and is an important element in the evidential use of OSINT discussed in Chap. 17.

Although the rules of evidence differ significantly 'civil law' jurisdictions (such as those countries whose legal systems evolved from the Napoleonic Code)¹² the effect of Art 6(1) and the broader entitlement to a fair hearing are very similar. As a general rule of fairness it can be safely assumed that the use of any OSINT material that is by its nature gravely

8 Note that there is a 'civil limb' to the ECHR – see Art 6(1) and Guide to Article 6 and the Right to a Fair Trial' Council of Europe www.echr.coe.int (Case-law – Case-law analysis – Case-law guides). Accessed 12 April 2016.

9 *Schenk v. Switzerland* (1988) ECHR 17; *Heglas v. the Czech Republic* (2007) ECHR 5564.

10 *Rowe and Davis v. the United Kingdom* (2000) ECHR 91

11 such as the Criminal Procedure and Investigations Act 1996 in England and Wales.

12 see *Law Society Gazette* 11 April 2016, pp 13–15 London.

prejudicial to the defendant is likely to be challenged and probably excluded.¹³ The entitlement to a fair hearing also involves giving a defendant the proper opportunity to challenge and question a witness [per Art. 6(3)(d)] and that would include the maker of OSINT materials relied on against him or her. Many, if not all, jurisdictions will have specific rules about hearsay evidence and its admissibility. In England and Wales hearsay is “a statement not made in oral evidence in the proceedings that is evidence of any matter stated”¹⁴ and it is governed by statute¹⁵ which provides fairly wide gateways through which hearsay evidence may be admitted. Clearly OSINT documents and material will, if used as proof of any matter stated within them,¹⁶ fall within this definition and the statutory rules, together with relevant guidelines for prosecutors should be consulted.

In relation to Art. 6(3)(b) the “facilities” that the defendant must enjoy will include the opportunity to acquaint him or herself with the results of investigations carried out throughout the proceedings.¹⁷ If the defendant is detained on remand pending trial those “facilities” may include “such conditions of detention that permit the person to read and write with a reasonable degree of concentration”.¹⁸ In order to facilitate the conduct of the defence, the defendant must not be hindered in obtaining copies of relevant documents and compiling and using any notes taken.¹⁹ All these considerations could have particular significance when relying on

13 For the general approach of the court in England and Wales see *Noor-Mohamed v R* [1949] ac 182.

14 s.114 (1) Criminal Justice Act 2003.

15 The Criminal Justice Act 2003.

16 e.g. SMS messages—*R v Leonard* (2009) EWCA Crim 1251) but cf *R v Twist* [2011] EWCA Crim 1143

17 *Huseyn and Others v. Azerbaijan* (application nos. 35485/05, 45553/05, 35680/05 and 36085/05); *OAO Neftyanaya Kompaniya Yukos v. Russia* (2014) ECHR 906.

18 *Mayzit v. Russia* application no. 42502/06; *Moiseyev v. Russia* (2011) 53 EHRR 9.

19 *Rasmussen v. Poland* (application no. 38886/05)

OSINT from the Internet and all relevant materials used by the LEA will need to be made available or accessible to the defendant.²⁰

18.6 Uses of OSINT as Evidence

Against that framework the potential evidential uses of OSINT are vast. For example the prosecution may want to use the defendant's use of certain expressions or idiosyncratic grammar to prove that she wrote a particular sentence in, say, a case of blackmail or harassment. Alternatively the state may wish to show that the defendant posted materials on social media showing that they were at a certain place at the time of an offence, that they were a member of a violent gang or that they were bragging openly about involvement in an incident²¹ Of course some criminal offences (such as the making of threats or insulting comments²² or posting 'revenge porn'²³) might directly involve the use of 'open source' material such as that found on social media. In those cases the material will be directly relevant to the facts in issue. An example can be found in one case²⁴ where a juror posted a grossly inappropriate Facebook message during the trial of an alleged sex offender. It was held that this posting of the message amounted to a contempt of court as it had been calculated to interfere with the proper administration of justice. In that case the defendant had used his smart phone to send the message when travelling home on a bus²⁵ and the message itself was direct evidence of the offence itself. Alternatively such material might include a recording made by a witness on their mobile phone and posted on YouTube to prove the manner of an assault (kicking, stamping etc.) and the presence/absence of anyone else at the time, or the geo-locator

20 Quaere whether these entitlements will ever extend to being able to access relevant materials via

the Internet where the hard or downloaded copies are incomplete or insufficiently verifiable by the defendant?

21 Bucknor v R (2010) EWCA Crim 1152.

22 See for example <http://www.theguardian.com/uk/2012/may/22/muamba-twitter-abuse-student-sorry>—accessed 16 April 2016.

23 see s. 33 Criminal Justice and Courts Act 2015.

24 Attorney-General v. Davey [2013] EWHC 2317 (Admin).

25 loc cit at 6

of a phone to undermine evidence of alibi. However, much OSINT material is unlikely to be directly probative of an offence and is more likely to be relied on by way of background or contextual information or to corroborate/contradict a specific fact in issue. In addition it may be the defendant who wishes to rely on OSINT, for instance to show that unsolicited pictures had been submitted by a complainant on his Facebook page.²⁶ In such cases the same evidential principles will apply. While these same principles can apply within the context of related civil proceedings by LEAs (such as applications for recovery of illegally obtained assets, injunctive relief or applications for confiscation orders) these are outside the scope of this book.

Finally, although OSINT is, by its nature, generally put into the public domain by others without the involvement of an LEA, investigators will need to be very cautious about any activity that may be regarded as encouraging or inciting the commission of an offence²⁷ and must not breach any laid down processes for accessing data.²⁸ As discussed above if the material has been obtained unlawfully there will be significant consequences and may even result in the dismissal of the entire case.²⁹

18.7 Conclusion

Intelligence and evidence are fundamentally different and while evidence can always provide some degree of intelligence the reverse is not the case. If intelligence is to be relied on evidentially it will need to meet the

²⁶ T v R (2012) EWCA Crim 2358.

²⁷ Khudobin v. Russia (application no. 59696/00); Teixeira v Portugal (application 44/1997/828/1034).

²⁸ See s. 1(1) of the Computer Misuse Act 1990 in England and Wales; DPP v. Bignell (1998) 1 Cr App R 1 and R v.

²⁹ El Haski v. Belgium (Application no. 649/08) Gäfgen v. Germany (2010) ECHR 759.

same forensic standards and clear the same legal hurdles as any other form of evidence. Therefore LEAs need to be aware of these standards and hurdles at the outset and to ensure—so far as practicable—that they are in a position to address them.

References

Akhgar B, Saathoff G, Arabnia H, Hill R, Staniforth A, Bayerl PS (2013) Application of big data for national security: a practitioner's guide to emerging technologies. Elsevier, Waltham MA USA

Armstrong T, Zuckerberg M, Page L, Rottenberg E, Smith B, Costelo, D (2013) An Open Letter to Washington, 9 December

Beguerisse-Díaz M, Garduno-Hernandez G, Vangelov B, Yaliraki S, Barahona M. (2014) Interest communities and flow roles in directed networks: the Twitter network of the UK riots, Cornell University Library <http://arxiv.org/abs/1311.6785>

Blackman J (2008) Omniveillance, Google, Privacy in Public, and the Right to Your Digital Identity: a Tort for Recording and Disseminating an Individual's Image over the Internet, 49 Santa Clara L. Rev. 313

Bruns A, Burgess J (2012) #qldfloods and @QPSMedia: Crisis Communication on Twitter in the 2011 South-East Queensland Floods. Queensland University of Technology, ARC Centre of Excellence for Creative Industries and Innovation, Brisbane, Australia

Casilli A, Tubaro P (2012) Social media censorship in times of political unrest—a social simulation experiment with the UK riots. *Bulletin de Methodologie Sociologique* 115:5–20

Copitch G, Fox C (2010) Using social media as a means of improving public confidence. *Safer Communities* 9(2):42–48

Crowe A (2011) The social media manifesto: a comprehensive review of the impact of social media on emergency management. *J Bus Continuity Emerg Planning* 5(1):409–420

Crump J (2011) What are the police doing on Twitter? Social media, the police and the public. *Policy Internet* 3(4):1–27

- Denef S, Kaptein N, Bayerl PS, Ramirez L (2012) Best practice in police social media adaptation. Composite project
- Earl J, Hurwitz H, Mesinas A, Tolan M, Arlotti A (2013) This protest will be Tweeted. *Inform Commun Soc* 16(4):459–478
- Howard P, Agarwal S, Hussain M (2011) When Do States Disconnect their Digital Networks? Regime Responses to the Political Uses of Social Media 9 Aug 2011. (Online) <http://ssrn.com/abstract=1907191>. Accessed 25 Nov 2014
- Kaplan A, Haenlein M (2010) Users of the world, unite! the challenges and opportunities of social media. *Bus Horiz* 53(1):59–68
- Kavanaugh AL, Yang S, Li L, Sheetz S, Fox E (2011) Microblogging in crisis situations: Mass protests in Iran, Tunisia, Egypt. CHI2011, Vancouver, Canada, May 7–12 2011
- Kokott J, Sobotta C (2013) The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR. *Int Data Privacy Law* 3(4):222–228
- Kotronaki L, Seferiades S (2012) Along the pathways of rage: the space-time of an uprising. In: Seferiades S, Johnston H (eds) *Violent protest, contentious politics, and the neoliberal state*. Ashgate, Surrey, pp 159–170
- Lanier J (2013) *Who Owns the Future?*. Simon and Schuster NY USA
- Liberty (2011) Liberty's Report on Legal Observing at the TUC March for the Alternative (Online) <https://www.liberty-human-rights.org.uk/sites/default/files/libertys-report-on-legal-observing-at-the-tuc-march-for-the-alternative.pdf> Accessed 22 Nov 2014
- Lin D (1998) Extracting Collocations from Text Corpora. First workshop on computational terminology. Montreal, Canada, pp 57–63
- Loveys K (2010) Come down from the roof please, officers tweeted, Mail Online 11 Nov 2010. (Online) <http://www.dailymail.co.uk/news/article-1328586/TUITION-FEES-PROTEST-Met-chief-embarrassed-woeful-riot-preparation.html>. Accessed 16 Mar 2011
- McSeveny K, Waddington D (2011) Up close and personal: the interplay between information technology and human agency in the policing of the 2011 Sheffield
- Anti-Lib Dem Protest. In: Akhgar B, Yates S (eds) *Intelligence management: knowledge driven frameworks for combating terrorism and organized crime*. Springer, New York, pp 199–212 NETPOL Network

for Police Monitoring (2011) Report on the Policing of Protest in London on 26 Mar 2011. (Online) <https://netpol.org/wp-content/uploads/2012/07/3rd-edit-m26-report.pdf>. Accessed 22 Nov 2014

NPIA (2010) Engage: digital and social media for the police service. National Policing Improvement Agency, London

Palen L, (2008) On line social media in crisis events Educause 3: 76-78. See also

Baron G. Social media and crisis: a whole new game. <http://www.youtube.com/watch?v=Mft7NXDhcmE>

Papic M, Noonan S (2011) Social media as a tool for protest. Security Weekly, 3 Feb 2011. (Online)

<http://www.stratfor.com/weekly/20110202-social-media-tool-protest#axzz3LWjMNk4d>. Accessed 10 Dec 2014

Poell T, Borra E (2011) Twitter, YouTube, and Flickr as Platforms of Alternative Journalism: The Social Media Account of the 2010 Toronto G20 protests Journalism 13(6):695–713

Procter R, Crump J, Karstedt S, Voss A, Cantijoch M (2013) Reading the riots: what were the police doing on Twitter? Policing Soc: An Int J Res Policy 23(4):413–436

Russell A (2007) Digital communication networks and the journalistic field: the 2005 French Riots. Critical Stud Media Commu 24(4):285–302

Sampson F (2015) Cybercrime presentation Project Courage and CAMINO Cyber Security Workshop, Montpellier, France 9 April

Searls D (2012) The intention economy: when customers take charge. Harvard University Press Cambridge, USA

Seretan V, Nerima L, Wehrli E (2003) Extraction of multi-word collocations using syntactic bigram composition. Proceedings of International Conference on recent advances in NLP Issue: Harris 51. Publisher, Citeseer, pp 424–431

Smadja F (1993) Retrieving collocations from text: xtract. Computational Linguistics 19(1):143– 177

Vieweg S, Palen L, Liu S, Hughes A, Sutton J (2008) Collective intelligence in disaster: an examination of the phenomenon in the aftermath of the 2007 virginia tech shootings. In: Proceedings of the information systems for crisis response and management conference (ISCRAM 2008)

Xiguang L, Jing W (2010) Web-based public diplomacy: the role of social media in the Iranian and Xinjiang Riots. *J Int Commu* 16(1):7-22.

Item 7

“The ATHENA Equation – Balancing the Efficacy of Citizens’ Response to Emergency with the Reality of Citizens’ Rights.” in *The Police Journal: Theory, Practice and Principles* 2017 pp 1-19
Sage Publications

<https://doi.org/10.1177/0032258X17701321>

The ATHENA Equation - Balancing the Efficacy of Citizens' Response with the Reality of Citizens' Rights around Data Protection

Introduction

The impact of social media on emergency management has been substantial (see e.g. Crowe 2010) and its “growing ubiquity, not only in geopolitical, economic and business spheres, but also in official responsiveness to crisis and disaster” has been well-documented (Akhgar *et al.* 2013). Until now, that impact has largely involved the relevant LEA and other bodies utilising the available networks as another source of mass communication in the prosecution of their ordinary tasks such as controlling public disorder and detecting/preventing crime (Coptich and Fox 2010). The ways and extent to which LEAs and other crisis responders might possibly harness new communication media - particularly web-based social media such as Twitter and Facebook, and the prolific use of high-tech mobile devices - to provide efficient and effective communication and enhanced situational awareness during a crisis is being explored by Sheffield Hallam University's EC-funded ATHENA project.

ATHENA's approach to crisis management emphasises and centres upon the necessity of effective responders to adjust their actions to the unfolding situation. Its underlying premise is that:

The public are under-utilized crisis responders; they are often first on the scene, vastly outnumber the emergency first responders and are creative and resourceful. In a crisis, the public self-organise into voluntary groups, adapt quickly to changing circumstances, emerge as leaders and experts and perform countless life-saving actions; and they are increasingly reliant upon the use of new communications media to do it. ATHENA will help them by joining their conversations and adding an enabling voice. ATHENA will give them the information they ask for, in a way they can understand. ATHENA will assist them in targeting their actions, by directing them to the places they need to be and away from danger.³²

³² ATHENA Master Document SJY Para B.1.1.1

In striving to meet this general objective, ATHENA is seeking to create and deploy two technical outputs: an ‘app’ and the information dashboard. The app envisages the person finding themselves at the centre of the relevant crisis situation as a ‘citizen reporter’ providing valuable, real time data to the responders while the dashboard provides a source of up-to-date information to those caught in crisis from a command and control centre (see fig.1).

ATHENA Toolkit and Crisis Information Processing

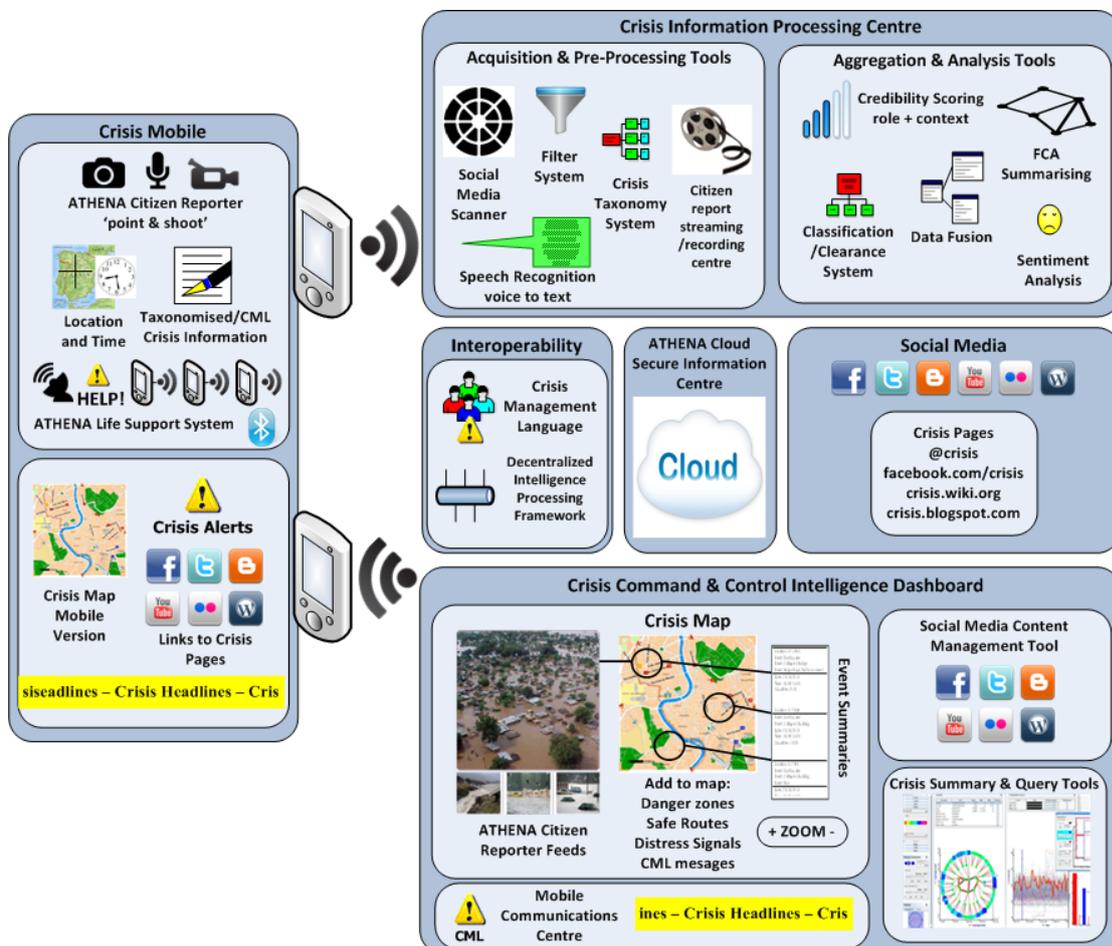


Fig. 1

These twin products are intended to deliver major enablers that will encourage users of new media to contribute to the security of ‘citizens in crisis situations’ by designing a set of best practice guidelines for law enforcement agencies (LEAs), first responders and citizens for the use of new media.

In pursuing its objectives ATHENA will necessarily create a complex series of legal relationships: relationships between contributors *inter se*, between contributors and the State, and also between contributors and their communications service providers, their employers, third sector crisis responders, potential litigants in criminal or civil proceedings, news media broadcasters etc. These relationships will be potentially problematic unless appropriately identified and catered for right from the start. Further, if there is to be additional realisation of intellectual property rights within the products and outputs it will be critical for ATHENA to have addressed all relevant legal issues arising from the creation of these complex relationships.

ATHENA recognises the existence and importance of legal considerations relating to privacy and data protection³³; what follows is intended to assist in that task and the research that will flow from it. By helping to formulate the requisite ethical and legal framework required of ATHENA, this article will also aim to provide a useful platform for discussion of any future initiatives of this type.

ATHENA: Understanding its Constituent Elements

The various elements of social media constituting the ATHENA approach to aiding citizens and LEAs in response to social crises may usefully be understood in terms of the process of *stoichiometry*. Stoichiometry is an activity (or exercise) involving the close analysis of the different relationships between relative quantities of elements taking part in a chemical reaction and is almost a perfect metaphor for the legal issues arising in ATHENA. The social reactions caused by 'crises' of the type envisaged by ATHENA (particularly where there is an investigative or criminal justice element) create legal relationships between the parties and agencies involved and arguably require an appropriate legal equation balancing, on the one hand, the efficacy of a collective response and, on the other, the observance of privacy and legal compliance around data protection.

³³ Task 2.8 (Legal and Ethical Framework)

ATHENA utilises Kaplan and Haenlein's (2010) six principal varieties of social media:

- collaborative projects (e.g. Wikipedia);
- blogs and microblogs(e.g. Twitter);
- content communities (e.g. YouTube);
- social networking sites (e.g. Facebook);
- virtual game worlds (e.g. World of Warcraft); and
- virtual social worlds (e.g. Second Life).

ATHENA looks at these media in four contextual crisis settings – public disorder, terrorism, acute threats to public health stemming from outbreaks of infectious disease/pandemics and natural disasters. The reactive communications of citizens caught in crisis already go way beyond the passive, information-consuming audience that the police (see, for example, Crump 2011) and press have previously been used to encountering. ATHENA seeks to invite those same citizens into a network of potentially limitless operational data.

West Yorkshire for Innovation (WyFi)³⁴ are leading the coordination of ATHENA which, in essence, is a 3 year, €5million project funded by the European Commission. Approved by the Chief Constable in 2011, ATHENA tackles the question of how the huge popularity of new smart mobile communications through social media can be harnessed to provide efficient and effective communication and enhanced situational awareness during a crisis for citizens and emergency responders. In terms of technical output, ATHENA will deliver two:

1. a set of best practice guidelines for emergency responders and citizens in the use of new and emerging communications media, tools and technologies during crisis situations and
2. a suite of prototype software tools (the ATHENA 'system' including the ATHENA 'app', and a command and control dashboard for multi-agency incident rooms).

From December 2013 to November 2016, ATHENA will seek to create a fundamental and permanent shift in the way crisis situations are managed by LEAs and other statutory first responders. ATHENA will ensure:

- a) that citizens are connected and better protected during crisis;

³⁴ part of the Office of the Police and Crime Commissioner for West Yorkshire

- b) the smarter use of police resources and technology;
- c) that commanders and key decision makers have increased visibility of online activity enhancing their situational awareness of dynamically unfolding events;
- d) that crises are better managed and resolved effectively, aiding swifter recovery and return to a state of 'normality'.

In achieving this, WyFi are leading a global consortium of 14 partners across the EU and in the US. The ATHENA project team consists of 26 professionals from partners including Harvard University and Blackberry. ATHENA provides €680k to WyFi to manage and deliver the project. There exists substantial future revenue potential for the post-project delivery and licensing of the ATHENA 'system' and 'app' to a global market.

In taking part in the 'reaction' to civil contingency and accepting the 'invitation' held out by the outputs (the app and the dashboard) citizens as elements will find themselves in legal relationships - both direct and vicarious – which are likely to prove operationally hazardous. ATHENA is therefore under a profound obligation to ensure that such relationships, their possible implications and consequences, are adequately considered and catered for in the project. The key issues to be included in this discussion are now explored in the following section which, for the purposes of brevity and illustration, are focused primarily on one of the major forms of crisis episode addressed by ATHENA: that of large-scale public disorder.

Understanding the legal relationships

Any consideration of the legal relationships arising from ATHENA needs to begin with the overarching regulatory framework governing data in the UK. The general protection, processing, sharing and retention of data in the UK is heavily regulated by a mixture of European and domestic law, some of which creates particular challenges and dilemmas for LEAs (see Sampson 2015). A detailed exposition of the relationship between these two areas of jurisprudence – EU and domestic – was set out by the Supreme Court in the context of data access and journalism (see *Kennedy v The Charity Commission* [2014] UKSC 20³⁵).

³⁵ See also *Osborn v Parole Board* [2013] UKSC 6; *R (Buckinghamshire County Council) v Secretary of State for Transport* [2014] UKSC 3; *R v Secretary of State for Transport ex p Factortame* (No 2) [1991] AC 601.

All questions arising from the retention and processing of data across LEAs of member states involved in ATHENA must demonstrate compliance with that legal framework and take account, not only of the relevant domestic legislation (i.e. the the Data Protection Act 1998, the Freedom of Information Act 2000 and the Protection of Freedoms Act 2012 in the UK) but also that of the European Union and decisions of the relevant tribunals.

The law relating to data protection across the EU derives from wider constructs of human rights and fundamental freedoms. In crude summary, there are two “distinct but related systems” protecting fundamental and human rights in Europe (see Kokott & Sobotta 2013). The first of these is the European Convention on Human Rights, an international agreement between the States of the Council of Europe³⁶. Convention matters are ultimately justiciable in the European Court of Human Rights (ECtHR). The Convention treats the protection of personal data as an extension of the broader right to privacy (Article 8 incorporates this with reference to an individual's private and family life, home and correspondence)³⁷. Interference by a member state (e.g. by the police) with the rights of an individual under the Convention must be “necessary in a democratic society” and have a legitimate aim to answer a “pressing social need”; they must also be proportionate³⁸. The second system of protection is found in the EU Charter of Fundamental Rights which enshrines data protection as a fundamental right in itself (also Article 8). This right is distinct from the protection of respect for private and family (Article 7) and is the province of the Court of Justice of the European Union (ECJ). Both systems converge at the point where activities – particularly those of the State - involve data capture, retention and analysis; non-compliance will create causes of action for individuals whose rights have been infringed. Thus both elements of EU jurisprudence are potentially engaged by ATHENA’s activities one key practical element of which is that of *purpose*.

Another important principle, that of ‘purpose limitation’, is a fundamental data protection mechanism³⁹ found in both the Convention on Human Rights and the Charter. This principle exists in order to achieve a balance between protection of data subjects’ rights against the necessary activities of data controllers by setting limits on how the data

³⁶ Along with others e.g. Switzerland, Russia, and Turkey

³⁷ Article 8 prohibits interference with the right to privacy except where such interference is in accordance with the generally applicable departures from the Convention article necessary in a democratic society. See *Gillan and Quinton v. The United Kingdom* (no 4158/05/2010)

³⁸ see *Coster v United Kingdom* (2001) 33 EHRR 479)

³⁹ See Article 6(1)(b) of Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281,23.11.1995, p. 31)

controllers are able to use their data. Purpose limitation has two components the first of which is purpose specification. Purpose limitation requires the collection and processing of certain types of data such as 'personal data'⁴⁰ to be carried out fairly for a 'specified, explicit and legitimate' purpose (purpose specification). It also means that the data must not be *further processed* in a way that is incompatible with the specified purpose(s); compatible use is the second component. The nature of the relationship between the controller and the data subject is critical when assessing use compatibility: any compatibility assessment will need to be more stringent if the data subject was not given sufficient freedom of choice at the point of data collection and arguably if there was a clear 'inequality of arms'⁴¹ between the State and the citizen at the point of the relationship's creation.

Addressing this element of informed choice and volitional acceptance will be essential for ATHENA, particularly where there are four different contexts envisaged by those recruiting the help (and data) of citizens. If relevant personal data is to be collected and retained lawfully by the agencies involved in ATHENA then key areas such as informed consent and compatible purpose will have to be addressed. To see why, it is helpful to look at the development of the legal regulatory framework around data retention.

On 8 April 2014, the Court of Justice of the European Union (ECJ) held that the EU's own legislation (the Data Retention Directive, the principal instrument for personal data retention in member states)⁴² was itself incompatible with various rights of the individual as it permitted data to be retained in a manner that allowed the identity of the person to be revealed, in addition to identifying the time of the communication and the place from which that communication took place⁴³. The Directive sought to ensure that data were available to prevent, investigate, detect and prosecute serious crimes and providers of publicly available electronic communications services or of public communications networks were obliged to retain the relevant data. The ECJ held that those data were capable of permitting "very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life ... daily or other movements, the activities carried out, the social relationships of those persons and the social environments

⁴⁰ personal data in England and Wales means data relating to an identified/identifiable living individual – Data Protection Act 1998

⁴¹ Equality of arms *stricto sensu* only arises in matters affecting the individual's right under Art 6 of the European Convention on Human Rights to a fair trial but the jurisprudential concept is a useful simile here.

⁴² EU Data Retention Directive 2006/24/EC

⁴³ Judgment in Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others*

frequented by them". It followed that their close, effective and certain regulation was of fundamental importance to the protection of the individual.

The response from within the UK was swift and controversial: Parliament enacted the Retention of Data and Investigative Powers Act 2014 which amends the principal statute⁴⁴, strengthening the requirements for a national security element and introducing a ministerial power to require communications companies to retain data. While this highly contentious legislative response has a built-in shelf life (by virtue of a 'sunset clause' – see s.8 (3)⁴⁵) the Government has also introduced a permanent response in the form of an equally controversial Data Communications Bill⁴⁶ which, at the time of writing, had the potential to be brought into force before the General Election in May 2015)⁴⁷. The ECJ also held that the retention of data might have a "chilling effect" on the use of electronic communication covered by the Directive on the exercise of freedom of expression guaranteed by Art 11 of the Charter of Fundamental Rights⁴⁸.

This is of substantial importance when read against the type of data collection and retention envisaged by ATHENA. While the principal focus of ATHENA is to provide first responders to crises with invaluable data that empowers them to tackle the immediate risks and threats, those same data may be critical to any subsequent investigation of criminal offences, of individuals caught up in the crises and of intelligence compilation generally. Against the broader juridical backdrop set out *supra*, the police record on data management in the UK underscores the importance of ATHENA getting this right. Although there may not be an express intention to retain personal data captured by/from participating citizens in ATHENA, several successful legal challenges (see *infra*) to the way in which the police have used and retained personal data illustrate the tensions between processing personal data for immediate use in detecting and preventing crime and the retention of such data on the basis of its potential value in future investigations/prosecutions.

⁴⁴ The Regulation of Investigatory Powers Act 2000

⁴⁵ i.e. the legislation effectively repeals itself at the end of the calendar year (see ss. 1-7 and the provisions inserted into the Regulation of Investigatory Powers Act 2000 by sections 3 to 6)

⁴⁶ The so-called "Snoopers' Charter" – see Alan Travis, *The Guardian* Monday 26 January 2015;

<https://www.liberty-human-rights.org.uk/campaigning/no-snoopers-charter>;

http://www.theregister.co.uk/2015/01/27/snoopers_charter_defeated_for_now_counter_terrorism_security_bill/

⁴⁷ In the event it was postponed and reappeared as a different bill in the Queen's Speech May 2015.

⁴⁸ For a fuller explanation see Boehm & Cole (2013)

The perennial public interest dichotomy for LEAs was well captured by Lord Bingham in a case involving more general police powers over two decades ago:

*“There is, first of all, a public interest in the effective investigation and prosecution of crime. Secondly, there is a public interest in protecting the personal and property rights of citizens against infringement and invasion. There is an obvious tension between these two public interests because crime could be most effectively investigated and prosecuted if the personal and property rights of citizens could be freely overridden and total protection of the personal and property rights of citizens would make investigation and prosecution of many crimes impossible or virtually so”.*⁴⁹

This dilemma has clearly become more challenging with the arrival and development of Big Data capabilities (see Sampson *loc cit*) and is possibly at its most acute in the field of the retention of personal data. In one of the examples referred to *supra*, *S & Marper v United Kingdom* [2008] ECHR 1581, the police retention of DNA samples of individuals arrested, but later acquitted or had the charges against them dropped, was held to be a violation of the data subject’s right to privacy). In another (*R (on the application of GC & C) v The Commissioner of Police of the Metropolis* [2011] UKSC 21) data subjects successfully challenged the policy of the Association of Chief Police Officers allowing indefinite retention of biometric samples, DNA and fingerprints, save in exceptional circumstances).

Conversely, the failings of the police in England and Wales to retain relevant personal data in a searchable shared way so as to enable the tracking of dangerous offenders such as Ian Huntley⁵⁰ were widely reported and criticised in the *Bichard Report*⁵¹ leading to wholesale changes in the police approach to operational IT capabilities. Data processing can all too easily be casually cast as mere ‘bureaucratic’ compliance⁵² and public and political tolerance of administrative niceties when faced with preventable criminality can be expected to be unforgiving of the LEAs involved. However, the link between police

⁴⁹ *R v Lewes Crown Court ex parte Hill* (1991) 93 Cr App R 60, at 65-66

⁵⁰ Convicted on 17 December 2003 of the murder of 10 year old schoolgirls Holly Wells and Jessica Chapman

⁵¹ Report of the Bichard Inquiry HC 653 22 June 2004, The Stationery Office, London

⁵² see e.g. <http://www.dailymail.co.uk/news/article-449456/Paper-tigers-lunatic-bureaucracy-crippling-police.html>

legitimacy and trust of their communities – particularly when it comes to use of intrusive powers and data processing – is too significant for ATHENA to ignore⁵³.

Should an LEA acquire personal data in the course of an ATHENA-related crisis (say, a civil contingency such as a flood) that will be potentially relevant to the investigation of subsequent criminal investigation (offences of looting) the temptation (or arguably *obligation*) for those agencies to retain those data beyond the time of the exigencies of the rescue/responder requirement, will often be irresistible. ATHENA-based data can – and in fact are *designed* to – produce specificity in key elements such as the time, identity and location of the contributor. While the value of such data in the course of the combined effort to neutralize the threat, risk and harm of the presenting crisis is self-evident, so too is the correlative value of those data to other – perhaps unrelated – investigations or simply intelligence. How far the participants can be taken to have consented to the retention and use of their personal data for divergent purposes will be important within the legal framework and ought, therefore, to be addressed at the point of recruiting ATHENA citizens.

Moreover, ATHENA is planning to go much further. For example, not only is it planning to analyse geotags to show where individuals were at the relevant time(s), or word collocation (where the frequency of occurrence of pairs or groups of words occurring in proximity is determined (Smadja 1993; Lin 1998; Seretan *et al.* 2003); the team is going to “*move the semantic analysis of social media data beyond current state of the art*”. The project will use automated processes to conduct sentiment analyses to locate and analyse digital content in real time to determine the contributor’s “emotional meaning”, developing “credibility assessments” and “scoring tools” to underpin the use of ATHENA data mining, social network and sentiment analysis tools to tag messages with reliability scores⁵⁴.

The importance of clarity and informed consent is underscored by the wider relationships between the police and the policed. In addition to the legal challenges already identified, the police have also suffered the ignominy of having their official recognition removed by the Office for National Statistics because their data processing approaches for recording

⁵³ See e.g. Hough *et al.* (2010); Bradford *et al.* (2012); Stanko (2011).

⁵⁴ see ATHENA submission Sentiment and reliability analysis - B.1.1.1

crime were found to be unreliable.⁵⁵ More recently, a report of HM Inspector of Constabulary into the reliability of crime recording data created and maintained by the police forces of England and Wales⁵⁶. Their interim report published on 1 May 2014 referred to the Inspectorate's "serious concerns" in the integrity of police crime recording data. ATHENA will need to address these issues head on, not only in order to ensure legal compliance, but also because the project relies heavily on citizens' trust and confidence in the relevant State systems. Shortcomings in data quality and reliability in the particular context of LEAs can have real and immediate detrimental impacts on and within the criminal justice process⁵⁷. The arrangements for holding LEAs and other bodies to account over their use of data collection and processing activities in an investigatory context have also attracted criticism⁵⁸.

Taken together with a degree of global mistrust of state use (and abuse) of personal data⁵⁹ and the development of what some have seen as a pervasive "omniveillance" made possible by Big Data (see Blackman 2008; Armstrong *et al.* 2013), the need to ensure transparency and legitimacy at all stages ought to be a cornerstone of ATHENA in all its settings.

In addition, other criminal justice services - such as those offered to victims of crime extended in compliance with the Victims' Code⁶⁰ in accordance with published guidance from the Office of the Information Commissioner⁶¹ - are beginning to focus on the data control and sharing arrangements. It is therefore probably time that data control protocols were built in to *all* State agencies' policies as a standard.

⁵⁵ See also "*Caught Red Handed*" - Report of the Public Administration Select Committee 13th session 2013/14 HC 760, The Stationery Office, London

⁵⁶ <http://www.justiceinspectors.gov.uk/hmic/programmes/crime-data-integrity/>.

⁵⁷ see <http://www.telegraph.co.uk/news/uknews/crime/11117598/Criminals-could-appeal-after-Home-Office-admits-potentially-misleading-DNA-evidence-presented-to-juries.html>

⁵⁸ (see, for example, the decision of the Investigatory Powers Tribunal, 5 December 2014, determining that the manner in which the US intelligence services supplied intercepted communications to the UK intelligence services,

and the latter's operation of the regime under the Regulation of Investigatory Powers Act 2000 s.8(4) was lawful and human rights-compliant -*Liberty (National Council for Civil Liberties) & Ors v Government Communications HQ & Ors* (2014) IPT 13/77/H).

⁵⁹ See <http://www.theguardian.com/world/the-nsa-files>

⁶⁰ See helpforvictims.co.uk a specific website set up by the Police and Crime Commissioner for West Yorkshire

⁶¹ https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

Although having a particular LEA frame of reference, in some respects the legal data considerations created by ATHENA reactions are similar to those affecting commercial relationships (Searls 2012), making the “customer” a fully empowered actor in the market place, rather than one whose power is entirely dependent on exclusive relationships – in this case with the State and its agencies rather than commercial vendors - particularly if those relationships are based on coerced agreement. However, a photo—sharing policy for a non-investigative agency appears relatively simple and very different from sharing with LEAs that have investigatory duties, powers and processes⁶².

One suggestion for how to manage the specific LEA-based stoichiometry of ATHENA would be to borrow from the commercial sector and create an End User Agreement Licence (EUAL) between ATHENA participants and the LEAs/State agencies in receipt of the data. Following the same principles as those being promoted in the context of commercial data exchange such an EUAL would make ATHENA transactions “bidirectional” (per Lanier 2013). It is submitted as part of this proposal that ATHENA needs to establish, if not a pure “intention economy” (per Searls *op cit*) in this regard, then at least an expressly consensual one.

The importance of having such an agreement or protocol will now be underlined with specific reference to ATHENA’s potential role in relation to major instances of public disorder.

Understanding the reaction

Much of the relevant data that will be captured, processed and retained by ATHENA in this context emanates from social media. There has been some significant research in the realm of social media and the policing of disorder generally, mostly focusing on the role played by communication in the mobilisation of disorder and coordination of participants (see e.g. Kotronaki and Seferiades 2012; Russell 2007 - French and Grecian riots of 2005

⁶² For examples see International Committee of the Red Cross(ICRC)<http://www.flickr.com/photos/ifrc/sets/72157623207618658/>
Maple Bluff [Wisconsin] Fire Department: <http://picasaweb.google.com/MapleBluffFireDepartment>
Virginia Department of Emergency Management:
<http://www.flickr.com/photos/vaemergency/>

and 2008 respectively - and Kavanaugh *et al.* 2011; Papic and Noonan 2011; Xiguang and Jing 2010 – riots and disorder around the so-called ‘Arab Spring’). There is also formal guidance for the police (NPIA 2010) though this gives no specific advice on personal data protection and compliance of the type being described here.

The relationship between public disorder and the State use of social media has largely developed around the possibility of governments using their powers to censor or curtail communication as a means of suppression (e.g. Casilli and Tubaro 2012; Howard *et al.* 2011)). However, the advances being offered by ATHENA intend to shift this and make the use of social media by public disorder responders a central tactical and strategic plank.

ATHENA considers South Yorkshire Police's social media strategy during protests around the Liberal Democrats' 2011 Spring Conference in Sheffield (McSeveny and Waddington 2011) and the force's use of Twitter and Facebook to interact with members of the public. ATHENA contrasts the police use of social media during the TUC's 'March for the Alternative' in 2011 which received praise from independent observers (Liberty 2011) but also criticism on the basis that the police seemed more concerned with managing public perception than facilitating communication, causing mistrust and unrest (Netpol 2011). They also compare the strategies of the Metropolitan Police Service (MPS) and Greater Manchester Police (GMP) during the riots of 2011 highlighting the “relative success” of GMP's more 'expressive' approach compared to that of the MPS's 'instrumental' strategy (Denef *et al.* 2013; Procter *et al.* 2013). ATHENA tracks how British police forces not only saw a tremendous growth in the number of Twitter followers but how they also, for the first time, engaged with the public on a large scale via social media, using Twitter as the main platform' (Denef *et al.*, *op cit.*).

ATHENA notes the work of researchers who found that the MPS's use of social media was hampered by the lack of a coherent social media strategy and of appropriate resources, failing to take advantage of the increasing number of people who - as events unfolded - followed the police on Twitter, creating a growing capacity for communicating risk and communicating about risk (Procter *et al.*, 2013). These authors observed varied approaches between the two police forces, citing one Metropolitan Police officer who concluded they had not been “wholly up to speed in using social media as an intelligence tool, an investigative tool and most importantly as an engagement tool” (*ibid.*, p. 21). By

contrast, Greater Manchester Police were congratulated on the way that they had chosen to use such media during the riots (*ibid.*).

While Manchester was less affected by the riots, their local police force had already established a reputation for embracing Twitter and had experimented with its use in campaigns before and ATHENA contrasts how the two forces had made use of social media during the disturbances. For example, during the period from 4-13 August, the MPS posted 132 tweets, but GMP almost three times as many (a total of 371). Beyond the quantitative difference there was also significant qualitative variation within the content and style of messages. The MPS's clear preference for using a much more impersonal style, directed to a generic audience as opposed to individual followers. While both forces employed Twitter primarily to gather and disseminate information about the riots (e.g. by posting CCTV images of perpetrators on Flickr and leaving phone numbers and website addresses) GMP placed a much greater emphasis on reassuring the public - i.e. 'noting that everything was calm and the public should not worry'. The MPS, by contrast, focused principally on maintaining law and order illustrating how one force's approach followed an *instrumental* strategy while the other's was primarily *expressive*.

Relying on other research (e.g. Deneff *et al. op cit.*) ATHENA⁶³ explores how GMP's commitment to engaging with their followers involved an immediate response to rumours (e.g. reacting to online suggestions that the nationwide riots were spreading into Manchester and having their officers of commenting directly on news reports) in a way that elicited direct personal queries submitted by followers and even remaining sensitive to the feelings and opinions of its followers (on one occasion, expressly apologising for a police Tweet that had been criticised for appearing to celebrate the length of a prison sentence subsequently handed down to a looter). The much more utilitarian approach adopted by the MPS contrasts quite starkly and almost seems to represent – at the time of the research – a conventional LEA communications strategy delivered via a new medium. Clearly ATHENA aims to inculcate a strategy – and encourage the attendant relationships between LEAs and crisis responders – based upon a qualitative shift that embraces the informal colloquy around which it has evolved.

⁶³ATHENA submission, D3.3 – A Review of Best Practices for Social Media in Crisis Communication, para 3.1.3.

While undoubtedly apprehending an innovative and sophisticated approach to social media by LEAs, the plans by ATHENA to exceed anything that has previously been done with the data generated by crisis relationships will need to be drawn to the attention of any crisis responder; arguably it needs to be publicised to communities at large. In other words, they too will be well advised to adopt an expressive strategy before drawing upon the vast social media capacity and taking on the reactivity of digital live-time communications. The parameters of their 'compatible purposes' will be particularly important in the setting of public disorder where protracted investigative process usually follows the settling of the dust. Criminal investigations can continue for months or even years beyond the emergency itself and the availability of relevant responders' data to be analysed, retained and shared with other agencies raises substantial legal issues, particularly where that data might be used for purposes that are adverse to the responder's individual interests. It is recommended that ATHENA makes explicit any likelihood that responders' data may be used for criminal intelligence, investigation and even prosecution purposes. Further legal issues arise in the case of political protest where LEAs are often as interested in upstream *prevention* as they are in real time responding (see for example the legal issues and criticisms of police action in *R (on the application of Laporte) v Chief Constable of Gloucestershire* [2006] UKHL 55)⁶⁴.

The proposals in ATHENA expect individuals voluntarily to become contributors of 'open source' intelligence, not just in the way the researchers looking at riots and public disorder have described (*supra*) but as active *agents* of the responders⁶⁵. Once they agree to do so these contributors need to be mindful that the enduring utility of their data retained is incongruous with the evanescent, situation-specific relationships created by crises. The very transient nature of digital relationships that coalesce around an event such as a public disturbance can be seen from analyses of social media patterns such as Twitter (see *Fig 2*), whereby once the event/activity/interest that unites members diminishes, so does the digital "community" itself (see Beguerisse-Díaz *et al.* 2014; also Bruns & Burgess 2012). In light of this, it is proposed that ATHENA takes account of, and prepares for the retention/deletion of relevant data once the uniting crisis (or at least an agreed phase of it)

⁶⁴ where it was held that the police action to prevent the applicant travelling from Gloucestershire to an anti-war rally in London interfered disproportionately and therefore unlawfully with the applicant's Convention rights of freedom of expression and assembly

⁶⁵ *Quaere* whether the data of citizens acting in this capacity can properly be regarded as open source?

distinct user accounts between 1pm on 6 August and 8pm on 17 August 2011 - see Procter *et al.* 2013a, 2013b).

In these settings the tactics of the police have produced a series of legal challenges and demonstrate how difficult it is to achieve the fine balance between the obligations of the State to ensure the security and safety of its citizens and its duty to ensure the protection of their human rights and fundamental freedoms⁶⁶. *Catt (loc cit)* involved, in simple terms, the concatenation of a lawful demonstration by citizens and the indefinite retention of personal data about the applicant by the police on the National Domestic Extremism Database. The case illustrates how, even where the relevant event takes place in public, the recording and retention of personal data about individuals involved can nevertheless amount to an unlawful interference with the right to respect for private life under Article 8 of the European Convention of Human Rights. The importance of retaining/regaining the holy trinity of trust, confidence and legitimacy for LEAs and their citizens is nowhere clearer perhaps than where the public disorder has a political complexion and covert tactics have been deployed.⁶⁷

These settings also raise the very real prospect of criminal proceedings or other coercive uses for the ATHENA responders' data, raising questions around non-consensual production of material and the extent to which any consent - express, implied, direct, vicarious and/or contingent – can be overridden by the relevant LEA, along with offenders' use of networks and mobile communication services to organize themselves⁶⁸. While there is not room to rehearse here the scope of police powers in obtaining such material, it is certainly worth ATHENA explaining the parameters to putative responders and the extent to which they are surrendering ownership and control of their images, texts etc. by participating.

If (as is not uncommon⁶⁹) the responders' material is used for journalistic purposes it attracts special statutory treatment in England and Wales (Sampson 2015). While material created by citizens acting alone *qua* citizens would probably not be protected by

⁶⁶ see e.g. *R (on the application of Catt) v The Association of Chief Police Officers of England, Wales and Northern Ireland and The Commissioner of Police for the Metropolis* [2013] EWCA Civ 192.

⁶⁷ (see <http://www.thetimes.co.uk/tto/news/uk/crime/article3306515.ece> also <https://netpol.org/2014/05/19/netpol-ico-complaint/>).

⁶⁸ even leading to a discussion on governments shutting off Twitter and censoring social media communication as a means of quashing protest and disorder ((Denef *et al.*, 2013; Casilli and Tubaro, 2012; Howard *et al.*, 2011)

⁶⁹ see e.g. Reynolds & Seeger (2012); Gillmor (2008); Greer (2010); Poell & Borra (2011); Russell (2007)

the usual statutory provisions enjoyed in England and Wales by journalists⁷⁰ (despite the ATHENA app's nomenclature of "Citizen Reporter") and is unlikely to abide by the strictures of journalists rules for gathering and contributing material⁷¹, material that they have shared at any stage with journalists generally might. Once this happens, the issues of compulsory disclosure to LEAs and prosecuting agencies become highly sensitive and potentially very difficult and are likely to involve questions of the journalist's substantive rights⁷². All of these legal relationship issues – and the methodology that relies as much on individual identifiable devices as much as identifiable individuals⁷³ - should be addressed by ATHENA, at least as part of its Public Awareness Plan⁷⁴ and arguably in the form of a free-standing protocol or agreement.

Finally, there may be difficult legal issues if data relationships are created between the State and its agencies and foreign nationals who become citizen responders for ATHENA. The prospect of sharing personal data across jurisdictions – both inside the EU and European Economic Area – and beyond is a challenging consideration in achieving the right balance within the stoichiometry of ATHENA, particularly as there is no Big Data equivalent of the international law concept of non-refoulement; the prospect of *compelling* such data sharing is even more so.

Conclusion

Building on other projects⁷⁵ ATHENA's underlying concept is beguilingly simple as *Fig.3* shows:

⁷⁰ See the Police & Criminal Evidence Act 1984 ss. 11 and 13

⁷¹ See the Journalists' Code published by the National Union of Journalists <https://www.nuj.org.uk/about/nuj-code/>; see also Clause 47 of the Deregulation Bill.

⁷² *R (on the application of British Sky Broadcasting Ltd.) v The Commissioner of Police of the Metropolis* [2014] UKSC 17.

⁷³ Along with associated capture, storage and processing issues such as ownership of personal devices and the additional personal data they might contain; what of borrowed or corporate devices? What of demonstrations against the commercial interests of one corporate entity and the responder is an employee? See too <http://www.theguardian.com/us-news/2015/jan/15/sp-secret-us-cybersecurity-report-encryption-protect-data-cameron-paris-attacks>

⁷⁴ per Task 9.4

⁷⁵ (including FP7 projects: Odyssey, CUBIST, DIADEM, and INDIGO and other security agency funded projects such as C-BML (NATO), 'Communicating in Crisis' (FBI), 'Community Resilience/Shielding for the National Capital Region' (U.S. Department of Defence) and 'Advice in Crisis' (Federal Emergency Management Agency))

3 Steps to Helping



Fig. 3

Public trust is arguably a *sine qua non* of any public engagement in the way envisaged - and indeed relied upon - by ATHENA. Any generally applicable issues of public trust around crises⁷⁶ are clearly made more acute by the involvement of LEAs who have coercive and intrusive powers. As such, an obvious caveat to ATHENA in this regard is that the remote utilisation of private social relationships forged by the reactions to crisis comes, if not to be used, then at least to be suspected by communities as another form of surveillance.

Given that the Council of Europe has expressed deep concerns on the legal implications of mass surveillance revealed by Edward Snowden and the correlative unlawful State use of personal data accumulated by private businesses⁷⁷, and given too that the Council has concluded that mass surveillance by LEAs has been ineffective in preventing terrorism⁷⁸ (one of the ATHENA contexts) it would be wise for ATHENA expressly to disavow any general surveillance purpose at the outset and to provide undertakings in relation to the further processing of personal data. Given also the concerns over State surveillance of public areas more generally⁷⁹ and the ongoing controversy around statutory powers for state interception of data and intrusive tactics⁸⁰ would be wise to address the very real risk that LEA usage of ATHENA Big Data might be seen as an extension of State surveillance - and a covert, unregulated one at that.

⁷⁶ For a discussion of the public's pre- and post-disaster trust of social media, engagement during disasters and behaviour and attitude change see Jin & National Liu (2010); Murdough (2009); see also Hagar (2013)

⁷⁷ Council of Europe Committee on Legal Affairs and Human Rights Draft Resolution and Recommendation adopted 26 Jan 2015

⁷⁸ Council of Europe Resolution 2031 (2015) Terrorist attacks in Paris: together for a democratic response para 14.2.

⁷⁹ see Council of Europe Doc. 11692 21 July 2008 Video surveillance of public areas Recommendation 1830 (2008) Reply from the Committee of Ministers adopted at the 1032nd meeting of the Ministers' Deputies (9 July 2008).

⁸⁰ See e.g. Liberty report on second reading of Counter-terrorism and Security Bill House of Commons Dec 2014

ATHENA aims ambitiously and pragmatically to harness the 'collective problem solving' (Palen 2008; Palen *et al.* 2009; Vieweg *et al.* 2008) of citizens using social media while, at the same time, developing “Europe-wide and internationally transferable guidelines for protocols, systems, technologies, techniques and good practice in the use of new communication media by the public to increase the security of citizens in crisis situations”⁸¹. If this civically responsive and responsible project is to succeed, those ‘guidelines’ must necessarily include a clear data protocol (possibly in the form of an end user licensing agreement) to protect the security of citizens’ personal data, identities and privacy and to safeguard the relationships that are critical to ATHENA’s scalability. If there was ever any doubt about the potency of emerging ‘citizen journalism’ then the case of officer Michael Slager⁸² surely removed it. The video footage of that police shooting in South Carolina acquired an authority and achieved a circulation to equal any establish news media agency and the substantial overlap between citizen journalism and conventional news data capture should be at the forefront of the minds of the ATHENA team and their putative responders.

Howsoever they approach the issues of legal relationships and the attendant data considerations, ATHENA would do well to revisit the contentious Draft Communications Data Bill⁸³ in which the Home Secretary describes the government’s commitment “to ensuring that ...we strike the right balance between protecting the public and safeguarding civil liberties”. This commitment to achieving equilibrium in the social reactions envisaged by ATHENA should be demonstrably present throughout the project, otherwise the vital and complex legal relationships formed and fostered by the team may become unstable and risk becoming a source of confusion, suspicion, resentment and challenge themselves.

References

Akhgar, B., Saathoff, G., Arabnia, H., Hill, R., Staniforth, A., Bayerl, PS (2013) “Application of Big Data for National Security: A Practitioner’s Guide to Emerging Technologies” Elsevier, Waltham MA USA

⁸¹ ATHENA submission, document B.1.1.12 para 4

⁸² International NY Times 10 April 2015

⁸³ CM 8359 June 2012 The Stationery Office, London

Armstrong, T, Zuckerberg, M, Page, L., Rottenberg, E., Smith, B., Costelo, D (2013) An Open Letter to Washington, 9 December

Beguerisse-Díaz, M., Garduno-Hernandez, G., Vangelov, B., Yaliraki, S., Barahona, M. (2014) Interest communities and flow roles in directed networks: the Twitter network of the UK riots, Cornell University Library <http://arxiv.org/abs/1311.6785>

Blackman, J., (2008) Omniveillance, Google, Privacy in Public, and the Right to Your Digital Identity: A Tort for Recording and Disseminating an Individual's Image over the Internet, 49 Santa Clara L. Rev. 313

Bruns, A., and Burgess, J. (2012) *#qldfloods and @QPSMedia: Crisis Communication on Twitter in the 2011 South-East Queensland Floods*. ARC Centre of Excellence for Creative Industries and Innovation, Queensland University of Technology, Brisbane QLD Australia

Casilli, A. and Tubaro, P. (2012) 'Social Media Censorship in Times of Political Unrest - a Social Simulation Experiment with the UK Riots'. *Bulletin de Methodologie Sociologique*, 115: 5-20.

Copitch, G. and Fox, C. (2010) 'Using Social Media as a Means of Improving Public Confidence'. *Safer Communities*, 9(2): 42-48.

Crowe, A. (2010) The social media manifesto: A comprehensive review of the impact of social media on emergency management *Journal of Business Continuity & Emergency Planning* Volume 5 Number 1

Crump, J. (2011) 'What are the Police Doing on Twitter? Social Media, the Police and the Public'. *Policy and Internet*, 3(4): article 7.

Denef, S., Kaptein, N., Bayerl, P., and Ramirez, L. (2012) *Best Practice in Police Social Media Adaptation*. COMPOSITE project

Earl, J., Hurwitz, H., Mesinas, A., Tolan, M. and Arlotti, A. (2013) 'This Protest will be Tweeted'. *Information, Communication and Society*, 16(4): 459-478.

Howard, P., Agarwal, S. and Hussain, M. (2011) *When Do States Disconnect their Digital Networks? Regime Responses to the Political Uses of Social Media* (August 9, 2011). [Online] <http://ssrn.com/abstract=1907191> last accessed 25th November 2014

Kaplan, A. and Haenlein, M. (2010) 'Users of the World, Unite! The Challenges and Opportunities of Social Media'. *Business Horizons*, 53(1): 59-68.

Kavanaugh, A., Yang, S., Li, L., Sheetz, S. and Fox, E. (2011) 'Microblogging in Crisis Situations: Mass Protests in Iran, Tunisia, Egypt'. *CHI2011*, Vancouver, Canada, May 7-12 2011

Kokott, J and Sobotta, C (2013) "The Distinction Between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR" *International Data Privacy Law*, , Vol. 3, No. 4 Pp 222 – 228

Kotronaki, L. and Seferiades, S. (2012) 'Along the Pathways of Rage: The Space-time of an Uprising.' In S. Seferiades and H. Johnston (Eds.) *Violent Protest, Contentious Politics, and the Neoliberal State*. Surrey: Ashgate, pp. 159-170.

Lanier, J. (2013) "Who Owns the Future?" Simon and Schuster NY USA

Liberty (2011) Liberty's *Report on Legal Observing at the TUC March for the Alternative* [Online] <https://www.liberty-human-rights.org.uk/sites/default/files/libertys-report-on-legal-observing-at-the-tuc-march-for-the-alternative.pdf> (last accessed 22nd November 2014)

Lin, D. (1998) Extracting Collocations from Text Corpora. In: First Workshop on Computational Terminology, pp. 57-63, Montreal, Canada.

Loveys, K. (2010) 'Come Down from the Roof Please, Officers Tweeted', Mail Online, 11 November, 2010. [Online] <http://www.dailymail.co.uk/news/article-1328586/TUITION-FEES-PROTEST-Met-chief-embarrassed-woeful-riot-preparation.html> (last accessed 16th March 2011)

McSeveny, K. and Waddington, D. (2011) 'Up Close and Personal: The Interplay between Information Technology and Human Agency in the Policing of the 2011 Sheffield Anti-Lib Dem Protest'. In Akhgar, B. and Yates, S. (eds.) *Intelligence Management: Knowledge Driven Frameworks for Combating Terrorism and Organized Crime*. New York: Springer, pp. 199-212

NETPOL Network for Police Monitoring (2011) *Report on the Policing of Protest in London on 26th March 2011*. [Online] <https://netpol.org/wp-content/uploads/2012/07/3rd-edit-m26-report.pdf> (last accessed 22nd November 2014).

NPIA (2010) *Engage: Digital and Social Media for the Police Service*. London: National Policing Improvement Agency.

Palen, L., (2008) "On Line Social Media in Crisis Events" Educause 3: 76-78. See also G. Baron "Social Media and Crisis: A Whole New Game" <http://www.youtube.com/watch?v=MFt7NXDhcmE>

Palen, L., Vieweg, S., Liu, S. and Hughes, A. (2009) 'Crisis in a Networked World: Features of Computer-Mediated Communication in the April 16 2007 Virginia Tech Event'. *Social Science Computer Review*, 27(4): 467-480.

Papic, M., and Noonan, S. (2011) 'Social Media as a Tool for Protest'. *Security Weekly*, Thursday 3rd February 2011. [Online] <http://www.stratfor.com/weekly/20110202-social-media-tool-protest#axzz3LWjMNk4d> (last accessed 10th December 2014)

Poell, T., and Borra, E. (2011) 'Twitter, YouTube, and Flickr as Platforms of Alternative Journalism: The Social Media Account of the 2010 Toronto G20 protests'. *Journalism*, 13(6): 695-713

Procter, R., Crump, J., Karstedt, S., Voss, A. and Cantijoch, M. (2013) 'Reading the Riots: What were the Police Doing on Twitter?'. *Policing and Society: An International Journal of Research and Policy*, 23(4): 413-436.

Russell, A. (2007) 'Digital Communication Networks and the Journalistic Field: The 2005 French Riots'. *Critical Studies in Media Communication*, 24(4): 285-302

Sampson, F., 2015 Cybercrime presentation Project Courage and CAMINO Cyber Security Workshop, Montpellier, France 9 April

Searls, D. (2012) "The Intention Economy: When Customers Take Charge". Harvard University Press Cambridge MA USA

Seretan V., Nerima, L. and Wehrli, E. (2003) Extraction of Multi-Word Collocations Using Syntactic Bigram Composition. In: Proceedings of International Conference on recent advances in NLP Issue: Harris 51, Publisher: Citeseer, Pages: 424–431

Smadja, F (1993): Retrieving collocations from text: Xtract. In: Computational Linguistics, 19(1):143--177

Vieweg, S. Palen, L., Liu, S., Hughes, A., and Sutton, J. (2008). Collective Intelligence in Disaster: An Examination of the Phenomenon in the Aftermath of the 2007 Virginia Tech Shootings. Proceedings of the Information Systems for Crisis Response and Management Conference (ISCRAM 2008)

Xiguang, L. and Jing, W. (2010) 'Web-based Public Diplomacy: The Role of Social Media in the Iranian and Xinjiang Riots'. *The Journal of International Communication*, 16(1): 7-22.

Item 8

“Legal Considerations Relating to the Police Use of Social Media” (with Lyle, A),
pp 171-188 in *“Application of Social Media in Crisis Management: Advanced Sciences
and Technologies for Security Applications”*
Akhgar, B., Staniforth, A., Waddington, D (Eds) 2017
Springer International Publishing, Switzerland

ISBN 978-3-319-52418-4

ISBN 978-3-319-52419-1 (eBook)

DOI 10.1007/978-3-319-52419-1

Library of Congress Control Number: 2017932904

Chapter 11 Legal Considerations Relating to the Police Use of Social Media

Fraser Sampson and Alison Lyle

11.1 Introduction

The impact of social media on emergency management has been substantial [1] and its 'growing ubiquity, not only in geopolitical, economic and business spheres but also in official responsiveness to crisis and disaster', has been well documented [2]. As preceding chapters have discussed, the ATHENA project will develop a system to allow the public to play a part in the effective and efficient management of a crisis situation by contributing to the 'conversation' through their use of social media networks and hi-tech mobile devices. Enabling the public to have a voice in such situations is a valuable asset, not only to those managing and responding to the crisis, but also by empowering communities to help themselves and communicate their needs (see Chaps. 5, 12 and 13). However, there are also opportunities for police to use the data collected by the ATHENA system to enable more effective and efficient investigations into criminal offences that occur at the time, or as a consequence, of the crisis. Additionally, there is a proposition that data collected throughout the crisis will be retained and shared with European LEAs. It can be seen then that there are several parties to whom the ATHENA system will be of benefit, and this theme of mutual benefit will run throughout this chapter, which addresses the legal issues that may or will arise through police use of social media, both within and related to the ATHENA context.

The concept of privacy has evolved steadily alongside changing practices of the societies in which we live, but with the rise in numbers of people living out their

F. Sampson
Office of the Police and Crime Commissioner for West Yorkshire, UK

A. Lyle (✉)
CENTRIC, Sheffield Hallam University, Sheffield, UK
e-mail: Alison.Lyle@westyorkshire.pnn.police.uk

© Springer International Publishing AG 2017
B. Akhgar et al. (eds.), *Application of Social Media in Crisis Management*,
Transactions on Computational Science and Computational Intelligence,
DOI 10.1007/978-3-319-52419-1_11

171

t.day@shu.ac.uk

lives in 'cyberspace', in the virtual world of social media, it has taken on new meaning for many people. Social media users typically post information, photographs and videos that reveal personal and often sensitive aspects of their lives, yet as recent surveys show [3], these same people are very concerned about who sees this information and, more importantly, who collects and uses it. Although social media platforms are perceived as public, free-for-all environments by organisations wishing to make use of the data, those who post information expect their privacy to be respected. This difference in perceptions is a crucial consideration for any law enforcement agency if they are to successfully share the social media world with the general population and make use of the valuable resource that it is. The key element to be established is trust; any successful relationship is built upon this and the one between the police and citizens is no different in this respect. Overall, police use of social media is seen as positive and of benefit to all those involved. However, the risk of certain activities being seen as surveillance by the State is high; this is a very sensitive area in the public arena.

ATHENA expressly recognises the existence and importance of legal considerations relating to privacy and data protection [4]; what follows is intended to help identify the legal considerations and assist in the research that will flow from the project. By contributing to the requisite legal—and ethical—framework required within ATHENA, this chapter also aims to provide a useful platform for discussion of any future initiatives of this type.

11.2 ATHENA

ATHENA is exploring the ways and extent to which LEAs and other crisis responders might possibly harness new communication media—particularly web-based social media such as Twitter and Facebook—to provide efficient and effective communication and enhanced situational awareness during a crisis (see Chap. 5).

The various elements of social media constituting the ATHENA approach to aiding citizens and LEAs in response to crises may usefully be illustrated by analogy using a process from chemistry rather than law. Stoichiometry is an activity (or exercise) involving the close analysis of the different relationships between relative quantities of elements taking part in a chemical reaction and is almost a perfect metaphor for the legal issues arising in ATHENA. The social reactions caused by 'crises' of the type envisaged by ATHENA (particularly where there is an investigative or criminal justice element) create legal relationships between the many parties and agencies involved and require an appropriate legal equation balancing; on the one hand, preserving/ensuring the safety and security of those involved and on the other, the observance of fundamental rights, including privacy, and legal compliance around data protection.

The reactive communications of citizens caught in crises already go way beyond the passive, information-consuming audience that the police [4] and press have previously been used to encountering. ATHENA seeks to invite those same citizens into providing and accessing a network of potentially limitless operational

data. This is one of its innovations and, at the same time, a significant legal consideration.

ATHENA will use social media during a crisis in two ways:

First, it will be used by one of the CCCID operators as a tool to send information out to citizens. In this way, those managing the crisis will be able to reach the maximum number of people as quickly as possible. ATHENA has two dedicated social media pages for this purpose, one on Twitter and one on Facebook. Each one is directly accessible from the ATHENA app (see Chap. 7).

Secondly, ATHENA will use web-crawling software to collect information from social media platforms¹ using algorithms, Natural Language Processing (NLP) and hashtag syntax. This will automatically identify social media posts that are relevant to the crisis. These will then be further processed, analysed and assigned credibility and priority ratings and fed into the CCCID as either aggregated reports or individually. Social media posts will be from the general public and those citizens acting as pre-first responders in the crisis, accessing social media pages through the buttons on the ATHENA app.

Moreover, ATHENA is planning to go much further. For example, not only it is planning to analyse geotags to show where individuals were at the relevant time(s), or word collocation (where the frequency of occurrence of pairs or groups of words occurring in proximity is determined [5]); the team is going to 'move the semantic analysis of social media data beyond current state of the art'. The project will use automated processes to conduct sentiment analyses to locate and analyse digital content in real time to determine the contributor's 'emotional meaning', developing 'credibility assessments' and 'scoring tools' to underpin the use of ATHENA data mining, social network and sentiment analysis tools to tag messages with reliability scores.² Such sensitive and intrusive processing will, if submitted, require an elevated degree of trust between data controller and data subject, and the latter will need to be in no doubt what level of analysis of their data has been signed up to. In that regard the ATHENA team will require clarity and a legal basis for the action. In taking part in the 'reaction' to civil contingency and accepting the 'invitation' to participate, citizens as elements will find themselves in legal relationships—both direct and vicarious—which are likely to prove operationally hazardous. ATHENA is therefore under a profound obligation to ensure that such relationships, and their possible implications and consequences, are adequately considered and catered for.

Any consideration of the legal relationships arising from ATHENA, and in particular police use of social media, needs to begin with the European regulatory framework governing human rights, data protection and the use of personal data in the police sector. The general protection, processing, sharing and retention of data are heavily regulated by both European and Member State law, some of which creates particular challenges and dilemmas for law enforcement authorities (LEAs) [6]. However, before the key issues that need to be included in this discussion are identified, it is useful to consider the various ways in which the police use social media and the growing importance of this new policing area.

¹Facebook and Twitter.

²see ATHENA submission Sentiment and reliability analysis—B.1.1.1.

11.3 Police Use of Social Media

The increasing use of social media has created a new, virtual environment for individuals and communities to live out part of their lives and has thus changed the way policing needs to be carried out. In order to keep the public safe and to detect, investigate and prevent crime the police need to be present in the new public space, in the same way as a geographical space, to ensure the safety of the public, provide reassurance and prevent or deal with crime and disorder (see Chaps. 2, 4 and 6).

The Police Foundation³ divides the police service's use of social media into three broad areas [7] as follows:

1. Providing Information—enabling specifically targeted information to be shared quickly, easily and cheaply;
2. Engagement—providing the police with a way of connecting and building relationships with local communities and members of the public;
3. Intelligence and Investigation—allowing the police to listen to what their communities are saying and to build evidence for investigations by monitoring social media content.

In respect of intelligence and investigation work, the police frequently post requests for specific information or post photographs or videos to gain assistance with identifications. Used in this way, social media is a valuable tool for police and an empowering tool for the general public who are directly supporting policing efforts. Police will also use social media sites to gain crucial information which may otherwise have been resource intensive or been unobtainable.⁴

A study from the COMPOSITE project [8] reveals that first results from a study of European police use of social media indicate high levels of general acceptance and perceived usefulness across all forces who responded. The three factors contributing to acceptance were as follows:

1. Usefulness for me as a police officer (improve performance).
2. Usefulness for my police force (improve force performance).
3. Fit with my task (is compatible with all aspects of my work).

The areas of policing ranking these more highly were community policing and crime investigations.

Another survey [9] reported that, on a global level,⁵ citizens have the same view and are enthusiastic about being involved with the police in a digital way. Overall, 79% of respondents were in favour of more digital interaction with the police and 72% were more willing, than a year before, to engage with the police using social

³The Police Foundation is the only independent charity that acts as a bridge between the public, the police and the Government in the UK, while being owned by none of them. See: www.police-foundation.org.uk.

⁴See the COMPOSITE project at: <http://www.composite-project.eu/>.

⁵Countries surveyed were Australia, France, Germany, Singapore, Netherlands, Spain, UK and the United States (Accenture 2014, p. 9).

media. It must be pointed out, however, that interaction on a voluntary basis is very different from large-scale collection of data from these sources, without citizens' knowledge or consent. This crucial difference forms the fine line between positive cooperation and perceived (or actual) surveillance.

Much of the relevant data that will be collected, processed and retained by ATHENA emanates from social media. There has been some significant research in the realm of social media and the policing of disorder generally, mostly focusing on the role played by communication in the mobilisation of disorder and coordination of participants [10].⁶ There is also formal guidance for the police [11] though this gives no specific advice on personal data protection and compliance of the type being described here.

The relationship between public disorder and the State use of social media has largely developed around the possibility of governments using their powers to censor or curtail communication as a means of suppression [12]. However, the advances being offered by ATHENA intend to shift this and make the use of social media by crisis responders a central tactical and strategic plank.

ATHENA considers South Yorkshire Police's social media strategy during protests around the Liberal Democrats' 2011 Spring Conference in Sheffield [13] and the force's use of Twitter and Facebook to interact with members of the public. ATHENA contrasts the police use of social media during the TUC's 'March for the Alternative' in 2011, which received praise from independent observers [14] but also criticism on the basis that the police seemed more concerned with managing public perception than facilitating communication, causing mistrust and unrest [15]. They also compare the strategies of the Metropolitan Police Service (MPS) and Greater Manchester Police (GMP) during the riots of 2011, highlighting the 'relative success' of GMP's more 'expressive' approach compared to that of the MPS's 'instrumental' strategy [16]. ATHENA tracks how British police forces not only saw a tremendous growth in the number of Twitter followers but how they also, for the first time, engaged with the public on a large scale via social media, using Twitter as the main platform' [17].

ATHENA notes the work of researchers who found that the MPS's use of social media was hampered by the lack of a coherent social media strategy and of appropriate resources, failing to take advantage of the increasing number of people who—as events unfolded—followed the police on Twitter, creating a growing capacity for communicating risk and communicating about risk [18]. These authors observed varied approaches between the two police forces, citing one Metropolitan Police officer who concluded they had not been 'wholly up to speed in using social media as an intelligence tool, an investigative tool and most importantly as an engagement tool' [18, p. 21]. By contrast, Greater Manchester Police were congratulated on the way that they had chosen to use such media during the riots [18].

While Manchester was less affected by the riots, their local police force had already established a reputation for embracing Twitter and had experimented with

⁶For example, the French and Grecian riots of 2005 and 2008 as well as the riots and social disorder around the so-called 'Arab Spring' [10].

its use in campaigns before, and ATHENA contrasts how the two forces had made use of social media during the disturbances. For example, during the period from 4 to 13 August, the MPS posted 132 tweets, but GMP almost three times as many (a total of 371). Beyond the quantitative difference, there was also significant qualitative variation within the content and style of messages. The MPS's clear preference for using a much more impersonal style, directed to a generic audience as opposed to individual followers. While both forces employed Twitter primarily to gather and disseminate information about the riots (e.g. by posting CCTV images of perpetrators on Flickr and leaving phone numbers and web site addresses), GMP placed a much greater emphasis on reassuring the public—i.e. 'noting that everything was calm and the public should not worry'. The MPS, by contrast, focused principally on maintaining law and order illustrating how one force's approach followed an instrumental strategy while the other's was primarily expressive.

While undoubtedly apprehending an innovative and sophisticated approach to social media by LEAs, the plans by ATHENA to exceed anything that has previously been done with the data generated by crisis relationships will need to be drawn to the attention of any crisis responder; arguably, it needs to be publicised to communities at large. In other words, they too will be well advised to adopt an expressive strategy before drawing upon the vast social media capacity and taking on the reactivity of digital live-time communications. The parameters of their 'compatible purposes' will be particularly important in the setting of public disorder where protracted investigative process usually follows the settling of the dust. Criminal investigations can continue for months or even years beyond the emergency itself and the availability of relevant responders' data to be analysed, retained and shared with other agencies raises substantial legal issues, particularly where that data might be used for purposes that are adverse to the responder's individual interests. It is recommended that ATHENA makes explicit any likelihood that responders' data may be used for criminal intelligence, investigation and even prosecution purposes. Further legal issues arise in the case of political protest where LEAs are often as interested in upstream prevention as they are in real time responding.⁷

The very transient nature of digital relationships that coalesce around an event such as a public disturbance can be seen from analyses of social media patters such as Twitter (see Fig. 11.1), whereby once the event/activity/interest that unites members diminishes, so does the digital 'community' itself [19]. In light of this, it is proposed that ATHENA takes account of and prepares for the retention/deletion of relevant data once the uniting crisis (or at least an agreed phase of it) has passed.

Where disorder emanates from political protest, the challenges for LEAs increase—and so they will for ATHENA. ATHENA has analysed a number of scenarios including the use of social media to create 'flash mobs' with thousands directed to riot hotspots such as Millbank [20]. The volume of social media

⁷R (on the application of Laporte) v Chief Constable of Gloucestershire [2006] UKHL 55; where it was held that the police action to prevent the applicant travelling from Gloucestershire to an anti-war rally in London interfered disproportionately and therefore unlawfully with the applicant's Convention rights of freedom of expression and assembly.

As illustrated, there are many ways in which the use of social media by the police is a vitally important means of communication, as well as a rich source of intelligence and information for investigations into specific crimes. The word 'specific' in this context is a key one; processing personal data in relation to specific crimes will likely satisfy the legal requirements. The difference is that ATHENA proposes to carry out web crawling for one purpose (information in a crisis) and to then retain this information and use it for policing purposes; herein lies the problem. This and related issues will need careful consideration if a balance is to be achieved and social media data is both protected and useful for policing purposes. The way to achieve this balance is to be aware of the legislative instruments that are effective in this area, to understand the principles behind those constraints and to adhere to best practices that take all these into consideration. The laws and legal instruments applying to this area stem from human rights laws at international and European level.

11.4 Legislative Instruments

The two sources of data protection at European level, the Council of Europe (CoE) and the European Union (EU), are separate legal systems but are closely related, and each has enacted specific legal instruments that aim to achieve a balance between the competing interests of protecting individuals' data and ensuring national and public safety.

The importance of providing protection for individuals against intrusion by the State was recognised in the United Nations Universal Declaration of Human Rights in 1948.¹⁰ This influenced the CoE European Convention on Human Rights (ECHR) in 1950, Article 8 of which provides that public authorities shall not interfere with the right to private life, except in specific circumstances, which are set out in Article 8(2).¹¹

The CoE recognised that more specific protection was needed in the digital age and in 1981 Convention 108¹² was opened for signature. Convention 108 remains the only legally binding international instrument in the area of data protection and specifically covers processing of information by police. Another CoE legal instrument that covers all areas of police work is the Police Recommendation.¹³ This

¹⁰ Article 12 – 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence....'

¹¹ Article 8(2)—'There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.

¹² CoE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Council of Europe, CETS No. 108, 1981.

¹³ CoE, Committee of Ministers (1987) Recommendation No. R(87)15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector. Adopted by the Committee of Ministers on 17 September 1987.

Recommendation addresses issues such as the collection of data for police purposes, methods of storage, access restrictions and rights and independent overview as well as data security. The main principles are necessity, proportionality, lawful processing and purpose limitation.

At EU level, data protection is afforded by the Data Protection Directive¹⁴; however, Article 3(2) of that Directive takes data processing by public authorities outside its remit.¹⁵ The Council Framework Decision 2008/977/JHA of 27 November 2008 (Framework Decision) addresses the processing of personal data for the purposes of police and judicial cooperation. It entered into force on 1 January 2009. The Framework Decision provides minimum standards to be maintained when processing personal data for the purposes of preventing, investigating, detecting or prosecuting criminal offences or executing criminal penalties of data which have been transmitted or made available between member states. Therefore, if the data were being shared with a police force in a different member state then this would apply, however the scope does not cover domestic processing of personal data by the competent judicial or police authorities in member states. Framework Decisions are similar to Directives in that they are binding as to the results to be achieved, but do not have direct effect.¹⁶ This leaves the situation that there is currently no binding European legislative instrument specifically addressing the processing of data for policing purposes. However, even though the Data Protection Directive does not directly apply, the principles contained therein, which derive from Convention 108, still need to be applied to policing purposes.

As outlined in the legal framework in a previous chapter, data protection laws at European level are being updated and policing purposes are now covered by legislation. The new EU laws are the General Data Protection Regulation¹⁷ (GDPR) and the Policing Directive,¹⁸ which are aimed at strengthening citizens' rights while

¹⁴ Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31 (Amended by Regulation (EC) of 29 September 2003 1882/2003 adapting to Council Decision 1999/468/EC the provisions relating to committees which assist the Commission in the exercise of its implementing powers laid down in instruments subject to the procedure referred to in Article 251 of the EC Treaty [2003] OJ L 284/1.

¹⁵ Article 3(2)—'This Directive shall not apply to the processing of personal data: ...in any case to processing operations concerning public security, defence, State security...and the activities of the State in areas of criminal law'.

¹⁶ The UK did not legislate to bring the Policing Framework Decision into effect, but issued administrative circulars.

¹⁷ European Parliament legislative resolution on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)11 – C7-0025/2012 – 2012/0011(COD)) Brussels 25.1.2012. Available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN>.

¹⁸ Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (COM(2012)10 final, Brussels 25.1.2012.

reducing burdens for public authorities. These were both finally approved in April 2016, and Member States will have until 2018 to comply. The modernisation of the CoE's Convention 108 will continue in 2016 and will compliment and reinforce the new EU laws. The diagram in Fig. 11.2 illustrates the evolution of data protection laws at European level.

11.5 Applying the Law

Any processing of personal data constitutes an interference with human rights and would need to be justified. In doing so, any law enforcement authority would have to consider the relevant requirements of the legal instruments set out earlier, as well as the overriding data protection principles that, although not directly applicable in this context, must be adhered to. This approach has been endorsed recently in respect of the new GDPR and Police Directive.¹⁹

The key data protection principles²⁰ can be summarised as follows:

1. Fair and lawful processing
2. Purpose limitation
3. Data minimisation
4. Data retention

To ensure fair and lawful processing, any police action must be in accordance with the law and part of a legitimate aim pursued, but also necessary in a democratic society.²¹ Purpose limitation and data minimisation are distinct but related principles: the first controls the reason for which certain data is being processed and the second specifies that the minimum amount of data to achieve the purpose can be processed.²² The European Court of Human Rights (hereafter ECtHR) has consistently held that the storing and retention of personal data by public authorities interferes with Art 8 ECHR. Such interferences must have a legal foundation and be justified,²³ must include sufficient and relevant reasons, have a clear link with the

Available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0010&rom=EN>.

¹⁹The Article 29 Data Protection Working Party. (2015). Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties and the free movement of such data, 3211/15/EN, WP 233. Adopted on December 1, 2015.

²⁰See Article 6 of the Data Protection Directive and Article 5 of Convention 108 for data protection principles.

²¹Article 8(2) ECHR.

²²See Article 6(b) and 6(c) of the Data Protection Directive, respectively.

²³ECtHR, *Leander v. Sweden*, No. 9248/81, 26 March 1987.ECtHR, *M.M. v. the United Kingdom*, No. 24029/07, 13 November 2012.

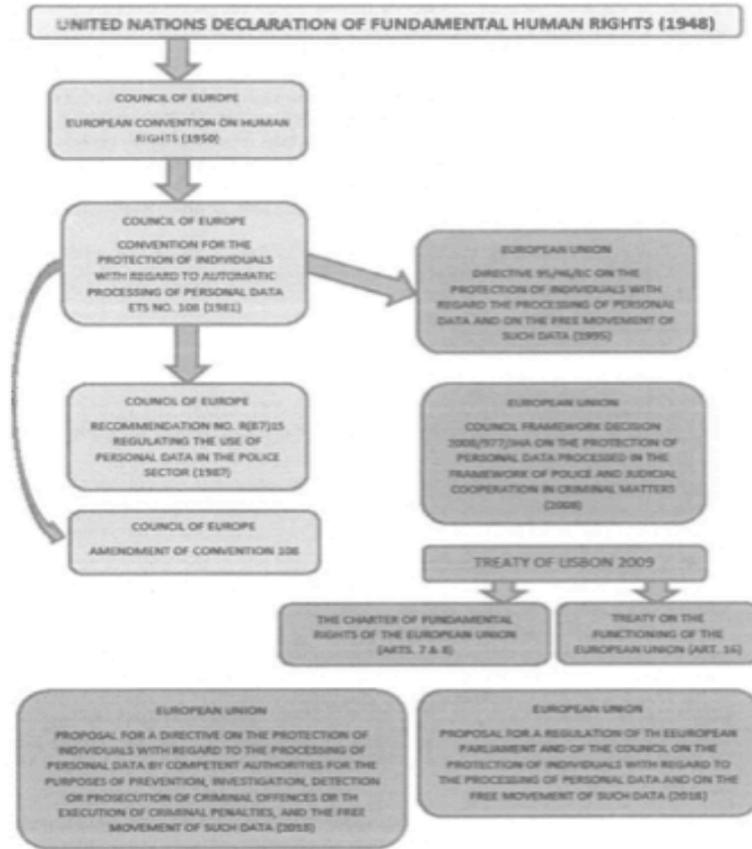


Fig. 11.2 Evolution of European Data Protection Laws

pressing social need and be proportionate. The retention of personal data by the police, particularly of non-suspects, is an area of concern.

Personal data that has been collected for one purpose (sharing information during a crisis) cannot be lawfully retained and shared with another data controller for

an entirely separate purpose, unless there was a legal basis for the new processing and the data subjects were informed of the second processing in a sufficiently clear and precise way that an informed decision could be made by them. A legal basis other than consent might consist of one of the derogations in the legislation.

Article 8 of the Charter provides protection for individuals in respect of processing their personal data. The derogation provided in Art 52 (1) would be the one which would allow this right to be limited but only if provided for by law and the essence of the stated rights and freedoms is preserved. The principles of proportionality and necessity are emphasized and were reiterated recently by the Court of Justice of the European Union in the Schrems²⁴ and Digital Rights Ireland and Others²⁵ judgments.

In respect of the ECHR, the ECtHR has set out three criteria that must be satisfied to ensure that any interference with privacy is in compliance with Article 8(2) and must be:

1. in accordance with the law;
2. in pursuit of one of the legitimate aims in 8(2); and
3. necessary in a democratic society.

The jurisprudence in this area has all been based around one or more of these tests and is well established. In *MM v United Kingdom*²⁶ the court set out the following criteria for the action to be in accordance with the law:

1. have some basis in domestic law and be compatible with the rule of law;
2. the law must be adequately accessible and foreseeable that is, formulated with sufficient precision to enable the individual to regulate his or her conduct.

To be in pursuant of a legitimate aim means that one of the aims set out in Article 8(2) must be met. In the case of *Peck v United Kingdom*²⁷ the police were in possession of CCTV footage that had been used for an investigation into an attempted suicide. This was passed to the media who then publicised the footage. The court held that there were no relevant or sufficient reasons for this disclosure without the individual's consent and there had been a violation of Article 8 ECHR.

In *Handyside v United Kingdom*²⁸ the court said that *'...necessary was not synonymous with indispensable...neither has it the flexibility of such expressions as admissible, ordinary, helpful, reasonable or desirable...'*²⁹ In the *Sunday Times* case³⁰ the court said that necessity shouldn't be interpreted too broadly nor too narrowly.

²⁴Case C-362/14, Maximilian Schrems v Data Protection Commissioner.

²⁵Joined cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others.

²⁶*MM v United Kingdom* Appl. No. 24029/07 (ECtHR 13 November 2012).

²⁷ECtHR, *Peck v. the United Kingdom*, No. 44647/98, 28 January 2003.

²⁸*Handyside v United Kingdom* Appl. No. 5493/72 (ECtHR 7 December 1976).

²⁹*Ibid.*, para 48.

³⁰*The Sunday Times v United Kingdom* Appl. No. 6538/74 (ECtHR 6 November 1980).

Any measure that interferes with an ECHR right should go no further than needed to fulfil the legitimate aim being pursued. In two cases³¹ considering proportionality, the court accepted legitimate aim of the prevention or detection of crime or disorder but then asked whether it was necessary in a democratic society.

The Court of Justice (CJ) will also apply necessity and proportionality test to Articles 7 & 8 of The Charter, which will be read together. In the Schwarz case,³² it was reiterated that limitations to fundamental rights must:

1. be provided for by law;
2. respect the essence of those rights;
3. be in accordance with the principle of proportionality, be necessary; and
4. genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

The court said it must establish whether the limitations placed on those rights are proportionate to the aims and to the objectives. It will look at whether the measures implemented are appropriate for attaining those aims and not go beyond what is necessary to achieve them. The Article 29 Working Party³³ (hereafter WP29) have emphasised the importance of the concepts of necessity and proportionality when interfering with human rights in relation to processing personal data.³⁴ The WP29 provides practical guidance to LEAs and state that thought should be given to:

- the legal basis for the measure, particularly under Article 8(2) ECHR;
- the specific issue to be tackled such as the seriousness of the issue and social and cultural issues;
- the reasons behind the measure which are closely linked to decisions about data retention, minimised collection and data quality; and
- providing sufficient evidence to support the reasons for choosing the measure.

The ECtHR has set itself three tests when determining whether a measure is 'necessary in a democratic society'. The following criteria would be useful when considering whether an action is lawful:

1. pressing social need
2. proportionality—interference proportionate to legitimate aim
3. relevant and sufficient reasons.

³¹ *S & Marper v United Kingdom*, Appl. No. 30562/04 (ECtHR 4 December 2008); *Z v Finland*, Appl. No. 2209/93 (ECtHR 25 February 1997).

³² *Schwarz v Stadt Bochum*, ECJ, C-291/12 (CJEU 17 October 2013).

³³ The Article 29 Data Protection Working Party was set up under the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. It has advisory status and acts independently. http://ec.europa.eu/justice/data-protection/article-29/index_en.htm.

³⁴ Article 29 Data Protection Working Party (2014) Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector, 536/14/EN, adopted 27 February 2014. Accessed 3 January 2016. Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf.

In the UK, all law enforcement bodies are subject to the Data Protection Act. As such the Information Commissioner's Office³⁵ took formal action against a police force that used ANPR (Automatic Number Plate Recognition) for all vehicles in and out of a small town. Although the data retention standards were being met, the purpose was a policing one and no irrelevant or inaccurate data were processed, the ECtHR held the processing was unlawful because the force had failed to show a sufficiently pressing social need to justify the intrusion into so many innocent lives. The collection of data by technical surveillance or other automated means should also be based on specific legal provisions.

In terms of 'pressing social need' the jurisprudence points to the following considerations:

- Is the measure seeking to address an issue which, if left unaddressed, may result in harm to or have some detrimental effect on society or section of society?
- Is there any evidence that such a measure may mitigate such harm?
- What are the broader views of society on the issue in question?
- Have any specific views/opposition to a measure or issue expressed by society been sufficiently taken into account?

Each case will depend on its own merits. Whether the processing will satisfy the legal requirements will depend on many things but following the principles outlined earlier, as a minimum, should be the priority before any processing takes place.

Each crisis, each crime and each investigation or prosecution will be unique, so prescriptive advice is not realistic or appropriate. However, in terms of legal instruments, it can be seen that a clear picture is being created for the future; one with a more even landscape and with greater certainty on the horizon. The principles and the core values are being emphasised by both the CoE and the EU and are being upheld by the CJEU and ECtHR. By following these standards as a minimum, European LEAs might better achieve the thus far elusive balance, which is the theme of this chapter.

11.6 Issues Relating to ATHENA

In pursuing its objectives, ATHENA will necessarily create a complex series of legal relationships: relationships between contributors inter se, between contributors and the State, and also between contributors and their communications service providers, their employers, third sector crisis responders, potential litigants in criminal or civil proceedings, news media broadcasters, etc. These relationships will be potentially problematic unless appropriately identified and catered for right from the start. Further, if there is to be additional realisation of intellectual property rights within the products and outputs, it will be critical for ATHENA to have addressed all relevant legal issues arising from the creation of these complex relationships.

³⁵Independent data protection regulatory authority in the UK. See: <https://ico.org.uk/>.

When it comes to the retention and processing of personal data, the LEA 'rap sheet' is arguably as relevant as anything the law might have to say on the subject. The level of public mistrust—particularly in the aftermath of the Snowden revelations³⁶—ought to be as important to ATHENA as the substantive legal issues. This is because ATHENA's approach is entirely dependent on the establishment and development of trusting relationships between the relevant crisis responders.

The dilemma faced by LEAs when it comes to balancing criminal investigation/prosecution and protection of the rights of citizens is nothing new,³⁷ but this dilemma has become more challenging with the arrival and development of Big Data capabilities and is possibly at its most acute in the field of the retention of personal data. In one of the examples referred to,³⁸ the police retention of DNA samples of individuals arrested, but later acquitted or had the charges against them dropped, was held to be a violation of the data subject's right to privacy.

Conversely, the failings of the police in England and Wales to retain relevant personal data in a searchable shared way so as to enable the tracking of dangerous offenders such as Ian Huntley³⁹ were widely reported and criticised in the Bichard Report⁴⁰ leading to wholesale changes in the UK police approach to operational IT capabilities. Data processing can all too easily be casually cast as mere 'bureaucratic' compliance,⁴¹ and public and political tolerance of administrative niceties when faced with preventable criminality can be expected to be unforgiving of the LEAs involved. However, the link between police legitimacy and trust of their communities—particularly when it comes to use of intrusive powers and data processing—is too significant for ATHENA to ignore.

Taken together with a degree of growing global mistrust of State use (and abuse) of personal data⁴² and the development of what some have seen as a pervasive 'omniveillance' made possible by Big Data [22], the need to ensure transparency and legitimacy at all stages ought to be a cornerstone of its settings.

In addition, other criminal justice services—such as those offered to victims of crime extended in compliance with the Victims' Code⁴³ in accordance with published guidance from the UK's Office of the Information Commissioner⁴⁴—are

³⁶ See: <http://www.theguardian.com/world/the-nsa-files>.

³⁷ This public interest dichotomy was captured by Lord Bingham at 65–66 of *R v Lewes Crown Court ex parte Hill* (1991) 93 Cr App R 60.

³⁸ ECtHR, *S. and Marper v. the United Kingdom*, Nos. 30562/04 and 30566/04, 4 December 2008.

³⁹ Convicted on 17 December 2003 of the murder of 10-year-old schoolgirls Holly Wells and Jessica Chapman.

⁴⁰ Report of the Bichard Inquiry HC 653 22 June 2004, The Stationery Office, London.

⁴¹ See e.g.: <http://www.dailymail.co.uk/news/article-449456/Paper-tigers-lunatic-bureaucracy-crippling-police.html>.

⁴² See: <http://www.theguardian.com/world/the-nsa-files>.

⁴³ See the specific website set up by the Police and Crime Commissioner for West Yorkshire: www.helpforvictims.co.uk.

⁴⁴ See: https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf.

beginning to focus on the data control and sharing arrangements. It is therefore probably time that data control protocols were built in to all State agencies' policies as a standard and ATHENA might make a useful contribution to this as a by-product.

When looking at the practicalities of how ATHENA should address these issues, it is worth looking beyond the criminal justice setting. Although having a particular LEA frame of reference, in some respects the legal data considerations created by ATHENA reactions are similar to those affecting commercial relationships [23], making the 'customer' a fully empowered actor in the market place, rather than one whose power is entirely dependent on exclusive relationships—in this case with the State and its agencies rather than commercial vendors—particularly if those relationships are based on coerced agreement. However, a photo-sharing policy for a non-investigative agency appears relatively simple and very different from sharing with LEAs that have investigatory duties, powers and processes.⁴⁵

One suggestion for how to manage the specific LEA-based stoichiometry of ATHENA would be to borrow from the commercial sector and create an End User Agreement Licence (EUAL) between ATHENA participants and the LEAs/State agencies in receipt of the data. Following the same principles as those being promoted in the context of commercial data exchange, such an EUAL would make ATHENA transactions 'bidirectional' [24].

Should an LEA acquire personal data in the course of an ATHENA-related crisis (say, a civil contingency such as a flood) that will be potentially relevant to the investigation of subsequent criminal investigation (offences of looting) the temptation (or arguably obligation) for those agencies to retain those data beyond the time of the exigencies of the rescue/responder requirement, will often be irresistible. ATHENA-based data can—and in fact are designed to—produce specificity in key elements such as the time, identity and location of the contributor. While the value of such data in the course of the combined effort to neutralize the threat, risk and harm of the presenting crisis is self-evident, so too is the correlative value of those data to other—perhaps unrelated—investigations or simply intelligence. How far the participants can be taken to have consented to the retention and use of their personal data for divergent purposes will be important within the legal framework and ought, therefore, to be addressed at the point of recruiting ATHENA citizens.

11.7 Conclusion

Public trust is arguably a *sine qua non* of any public engagement in the way envisaged—and indeed relied upon—by ATHENA. Any generally applicable issues of public trust around crises⁴⁶ are clearly made more acute by the involvement of LEAs

⁴⁵For example see: International Committee of the Red Cross (ICRC) at: <http://www.flickr.com/photos/ifrc/sets/72157623207618658/>; See also: Maple Bluff [Wisconsin] Fire Department at: <http://picasaweb.google.com/MapleBluffFireDepartment>; See also Virginia Department of Emergency Management: <http://www.flickr.com/photos/vaemergency/>.

⁴⁶For a discussion of the public's pre- and post-disaster trust of social media, engagement during disasters and behaviour and attitude change, see: Jin & National Liu (2010); Mardogh (2009); and Hagar (2013).

who have coercive and intrusive powers. As such, an obvious caveat to ATHENA in this regard is that the remote utilisation of private social relationships forged by the reactions to crisis comes, if not to be used, then at least to be suspected by communities as another form of surveillance.

Given that the Council of Europe has expressed deep concerns on the legal implications of mass surveillance revealed by Edward Snowden and the correlative unlawful State use of personal data accumulated by private businesses,⁴⁷ and given too that the Council has concluded that mass surveillance by LEAs has been ineffective in preventing terrorism,⁴⁸ it would be wise for ATHENA expressly to disavow any general surveillance purpose at the outset and to provide undertakings in relation to the further processing of personal data. Given also the concerns over State surveillance of public areas more generally⁴⁹ and the ongoing controversy around statutory powers for State interception of data and intrusive tactics,⁵⁰ it would be wise to address the very real risk that LEA usage of ATHENA Big Data might be seen as an extension of State surveillance—and a covert, unregulated one at that.

ATHENA aims ambitiously and pragmatically to harness the 'collective problem solving' [25] of citizens using social media while, at the same time, developing 'Europe-wide and internationally transferable guidelines for protocols, systems, technologies, techniques and good practice in the use of new communication media by the public to increase the security of citizens in crisis situations'.⁵¹ These 'guidelines' must necessarily include a clear data protocol (possibly in the form of an End User Agreement License) to protect the security of citizens' personal data, identities and privacy and to safeguard the relationships that are critical to ATHENA's scalability.

The EU and the CoE have consistently stressed the importance of fundamental rights in relation to the digital age and any interference with them must be justified and lawful, satisfy the principles of necessity and proportionality in particular, and also adopt a citizen's perspective. After all, joining in the conversation on social media platforms is not a right that the police have; it is only possible if the general public consent to it, it is based on the will and acceptance of the citizens and if this good will and acceptance goes, the police will have nothing. The police are facing an uphill struggle in the face of increasing concerns about surveillance and data processing by public authorities. The public are more aware than ever of their rights and more determined than ever to give effect to them. Consent and good will are key elements of any successes in this area.

⁴⁷Council of Europe Committee on Legal Affairs and Human Rights Draft Resolution and Recommendation adopted 26 Jan 2015.

⁴⁸Council of Europe Resolution 2031 (2015) Terrorist attacks in Paris: together for a democratic response para 14.2.

⁴⁹See Council of Europe Doc. 11692 21 July 2008 Video surveillance of public areas Recommendation 1830 (2008) Reply from the Committee of Ministers adopted at the 1032nd meeting of Ministers' Deputies (9 July 2008).

⁵⁰See e.g.: Liberty report on second reading of Counter-terrorism and Security Bill House of Commons December 2014.

⁵¹ATHENA submission, document B.1.1.12 para 4.

It can be seen that the main difficulty is finding the appropriate balance between respect for personal privacy and securing the safety and the welfare of the community at large. This dilemma has been illustrated in a number of ways and although several battles have been fought, the war continues. Weighing up public interest against State interests is an almost impossible task and will inevitably be decided on a case-by-case basis. What is clear though is that there are key principles that run through all the legislative instruments in this area: transparency, proportionality, necessity, data quality, data minimisation and purpose limitation. These have been repeated and will certainly feature in the forthcoming EU Directive. Both the ATHENA system and the use of social media by the police have one thing in common; they rely upon cooperation by the public.

There are many positive aspects to police use of social media, but just as this aspect of public life has changed, so must the way the police operate. This is true policing by consent and great care must be taken to achieve the correct tone and balance. Just as social media is a powerful resource for law enforcement agencies, so it is a powerful tool for uniting people the world over, and any disrespectful or overly intrusive methods of such policing has the potential to shut many virtual doors. It is clear that both the EU and the Council of Europe have digital security at the heart of their core principles; this issue isn't going to go away and will not remain unnoticed. The police need to get it right and ensure transparency, legitimacy and integrity. The public and the law makers will stand for nothing less.

References

1. Patrick Meier Digital Humanitarians. (2015). CRC Press, Taylor & Francis Group; Wendling, C., Radisch, J., & Jacobzone, S. (2013). The use of social media in risk and crisis communication. *OECD Working Papers on Public Governance*, No. 24. OECD Publishing. Accessed 9 September 2015. Retrieved from <http://dx.doi.org/10.1787/5k3v01f8kp9s-en>; Waton, H., et al. (2014). Citizen (in)security?: Social media, citizen journalism and crisis response. In *Proceedings of the 11th International ISCRAM Conference*, University Park, PA.
2. Akhgar, B., & S. Yates (Eds.). (2013). *Strategic intelligence management*. Butterworth-Heinemann. Retrieved from <http://dx.doi.org/10.1016/B978-0-12-407191-9.00015-6>.
3. UK Information Commissioner's Office (ICO). (September 2014). *Annual track 2014*. Retrieved March 30, 2016, from <https://ico.org.uk/media/about-the-ico/documents/1043485/annual-track-september-2014-individuals.pdf>; Special Eurobarometer 431, Data protection. Retrieved from http://ec.europa.eu/public_opinion/archives/eb_special_439_420_en.htm#431.
4. Crump, J. (2011). What are the Police Doing on Twitter? *Social Media, the Police and the Public*. *Policy and Internet*, 3(4), article 7.
5. Smadja, F. (1993). Retrieving collocations from text: extract. *Computational Linguistics*, 19(1):143–177; Lin, D. (1998). Extracting collocations from text corpora. In *First Workshop on Computational Terminology* (pp. 57–63), Montreal, Canada; Seretan V., Nerima, L., & Wehrli, E. (2003). Extraction of multi-word collocations using syntactic bigram composition. In *Proceedings of International Conference on Recent Advances in NLP*. Issue: Harris 51. Publisher: Citeseer.
6. Sampson, F. (2015). Cybercrime presentation Project COuRAGE and CAMINO Cyber Security Workshop, Montellier, France.

7. The Police Foundation. (2014). *The briefing: Police use of social media*. Retrieved from <http://www.police-foundation.org.uk/publications/briefings/police-use-of-social-media>.
8. Bayerl, P. S. (2012). Social media study in European Police Forces: First results on usage and acceptance. *COMPOSITE project*. Retrieved from www.composite-project.eu.
9. Accenture. (2014). *How can digital police solutions better serve citizens' expectations?* Retrieved March 30, 2016, from https://www.accenture.com/gb-en/-/_acnmedia/Accenture/Conversion-Assets/DocCom/Documents/Local/en-gb/PDF_2/Accenture-How-Can-Digital-Police-Solutions-Better-Serve-Citizens-Expectations.pdf#zoom=50.
10. Kotronaki, L., & Seferiades, S. (2012). Along the pathways of rage: The space-time of an uprising. In S. Seferiades, & H. Johnston (Eds.), *Violent protest, contentious politics, and the Neoliberal State* (pp. 159–170). Surrey: Ashgate; Russell, A. (2007). Digital communication networks and the journalistic field: The 2005 French riots. *Critical Studies in Media Communication*, 24(4): 285–302; Kavanaugh, A., Yang, S., Li, L., Sheetz, S., & Fox, E. (2011). Microblogging in crisis situations: Mass protests in Iran, Tunisia, Egypt. *CHI2011*, Vancouver, Canada, May 7–12, 2011; Papic, M., & Noonan, S. (February 3, 2011) *Social media as a tool for protest*. *Security Weekly*. Retrieved December 10, 2014, from <http://www.stratfor.com/weekly/20110202-social-media-tool-protest#axzz3LWjMNk4d>; Xiguang, L., & Jing, W. (2010). Web-based public diplomacy: The role of social media in the Iranian and Xinjiang Riots. *The Journal of International Communication*, 16(1): 7–22.
11. NPIA. (2010). *Engage: Digital and social media for the police service*. London: National Policing Improvement Agency.
12. Casilli, A., & Tubaro, P. (2012). Social media censorship in times of political unrest—A social simulation experiment with the UK riots. *Bulletin de Methodologie Sociologique*, 115, 5–20; Howard, P., Agarwal, S., & Hussain, M. (August 9, 2011). *When do states disconnect their digital networks? Regime responses to the political uses of social media*. Retrieved November 25, 2014, from <http://ssrn.com/abstract=1907191>.
13. McSeveny, K., & Waddington, D. (2011). Up close and personal: The interplay between information technology and human agency in the policing of the 2011 Sheffield Anti-Lib Dem Protest. In B. Akhgar & S. Yates (Eds.), *Intelligence management: Knowledge driven frameworks for combating terrorism and organized crime* (pp. 199–212). New York: Springer.
14. Liberty. (2011). *Liberty's report on legal observing at the TUC March for the alternative*. Retrieved November 22, 2014, from <https://www.liberty-human-rights.org.uk/sites/default/files/libertys-report-on-legal-observing-at-the-tuc-march-for-the-alternative.pdf>.
15. NETPOL-Network for Police Monitoring. (2011). *Report on the policing of protest in London on 26 March 2011*. Retrieved November 22, 2014, from <https://netpol.org/wp-content/uploads/2012/07/3rd-edition-m26-report.pdf>.
16. Denef, S., Kaptein, N., Bayerl, P., & Ramirez, L. (2012). Best practice in police social media adaptation. *COMPOSITE project*; Procter, R., Crump, J., Karstedt, S., Voss, A., & Cantijoch, M. (2013). Reading the riots: What were the police doing on Twitter? *Policing and Society: An International Journal of Research and Policy*, 23(4), 413–436.
17. Denef, S., Kaptein, N., Bayerl, P., & Ramirez, L. (2012). Best practice in police social media adaptation. *COMPOSITE project*.
18. Procter, R., Crump, J., Karstedt, S., Voss, A., & Cantijoch, M. (2013). Reading the riots: What were the police doing on Twitter? *Policing and Society: An International Journal of Research and Policy*, 23(4), 413–436.
19. Beguerisse-Díaz, M., Garduno-Hernandez, G., Vangelov, B., Yaliraki, S., & Barahona, M. (2014). *Interest communities and flow roles in directed networks: The Twitter network of the UK riots*. Cornell University Library. Retrieved from <http://arxiv.org/abs/1311.6785>; Bruns, A., & Burgess, J. (2012). *#qldfloods and @QPSMedia: Crisis Communication on Twitter in the 2011 South-East Queensland Floods*. ARC Centre of Excellence for Creative Industries and Innovation: Queensland University of Technology, Brisbane, QLD.
20. Loveys, K. (November 11, 2010). Come down from the roof please, officers tweeted. *Mail Online*. Retrieved from <http://www.dailymail.co.uk/news/article-1328586/TUITION-FEES-PROTEST-Met-chief-embarrassed-woeful-riot-preparation.html>.

t.day@shu.ac.uk

21. Procter, R., Crump, J., Karstedt, S., Voss, A., & Cantijoch, M. (2013). Reading the riots: What were the police doing on Twitter? *Policing and Society: An International Journal of Research and Policy*, 23(4), 413–436.
22. Blackman, J. (2008). *Omniveillance, Google, privacy in public, and the right to your digital identity: A tort for recording and disseminating an individual's image over the Internet*. 49 Santa Clara L. Rev. 313; Armstrong, T., Zuckerberg, M., Page, L., Rottenberg, E., Smith, B., & Costello, D. (December 9, 2013) *An Open Letter to Washington*.
23. Searls, D. (2012). *The intention economy: When customers take charge*. Cambridge, MA: Harvard University Press.
24. Lanier, J. (2013). *Who owns the future?* New York, NY: Simon and Schuster.
25. Palen, L. (2008). On line social media in crisis events. *Educuse*, 3, 76–78; See also: G. Baron. *Social Media and Crisis: A Whole New Game*. Retrieved from <http://www.youtube.com/watch?v=MP7NXDhemE>; Vieweg, S., Palen, L., Liu, S., Hughes, A., & Sutton, J. (2008). Collective intelligence in disaster: An examination of the phenomenon in the aftermath of the 2007 Virginia Tech Shootings. In *Proceedings of the Information Systems for Crisis Response and Management Conference (ISCRAM 2008)*.

Article 9

Principles for Accountable Policing –
a taxonomy of legal and ethical principles of practical use
to the police and oversight bodies and the public

Accepted by the Scottish Universities Insight Institute Oct 2019
[https://www.ScottishInsight.ac.uk/Programmes
opencall201516/principlesofaccountablepolicing.aspx](https://www.ScottishInsight.ac.uk/Programmes
opencall201516/principlesofaccountablepolicing.aspx)
and the Police Foundation May 2020

INTRODUCTION

The following *Principles for Accountable Policing* (hereafter '*The Principles*') are intended to provide a practical baseline which will inform the practice and structure of accountable policing. *The Principles* apply to the police and oversight bodies. *The Principles* have been drafted primarily with public bodies in mind but are applicable to all forms of policing.

The first section sets out the 12 *Principles*. They are divided into four parts. Part A describes general principles that underpin all accountability. Part B discusses the conduct of accountability, how it's to be done. Part C examines participation in accountability. Part D focuses on implementation and evaluation.

The second section expands upon each principle, detailing the relevant evidential base. Reflecting the focus of the workshops, most examples are drawn from the various police forces across England and Wales, Scotland, Northern Ireland and the Republic of Ireland.

The third section provides a reference guide which can be used to check how accountable the police are. It is organised as a simple checklist.

Expert Group Composition

The Principles of Accountable Policing evolved from a series of workshops held in Glasgow in 2016. Supported by the Scottish University Insight Institute, these workshops brought together leading policing experts from the police, police accountability bodies and academia. Participants from the police and oversight bodies were purposively selected to ensure a geographic representation from across Great Britain and Northern Ireland and the Republic of Ireland and a range of oversight bodies.

- Miranda Alcock – Steering Group. Former Policy Lead for Justice in Audit Scotland; Scottish Institute for Policing Research Associate
- Alice Belcher – Professor of Law, University of Dundee
- Vicky Conway – Lecturer in Law, Dublin City University; Irish Policing Authority
- Siobhan Fisher - Northern Ireland Policing Board
- Alistair Henry - Lecturer in Criminology, University of Edinburgh
- Trevor Jones – Speaker. Professor, Cardiff University
- Ciarán Kearney – Research student, University of Ulster
- Alyson Kilpatrick - Human Rights Advisor to the Northern Ireland Policing Board
- Peter Langmead-Jones - Head of Research & Development, HMIC
- John McNeill – Steering Group. Former Commissioner of the Police Investigations & Review Commission

- Lindsey McNeill - Director of Governance and Assurance, Scottish Policing Authority
- John McSporran - Police Investigations & Review Commissioner Scotland
- Ali Malik - Research student, University of Edinburgh
- Gordon Marnoch - University of Ulster
- Lawrence Marzell – Speaker. Combined Effect Lead, SERCO
- John Mitchell - Director of Investigations, Police Investigations & Review Commission
- Gareth Morgan – Speaker. Emeritus Professor of Charity Studies, Sheffield Hallam University
- Christian Mouhanna - Université Versailles Saint-Quentin- Université Paris Saclay / Université de Cergy Pontoise
- Rick Muir – Speaker. Director, Police Foundation
- Chris Noble - Chief Superintendent, District Commander / Area Co-ordinator, Police Service Northern Ireland
- Franklin Ngwu – Speaker. Lecturer in Finance and Financial Services, Glasgow Caledonian University
- Paul Nolan - Northern Ireland Policing Board
- Megan O’Neill - Senior Lecturer, School of Social Sciences, University of Dundee
- Derek Penman – (former) HM Inspector of Constabulary in Scotland
- Fraser Sampson – Steering Group. Chief Executive, Police & Crime Commissioner for West Yorkshire
- Bill Skelly – Speaker. Deputy Chief Constable, Devon and Cornwall Police
- David Steel – Speaker. Senior Research Fellow, University of Aberdeen; former Chief Executive, NHS Quality Improvement Scotland
- Amanda Stewart - Northern Ireland Policing Board
- Paddy Tomkins – Steering Group. Director, DROMAN Ltd.
- John Keegan - Superintendent, An Garda Síochána
- Debbie Watters - Vice Chair, Northern Ireland Policing Board

SECTION 1

GENERAL PRINCIPLES

This section outlines the general principles that underpin all policing accountability.

Principle 1: Universality – all policing must be accountable

Principle 2: Independence

Principle 3: Compellability

Principle 4: Enforceability and redress

Principle 5: Legality

CONDUCT

Principle 6: Constructiveness

Principle 7: Clarity

Principle 8: Transparency

PARTICIPATION

Principle 9: Pluralism and multi-level participation

Principle 10: 'Recognition' and 'Reason'

IMPLEMENTATION AND EVALUATION

Principle 11: Commit to Robust Evidence and Independent Evaluation

Principle 12: Be a Learning Organisation

SECTION 2

GENERAL PRINCIPLES

Principle 1: Universality

While the forms of accountability may differ, all policing must be accountable. This includes:

- i) Individual officers within the police
- ii) Public police
- iii) Transnational police (whether convened on a permanent or temporary basis)
- iv) Private police
- v) Mixed public / private police
- vi) Oversight bodies

It is appropriate that there are layers of accountability and different powers among the accountability bodies. There must not be two-tiered policing where some police are subject to accountability and others are not.

The growth of public and private policing agencies with overlapping remits can create challenges in relation to their own accountability structures, particularly regarding democratic accountability, and for police organisations who collaborate with them. The rise of transnational crime and, consequentially, transnational policing creates similar difficulties. There is a risk that there will be gaps in accountability, or that lines of accountability be blurred or confused.

Many police operate within complex systems. Oversight bodies must avoid replicating silos and provide holistic accountability that considers the entire system. By system, we mean not only the criminal justice system but a wider system of public private and third sector bodies. Effective accountability may help foster a shared ownership of risk. Such accountability should be inter-operable; that is, that the processes and outcomes of the accountability bodies are comprehensible to all the bodies involved and not just the body which is specifically being held to account.

Case-study: The UK's National Crime Agency (NCA) is a non-ministerial government department that was created in 2013, replacing the Serious Organised Crime Agency. It is responsible for serious and organised crime, fraud, cyber-crime, border security and sexual offences against and exploitation of children. Its officers have the powers of police constables in the various UK jurisdictions. Its direct accountability is to the Home Secretary. Unlike other UK public police forces it does not answer to a dedicated civilian oversight body, although it does come under scrutiny of organisations such as the HMIC and the IPCC as well as national regulators relating to interception and surveillance powers.

The Northern Irish Assembly initially blocked the NCA's operation in Northern Ireland due to concerns that it would not be accountable to the Northern Irish Policing Board. The NCA agreed to a number of changes, including an explicit role for the Northern Irish Policing Board and the requirement that NCA officers had to successfully complete ethics training before exercising the functions of a constable in Northern Ireland. The Assembly then passed the legislative consent motion enabling the NCA to operate.

This example of the NCA's operation in Northern Ireland highlights some of the challenges facing policing agencies that operate in addition to, and in collaboration with, local police. It applies to transnational police as much as national ones. Such policing bodies must ensure accountability in relation to their own organisation and organisations they collaborate with, giving particular attention to democratic accountability. As discussed further in relation to Principle 9, democratic accountability requires there be some local accountability over all policing that occurs in that locale (be it a region, state, country etc.).

Oversight body/bodies should ensure procedures in place to avoid an accountability gap. This may occur

- i) If officers are not subject to the oversight body in the area where the actions took place and also unaccountable to their 'home' oversight body as the actions took place elsewhere.
- ii) If information is or cannot be shared between the oversight body or force in the other locale with the 'home' oversight body or vice versa

- iii) If the 'home' oversight body cannot compel the police from the other locale to provide information, personally or through data, or vice versa

Principle 2: Independence

Those conducting accountability must be independent from those whose actions are being held to account. The police should not police themselves. Of course, internal accountability through force based professional standards departments is an appropriate and necessary form of oversight but it cannot be the only form of accountability. Those persons and institutions who perform accountability functions must be functionally independent from those they are holding to account. In the case of internal accountability, the person whose conduct is being held to account must not be involved in the actions being held to account, directly or indirectly.

An oversight body should not be dependent on the police for resources, whether personnel or financial. (See further Principle 9). Nor should it depend on the police to initiate its investigations.

Case-study: The English and Welsh Police Complaints Board was established by the Police Act 1976. It was the first time the police did not investigate complaints against themselves. However, it had no independent powers of investigation, being restricted to scrutinising the police investigation. It was criticised for its lack of independence by the Scarman Report and replaced in 1985 by Police Complaints Authority.

Principle 3: Compellability

The police can control oversight by controlling information. If oversight bodies are only privy to part of the information they cannot exercise informed control. It is therefore imperative that oversight bodies may compel the police to provide information, whether in person or through the provision of other evidence. This is in addition to Principles of Transparency, below, under which the police should ensure that relevant information is routinely published.

In common with a number of the other Principles, it is not appropriate that all oversight bodies may compel witnesses or information. In addition to the usual criterion of relevance, it may be appropriate for some limitations to be imposed in relation to information that may be compelled. The courts' ability to compel evidence is, for example, subject to some exceptions, such as, in the UK, the doctrine of public interest immunity or, in the USA, the state secrets doctrine.

Case study: In 2015 the Interception of Communications Commissioner's Office held that Police Scotland had breached the Regulation of Investigatory Powers (Scotland) Act 2000 when intercepting

communications sent to journalists. When the Scottish Parliament's Justice Committee investigated the matter in January 2016 Police Scotland refused the Committee's request to send four officers. The Committee have the power to compel witnesses but chose not to exercise it. In January 2017 Police Scotland were held to have acted unlawfully.⁸⁴

This case study highlights the, sometimes complex, practicalities of compelling information from the police, as well as how different layers of accountability can interact. Often oversight bodies prefer to use 'soft power', often hoping that simply publicising an invitation will cajole or embarrass the invitee to attend without requiring the body to formally compel their attendance. An oversight body may choose not to exercise the power to compel a witness in order to preserve the long term relationship between it and the police, particularly if the actions under question will be addressed by another oversight body. (Which is not to suggest this was the motivation of the Justice Committee in this case).

Some oversight organisations have powers to conduct search and seizure and arrest police. The officers of the Office of Police Ombudsman of Northern Ireland have powers of a constable in relation to its investigations. Powers to compel must be clearly set out in a legal framework which identifies the situations in which they can be used and the sanctions, should the police fail to follow the directions.

Principle 4: Enforceability and redress

Accountability bodies must be able to effect change. As with the Principle of Compellability, it is appropriate that different oversight bodies have different powers in this respect. Courts may impose criminal and/or civil sanctions. Providing a public account of particular conduct may be appropriate and sufficient redress for other oversight bodies.

It may be appropriate that the conclusions of one oversight body are enforced by another. For example, a local oversight body, comprised of civilians, may uncover evidence of unlawful activity. Appropriate redress in such circumstances would be obtained through the courts. Or, an oversight body may compel answerability (ie an obligation to report) without any power to sanction. Rather than analysing each oversight body individually, the imperative is to ensure that within the system there are effective mechanisms for enforceability and redress.

Oversight bodies must have the means to enforce their recommendations and monitor police progress towards implementation.

⁸⁴ Investigatory Powers Tribunal 31 Jan 2017 (IPT/15/586/CH; IPT/16/448/CH). Note the Chief Constable of Cleveland Police was the respondent. This was one of the eight police forces that merged in April 2013 to form Police Scotland.

There are various levers that may be used to effect change. Publicising findings may prompt a response from the police body in order to avoid or repair reputational damage.

Case study: In 2014 findings from a PhD study detailed how Scottish rates of stop and search were around four times higher than in England and Wales, with a disproportionate impact on children and a heavy reliance on nominally 'consensual' searches, which do not require reasonable suspicion.⁸⁵ There was significant initial resistance from the police and Justice Minister regarding reform. Following media focus on the story,⁸⁶ further research briefings and a report by the HMICS,⁸⁷ an Independent Advisory Group was established in 2015 which advocated legislative change to prohibit 'consensual searches' and institute a Code of Practice.⁸⁸ Rates of stop and search dropped precipitously.

Principle 5: Legality

There are three elements to this Principle.

- i. The police are accountable to the law
- ii. Accountability must be exercised in accordance with the law
- iii. Accountability structures should be governed by formal rules with major lines of accountability defined by law

The Principle of Legality touches on a number of fundamental policing doctrines. Ultimately, police are accountable to the law. They are empowered and bound by the law. This is why police cannot be ordered to enforce the law in a particular way and why they are required to not follow illegal orders.⁸⁹

It follows that the public policing bodies must be established by law. All policing powers, for private and public forces, must be established by law. There must be a clear, legal framework governing joint operations and secondment. These are necessary prerequisites for accountability. The police cannot be held to account unless their powers are clearly delineated.

⁸⁵ K Murray 'Stop and Search in Scotland: an evaluation of Police Practice' (SCCJR Research Report 1/2014, 2014); K Murray 'Stop and Search in Scotland: A Post Reform Overview – Scrutiny and Accountability' (SCCJR Research Report 6/2015, 2015).

⁸⁶ See, e.g., L Adams 'Police questioned on search tactics' (*The Herald*, 18 Jan 2014).

⁸⁷ HMICS 'Audit and assurance review of stop and search: phase 1' (HMICS 2015).

⁸⁸ Criminal Justice (Scotland) Act 2016.

⁸⁹ See, e.g. 'The European Code of Police Ethics' (Council of Europe 2002).

Case-study: The Association of Chief Police Officers (ACPO). ACPO was established in 1948 through the merger of the Chief Constables' Club and the Chief Constables' Association of England and Wales. It was funded by central Government from 1990 and became a limited company in 1997. It styled itself as a 'strategic body' whose main functions were to coordinate strategic responses among the Chief Constables. It became increasingly involved in determining best practice and developing policies which, while not legally binding, were highly influential. It also had corporate functions.

Issues arose from its not being established by statute. For example, it was not initially subject to the Freedom of Information Act 2000 as it was not a public authority.⁹⁰ Thus one of the major policing bodies – which was one of the best known police 'brands' – avoided an important aspect of public accountability due to its informal structures. It was criticised for its lack of transparency and the obscurity of its accountability processes in 2013.⁹¹ It was replaced by the National Police Chiefs' Council in 2015 which is subject to a clearer structure, set out in statute, and improved accountability.

Ethical policing is built upon the rule of law. It is at the heart of accountability also. Accountability should be bound by clear, accessible rules and be proportionate. Major oversight bodies should be established by law, with the major lines of responsibility set out in law. This ensures that key characteristics, such as independence, are guarded. It reduces the risk of policy churn and constantly shifting landscapes of accountability. It helps to ensure that relationships between police and oversight bodies are not solely reliant on personal relationships.

Part B: Conduct

Principle 6: Constructiveness

Accountability should be responsive, enabling and non-confrontational. It should be a dialogic process between those performing accountability functions and the police. It should form a feedback loop where lessons are learned, not just identified.

In relation to accountability, responsiveness requires the police be receptive to the oversight bodies (including the public) and vice versa. This does not mean the police can 'edit' the oversight bodies' conclusions to ensure a more favourable light is cast upon their actions. It means that the oversight bodies listen to the police' response regarding the context and feasibility of proposed changes. Responsiveness neither requires nor implies that the two parties will always agree. The oversight bodies must also be responsive to the concerns and needs of those who are subject to policing.

⁹⁰ It became subject to the Act in 2011 under the Freedom of Information (Designation as Public Authorities) Order 2011 / 2598.

⁹¹ Parker 'Independent Review of ACPO' (2013).

Case-study: In 2013 Her Majesty's Inspectorate of Constabulary (HMIC) published its report on the use of stop and search powers by English and Welsh police forces.⁹² It was broadly critical, concluding that the powers were not being used effectively, that recording requirements were not being followed, and that almost a third of recorded stops failed to provide an adequate justification for the exercise of the power. A majority of the Police and Crime Commissioners responded to the report. In 2014 the HMIC revisited the issue, publishing a follow-up report which tracked the progression towards their original ten recommendations.⁹³ It also investigated two new areas of stop and search. A number of Police and Crime Commissioners responded to the new report. The HMIC then published a report into forces' compliance with the Best Use of Stop and Search (BUSS) scheme, finding that only 11 of the 43 forces were in compliance. The HMIC conducted a further follow-up investigations of non-compliant forces through 2015 and 2016.⁹⁴ By 2017 HMIC determined that 41 of 42 forces were now compliant.⁹⁵

Related to responsiveness, it is imperative that oversight bodies enable the police to improve their accountability. Recommendations and requirements should be realistic and achievable. Accountability must aim towards developing positive behaviours and culture rather than simply focusing on particular decisions. In this way decision making and broader cultures can be positively influenced. While accountability must involve independent oversight bodies, the process of accountability should aim to embed best practice within policing. This requires the police be involved in and engaged with the process, rather than feeling like – or being – inert actors to whom accountability is 'done'.

Principle 7: Clarity

Police and oversight bodies must ensure

- Clarity of oversight
- Clarity of expectations
- Clarity of expression
- Clarity of data

Clarity of oversight: It is appropriate that there are some overlapping responsibilities in relation to oversight. For example, local accountability over cross-jurisdictional policing (see case-study for Principle 1). Care must taken to ensure clarity regarding each bodies' role and their

⁹² HMIC 'Stop and search powers: Are the police using them effectively and fairly?' (HMIC 2013).

⁹³ HMIC 'Stop and search powers 2: Are the Police Using them Effectively and Fairly?' (HMIC 2015).

⁹⁴ See HMIC 'PEEL: Police legitimacy 2015' (HMIC 2015); HMIC 'Best Use of Stop and Search (BUSS) Scheme' (HMIC 2016).

⁹⁵ HMIC 'Best Use of Stop and Search (BUSS) Scheme' (HMIC 2017).

interactions with each other and with the police. A lack of clarity regarding their respective roles can undermine their relationships.

The oversight landscape can become complex if not cluttered, especially in relation to multiple policing bodies. Unnecessary replication

- wastes police' and oversight bodies' resources
- creates unneeded complexities which obfuscate the objectives of accountability and undermine the Principle of Transparency, and
- may cause accountability fatigue.

A fine balance is required. Policing is an exceptionally complex activity which operates with a system of systems. Complexity of itself is not something to be avoided. Oversight bodies must resist the temptation to move towards a silo-mentality in the name of simplicity, thereby overlooking the interactions of multiple agencies (both police and other private and public bodies). A pluralist approach also helps to minimise the limitations inevitable in each paradigm of accountability. Ensuring that lines of oversight are clearly set-out and understood by all parties will help the police and oversight bodies to ensure a constructive pluralist approach rather than redundant duplication.

Clarity of expectations: Effective accountability requires clarity regarding the powers and duties of the oversight bodies and the police. There must be clear expectations as to what the oversight body can and should do. There must be clarity regarding the roles of the individuals on that body. There may, for example, be the impression of different, even competing, mandates from elected persons on a mixed oversight body compared with experts or lay people.

There must be clarity regarding the outcomes and consequences of oversight bodies' decisions. Is their role to provide an account by publicising an accurate record of events? Is it to mandate that specific changes occur? Clarity of expectations will help ensure collaborative and effective working relationships between the police and oversight bodies.

Clarity of expression is closely linked with clarity of expectation. It applies to the interactions of the police and oversight bodies with each other and with the public. Reports, submissions etc. should be written in a clear and accessible style, with technical terms used only when necessary. Oversight bodies' communications must be accessible to the public with consideration given to the target audience.

Clarity of data: 'clarity' here encompasses quality and quantity. Informed decisions cannot be made on the basis of unreliable data. Data must be of a requisite quality and, where there are multiple policing bodies, standardised to permit comparison. Data must not be used as a means of concealment; the quantity must be appropriate for the objectives and sufficient to permit methodologically sound analysis.

As discussed in relation to the Principle of Transparency, the default position should be to publish data. It must be provided in an accessible and useful format (e.g. analysable datasets) which is appropriate for the target audience. As discussed further in Principle 9, it is vital that there is requisite expertise on the oversight bodies to understand and analyse the information given and assess its quality.

Case-study: In 2002 two 10 year old girls were murdered by Ian Huntley. It emerged after his conviction that he had been the subject of eight allegations of sexual offences in a different police force area. None of these were discovered when he was vetted for his job at the school the two girls attended. The subsequent 'Bichard Inquiry' concluded that poor data quality, and flawed intelligence systems, contributed to the police failing to identify Huntley's pattern of behaviour in relation to the allegations of sexual offences.⁹⁶ The police force conducting the vetting incorrectly entered Huntley's date of birth and failed to check against all aliases.

Principle 8: Transparency

Accountability is a means to transparency and must itself be conducted in a transparent manner. There can be no accountability without transparency. Information is the lifeblood of accountability. Without accurate, relevant and timely information, oversight bodies cannot function.

Oversight bodies must make their findings and workings public. Without transparency regarding their process and conclusions, the oversight bodies cannot hope to garner confidence from the public or the police.

While it is appropriate that, at least some, oversight bodies may compel the police to provide information, it is imperative that the default position for the police is to routinely publish data on police performance (including the exercise of coercive powers). The 'Race and the Criminal Justice System' statistics, for example, have been published since 1992. While there are limitations to the data, it provides an important overview of the experiences of Black and Minority Ethnic groups with the criminal justice system in England and Wales, permitting trends to be accessed over decades. Such publications enable people and institutions outside the formal oversight structures to participate in the accountability process. Key groups include the media, academia and community groups, in addition to the general public. These groups provide additional oversight, helping in particular to identify issues that have fall outside the normal remit of formal accountability structures, or have been deliberately covered-up.

Case-study: In 2011 two Guardian journalists revealed how an undercover police officers working within the Metropolitan Police Service's National

⁹⁶ Bichard 'The Bichard Inquiry' (HMSO, HC653, 2004).

Public Order Intelligence Unit infiltrated a number of activist movements.⁹⁷ Some of the officers had long-term intimate relationships with activists under their assumed identities. Some fathered children. The media revelations prompted number responses from other formal a number of legal cases and a public inquiry, which has not yet reported.⁹⁸

Part C: Participation

Principle 9: Pluralism and multi-level participation

Participation in oversight requires a pluralistic approach and should be achieved through a combination of democratic processes, epistocratic bodies and consultative forums at national and local levels.

Quis custodiet ipsos custodiet? or ‘Who guards the guardians?’ brings into focus the question of who should participate in the accountability of policing. Oversight bodies need a degree of democratic legitimacy so participation may be achieved may be through electoral processes. However, it is a mistake to equate voting with democracy and while free and fair elections to oversight bodies might be necessary, this is not a sufficient condition for democratic accountability of policing. Tying participation in police accountability arrangements to an electoral process poses a danger to vulnerable minorities who may be subject to the tyranny of the majority; and also creates a risk of plutocracy as a result of unequal resources to affect the political process. There might also be concerns that those elected on to oversight bodies might not have adequate expertise to offer robust scrutiny of policing policies and practice or to provide appropriate guidance around strategic priorities.

To address this potential weakness, a complementary approach to processes of participation in police accountability is rooted in epistocracy (the ‘rule of the knowers’) with people are appointed to oversight bodies on the basis of pre-determined skills and competencies. The justification of an epistocratic arrangement of police governance is that drawing on expert knowledge will result in better policies and create confidence in the decision-making process⁹⁹. Epistocratic arrangements are not without their challenges. Critics argue they risk being elitist and exclusionary and there must therefore be a level of responsiveness to the public (vertical responsiveness) and to a range of other institutions and organisations (horizontal responsiveness)¹⁰⁰.

⁹⁷ See further Lewis & Evans *Undercover: The true story of Britain’s secret police* (Guardian Faber, 2013) and the Guardian blog: ‘Undercover, with Rob Evans and Paul Lewis’ <<https://www.theguardian.com/uk/undercover-with-paul-lewis-and-rob-evans>>.

⁹⁸ Pitchfork ‘Inquiry into undercover policing’.

⁹⁹ Malik 2016

¹⁰⁰ Aitchison and Blaustein 2013

Consultative forums play an important role in the local oversight of policing, providing opportunities for a range of individuals and groups to express their views directly to local police commanders. However, such forums raise important questions about the representativeness of the participants of the wider community and the mandate they have to speak on behalf of different sections of the local population. To be effective, consultative forums must also engage with local police commanders who have sufficient organisational autonomy to be able to respond to requests of the participants.

Whether participants in oversight bodies are elected or selected, it is important that, in accordance with Principle 2, that they are independent of police organisations if they are to command the trust and confidence of citizens.

Principle 10: 'Recognition' and 'Reason'

Underpinning the importance of participation are two related principles that are key to the democratic oversight of policing: 'recognition' and 'reason'¹⁰¹. Recognition is based on the notion that the state should foster routine democratic deliberation among all those affected by its decisions about security problems so there need to be participatory spaces for public conversations in which different voices can express themselves and be heard which will bring benefits of both legitimacy (by allowing different constituencies are listened to) and effectiveness (by improving the knowledge base on which decision are taken).

The principle of reason (or more specifically public reason) is closely allied to that of recognition. It demands that claims made in public deliberation are questioned, scrutinized, defended and revised in ways which align with idea of security as a public good. The aim is to ensure that unreasoned claims lacking a base in evidence for particular levels of policing provision are not treated as immutable facts of political life but are subject to democratic scrutiny¹⁰².

Case study: As a result of the restructuring of police governance in England and Wales and the mergers of Scotland's eight police forces to create a national police service very different forms of police accountability have been established. In England and Wales, the 2011 Police Reform and Social Responsibility Act introduced directly elected Police and Crime Commissioners with the power to set objectives and budgets and hire and fire chief constables. In Scotland, the 2012 Police and Fire Reform

¹⁰¹ Loader and Walker

¹⁰² Loader and Walker, p.229 As Loader and Walker observe, 'Such practices of inclusive and reflexive public reasoning and justification at least maximise the prospect of political communities thinking about security ... in ways which foster greater acknowledgement of mutual vulnerabilities and social connectedness that exist among their members'. (230-231).

(Scotland) Act a new national body, the Scottish Police Authority, has been established with a selected rather than elected membership appointed on the basis of possessing skills and expertise relevant to the functions of the SPA. At a local authority level there are local scrutiny and engagement groups made up of local councillors which have no formal powers but liaise with the local commander around the preparation of the local policing plan.

Part D: Evidence and Evaluation

Principle 11 Commit to Robust Evidence and Independent Evaluation

The deliberations of oversight bodies need to be informed by robust evidence and rigorous, independent evaluation of policing. Following Sherman, police organisations should use the results of rigorous evaluations of policing tactics and strategies to guide decision-making; second, they should generate and apply analytical knowledge derived from a police data on a range of issues, from crime problems to trust and public confidence.¹⁰³

Both the practices of policing and the *Principles for Accountable Policing* set out in this document should be considered as ‘testable hypotheses’. Their assessment should not be based on ‘hunches’ or ‘gut feelings’ but subject to independent evaluation of ‘what works’ and ‘what doesn’t work’. Evaluation will allow assessment of the extent to which individual principles have been implemented and whether this has led to expected or unanticipated outcomes. It will also allow assessment of the influence of context on the effectiveness of *The Principles*, for example, in relation to the impact of pre-existing institutional structures, norms, values and relationships.

Case study: The Violence Reduction Unit (VRU) was established in 2005 by Strathclyde Police to target all forms of violent behaviour but with a particular focus on gang violence and knife crime in Glasgow. Informed by research evidence, the approach of VRU marked a significant departure from a traditional law enforcement centred strategy and instead adopted a public health approach with the police working with multiple agencies in health, education and social work. This was exemplified by the VRU’s Community Initiative to Reduce Violence (CIRV) which focused on the diversion of young people away from gang activity by deploying evidence-based interventions relating to parenting, health, careers and social behaviour. Independent evaluation of VRU and CIRV has highlighted its contribution to reduced levels of knife crime in Glasgow and led to the adoption of some of its initiatives in the UK and internationally.

¹⁰³ Sherman, L. (1998) *Evidence-based Policing*, Police Foundation: Washington DC.

Principle 12 Be a Learning Organisation

Oversight bodies and the police need to be learning organisations. This means that they are skilled in creating, acquiring and transferring knowledge, and modifying their behaviour to reflect new knowledge and insights. There is active management of the knowledge process and that subsequent learning translates into new ways of operating.¹⁰⁴ Evaluation can thus contribute to a 'cycle of enlightenment' with regard to the *Principles* in which those with responsibility for evaluation learn how stakeholders make sense of their situation and then use this knowledge to 'teach' stakeholders how accountability is working or not working and then modify structures, processes and behaviours to address this. This focus on being a learning organisation therefore complements and reinforces Principle 6 regarding the need for constructive engagement and a process in which lessons are learned and acted upon rather than simply identified and then subsequently ignored.

Case Study: The What Works Centre for Crime Reduction (WWCCR) was established in 2013 and is based in the UK College of Policing. The WWCCR has been supported by a consortium of 8 UK universities who have carried out systematic reviews of crime reduction topics, developed an online toolkit to improve police practitioner access to and understanding of research on the impacts of different interventions to reduce crime, and the design and delivery of a training programme for police officers on how to use the toolkit to inform their decision-making. The toolkit encourages police practitioners to engage with research evidence, apply the knowledge gained about the effectiveness of different interventions, and then undertake an evaluation of the local impact of crime reduction initiatives. The crime reduction toolkit is available on the College of Policing Website.¹⁰⁵

¹⁰⁴ Garvin, D. (1993) Building a Learning Organisation, Harvard Business Review, 71 (4), 78-91.

¹⁰⁵ See

<https://whatworks.college.police.uk/toolkit/Pages/Welcome.aspx>

EXPLANATORY GUIDANCE ON PRINCIPLES FOR ACCOUNTABLE POLICING

Abstract

The nature of policing, the powers and privileges it endows upon its agents and the extent to which it impacts on the lives, liberties and livelihoods of the communities in which it takes place, makes accountability more elemental than some qualitative performance measures or governance processes for other public bodies. Accountability is an essential, delineating feature of policing the limits of which validate and licence the police themselves. In other words, the accountability of the police is central to their legitimacy within their communities. The concept of accountable policing therefore apprehends a range of features of democratic public service incorporating staples of good governance such as legal compliance, regulatory standards, transparency of decision-making and fiscal probity, together with more sensitive and complex areas such as the appropriate machinery for addressing misconduct, the position of the sworn constable at common law and the constant tension between upholding the law and rights of citizens with proportionality, openness and restraint and the necessary activities that involves. All are connected in one way or another to the notion of policing accountability. One of the challenges in collating a set of principles then has been that very interrelatedness. What follows is the product of the workshops and input of the Group; it is necessarily selective and inevitably subjective in parts but the Group has drawn upon its significant collective experience in order to distill a set of guiding principles to help assess and adjust the extent to which their police are truly accountable.

Introduction to accountable policing

When considering the accountability of critical public services - and more particularly, that of their key decision makers - there can be a tendency to do so solely from the vantage point of governance and therefore of the governors. The approach adopted by the Group was at times to invert this top-down approach and to review the concept of accountability and its component parts from the perspective of the user, the citizenry who are the intended beneficiaries of policing services. Arguably accountability in any elemental service on which a democratic society depends can *only* meaningfully be judged from the perspective of those in whose name any holding to account is done, *a fortiori* where that service incorporates coercive powers and legitimises the use of force against citizens. However, it is important to clarify at the outset the subtleties of definition: we are concerned here with more than the police-as law-enforcement approach; we are concerned with accountable *policing*, a descriptor that applies to services that include, but also extend beyond, the enforcement of the law.

* Fraser Sampson LL.B (Hons), LL.M., MBA., Solicitor, Hon Professor Sheffield Hallam University

There are many definitions of, and more approaches to, accountability in policing than there is room for here. The literature on the accountability of the police generally, and that of UK police forces and mechanisms in particular, forms a rich and deep seam albeit often found running through sociological, criminological, historical and jurisprudential strata (Reith 1952; Stenning 1995; Simey 1988; Uglow 1988; Reiner 1992, 2000; Goldsmith 1991; Waddington 1993,1999; Morgan 1989a, 1989b; Oliver 1997; Loader 2000, 2016; Bovens 2005; Walker and Archbold 2014; Lister and Rowe 2016). Traditional approaches combine – and sometimes conflate – functions of governance, regulation and oversight making the identification of principles as opposed to ‘rules’ more practicable. Nevertheless, differentiated approaches notwithstanding, the police and policing are – irrespective of jurisdictional differences, subject to a framework of laws, international and domestic, which can be enforced by citizens against the relevant body, the relevant State and/or the relevant individual.

Throughout the principles that follow is the accountability paradox that policing brings: the fact that preventing harm and enforcing the law will sometimes require the use of coercive power and covert practice which conflicts with individual rights and freedoms of the citizen (Kleinig 1996; Bowling 2007). Policing accountability – which goes far wider than what one commentator calls their monopoly on legitimate violence (Loader 2000) - is concerned with ensuring the appropriate balance in the equation and that unnecessary or unacceptable harm is effectively, lawfully and transparently addressed. Failure to achieve demonstrable accountability, to the law and to the populace, can lead to the undermining of public confidence and the erosion of legitimacy (Stanko 2009; Jackson *et al* 2011)

Among the voluminous literature that has grown up around policing accountability are numerous reports and official publications evincing the evolution of democratic policing. Among them is one report that offers a reliable and pragmatic structure for approaching the subject across the jurisdictions represented on the Group. The Report of The Independent Commission on Policing for Northern Ireland (the Patten Commission) published in September 1999 not only tackles some of the intrinsic challenges of accountable policing in the context of Northern Ireland, but also lends itself to far wider application and has been described as providing “a blueprint for democratic policing anywhere in the world” (Ellison 2007). In approaching its task the Commission adopted two broad senses of policing accountability:

1. the “subordinate or obedient” sense – incorporating the applicability of the law and the jurisdiction of higher authorities and

2. the “explanatory and cooperative” sense - being answerable for what they do/fail to do and cooperating with the processes of inquiry (Marshall 1978)

This approach is apparent throughout the principles set out here.

Citing the Agreement of 10 April 1998 (the so-called Good Friday Agreement) the Commission stated¹⁰⁶:-

“[The parties] believe it essential that policing structures and arrangements are such that the police service is professional, effective and efficient, fair and impartial, free from partisan political control; accountable, both under the law for its actions and to the community it serves; representative of the society it polices, and operates within a coherent and cooperative criminal justice system, which conforms with human rights norms. [...] these structures and arrangements must be capable of maintaining law and order including responding effectively to crime and to any terrorist threat and to public order problems. A police service which cannot do so will fail to win public confidence and acceptance. [...] any such structures and arrangements should be capable of delivering a policing service, in constructive and inclusive partnerships with the community at all levels, and with the maximum delegation of authority and responsibility, consistent with the foregoing principles. These arrangements should be based on principles of protection of human rights and professional integrity and should be unambiguously accepted and actively supported by the entire community”

It is difficult to think of a more complete and compelling introduction to the subject of accountable policing.

International Framework

The starting point for the Principles is the international framework by which participating States have undertaken to uphold the fundamental rights and freedoms of their citizens, to set out the minimum standards for their policing bodies and to provide effective remedies and redress when they fall short of those standards. The major international legal instruments that create rights for citizens and policing obligations on their parent States are considered below.

While this framework and the standards it inculcates are drafted to address the activities of ‘law enforcement officers’ (LEO) the individual actions of whom are, of course, critical to aspects of accountability (see e.g. Reiner 1992; Holdaway 1984) the framework sits above both the individual actions of all officials carrying out policing functions (originally more about ‘peacekeeping than law enforcement – Banton 1964) and the more discursive proliferation of obligations and undertakings engaged by policing

¹⁰⁶ Para 1.9

in collaborations and partnerships. The European Code of Police Ethics¹⁰⁷ expressly recognises¹⁰⁸ that “most European police organisations – in addition to upholding the law – are performing social as well as service functions in society” while a College of Policing study published in 2015 indicated that non-crime related incidents account for 83% of all recorded incidents dealt with by the police in England and Wales. To this extent, to categorising policing as ‘law enforcement’ is like describing fire and rescue services as ‘fire extinguishers’.

Universal Declaration of Human Rights

Adopted by the United Nations General Assembly on 10 December 1948, the Declaration is in many ways the genesis of the international and domestic frameworks that have subsequently set the standards for policing accountability within the local jurisdictions of signatory States.

Article 29,

(1) Everyone has duties to the community in which alone the free and full development of his personality is possible.

(2) In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.

Paragraph (1) underscores a key element of the policing model within the UK and Ireland, namely the generic duties of citizens to their communities, a mutuality of accountability that is reflected in the so-called Peelian principles of policing (see Loader 2016)¹⁰⁹. Article 28 enshrines a right for people to be provided with social and international order in which to enjoy their broader fundamental rights, a further elemental entitlement sitting at the centre of accountable policing.

United Nations Code of Conduct for Law Enforcement Officials

The Code of Conduct for LEO was adopted by the general Assembly of the UN in 1979¹¹⁰, Art 1 of which states that:

Law enforcement officials shall at all times fulfil the duty imposed upon them by law, by serving the community and by protecting all persons against illegal acts, consistent with the high degree of responsibility required by their profession.

¹⁰⁷ European Code of Police Ethics *Adopted by the Committee of Ministers on 19 September 2001 at the 765th meeting of the Ministers’ Deputies*, Council of Europe Publishing F-67075 Strasbourg Cedex
March 2002

¹⁰⁸ At p.5

¹⁰⁹ and one that is corroborated by the common law duty for citizens to come to the assistance of a constable in England & Wales

¹¹⁰ General Assembly resolution 34/169 of 17 December 1979

The Commentary to art 1 defines ‘law enforcement officials’ as including all officers of the law who exercise police powers, especially the powers of arrest or detention and the subsequent Guidelines provide that “*The definition of law enforcement officials shall be given the widest possible interpretation*”¹¹¹. The developing role of non-sworn staff in delivering policing outcomes means that the concept of an LEO is too narrow a focus for true accountability and, even with the expansive wording of the Guidance, the Code itself requires teleological amendment in national instruments. The Code nevertheless underscores both the nature of law enforcement activities (which here include any such activity by the State’s armed forces) and the importance of conspicuously regulating the interface between those activities and the rights of citizens.

Article 2 expressly identifies an overarching obligation on law enforcement officials to respect and protect human dignity and maintain and uphold those human rights of all persons in the performance of their duty, while the Commentary goes on to identify and incorporate some particular rights enshrined within international instruments that LEO are under a duty to respect and protect. These are:

The Universal Declaration of Human Rights¹¹²

The International Covenant on Civil and Political Rights¹¹³

The Declaration on the Protection of All Persons from Being Subjected to Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment¹¹⁴

The Declaration on the Elimination of All Forms of Racial Discrimination¹¹⁵

The International Convention on the Suppression and Punishment of the Crime of Apartheid¹¹⁶

The Convention on the Prevention and Punishment of the Crime of Genocide¹¹⁷

The Standard Minimum Rules for the Treatment of Prisoners¹¹⁸

¹¹¹ Guidelines for the Effective Implementation of the Code of Conduct for Law Enforcement Officials, UN resolution 1989/61, May 24

¹¹² <https://www.un.org/en/universal-declaration-human-rights/index.html>

¹¹³ Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966 entry into force 23 March 1976, in accordance with Article 49

<https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx>

¹¹⁴ Adopted by General Assembly resolution 3452 (XXX) of 9 December 1975

<https://www.ohchr.org/EN/ProfessionalInterest/Pages/DeclarationTorture.aspx>

¹¹⁵ Adopted and opened for signature and ratification by General Assembly resolution 2106 (XX) of 21 December 1965

entry into force 4 January 1969, in accordance with Article 19

<https://www.ohchr.org/EN/ProfessionalInterest/Pages/CERD.aspx>

¹¹⁶ G.A. res. 3068 (XXVIII), 28 U.N. GAOR Supp. (No. 30) at 75, U.N. Doc. A/9030 (1974), 1015 U.N.T.S. 243, entered into force July 18, 1976

¹¹⁷ Approved and proposed for signature and ratification or accession by General Assembly resolution 260 A (III) of 9 December 1948 Entry into force: 12 January 1951, in accordance with article XIII

<https://www.ohchr.org/EN/ProfessionalInterest/Pages/CrimeOfGenocide.aspx>

The European Convention on Human Rights

The Convention for the Protection of Human Rights and Fundamental Freedoms, drawn up within the Council of Europe in 1950¹²⁰ is probably the most well-known instrument in the international framework. Often referred to as the European Convention on Human Rights this seminal post-WW2 undertaking by signatory States has been at the heart of some of the most important legal decisions and judgments around policing accountability in recent years. Rehearsing and reinforcing many of the rights and freedoms set out elsewhere in the framework *supra*, the Convention has provided an avenue of challenge and redress in a whole spectrum of policing activity from the use of lethal force, arrest and detention, the use of torture and inhumane treatment and the retention of DNA samples¹²¹. The provisions of the Convention are directly relevant to the Principles.

European Code of Police Ethics

This Code was adopted by the European Council in September 2001 and sets out in some detail a series of elements and features that should exist in an ethical policing service, for example the training of officers, the conduct of suspect interviews and the provision of assistance to victims of crime. The Code is highly relevant to several of the Principles and of particular relevance is para IV which provides:

12. The police shall be organised with a view to earning public respect as professional upholders of the law and providers of services to the public.
- ...
15. The police shall enjoy sufficient operational independence from other state bodies in carrying out its given police tasks, for which it should be fully accountable.
16. Police personnel, at all levels, shall be personally responsible and accountable for their own actions or omissions or for orders to subordinates.
17. The police organisation shall provide for a clear chain of command within the police. It should always be possible to determine which superior is ultimately responsible for the acts or omissions of police personnel.

¹¹⁸ Adopted by the First United Nations Congress on the Prevention of Crime and the Treatment of Offenders, held at Geneva in 1955, and approved by the Economic and Social Council by its resolutions 663 C (XXIV) of 31 July 1957 and 2076 (LXII) of 13 May 1977

¹¹⁹ Vienna on 24 April 1963. Entered into force on 19 March 1967. United Nations, Treaty Series, vol. 596, p. 261

http://legal.un.org/ilc/texts/instruments/english/conventions/9_2_1963.pdf

¹²⁰ signed on 4 November 1950

¹²¹ *Ireland v UK* [1978] ECHR 5310/71; *McCann & Ors v UK* [1995] ECHR 18984/91; *S & Marper v. United Kingdom* [2008] ECHR 1581.

18. The police shall be organised in a way that promotes good police/public relations and, where appropriate, effective co-operation with other agencies, local communities, non-governmental organisations and other representatives of the public, including ethnic minority groups.

19. Police organisations shall be ready to give objective information on their activities to the public, without disclosing confidential information. Professional guidelines for media contacts shall be established.

20. The police organisation shall contain efficient measures to ensure the integrity and proper performance of police staff, in particular to guarantee respect for individuals' fundamental rights and freedoms as enshrined, notably, in the European Convention on Human Rights.

21. Effective measures to prevent and combat police corruption shall be established in the police organisation at all levels.

The Code takes account of a significant amount of prior work on accountability including that of the European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (CPT), the principles within the European Social Charter with regard to the social and economic rights of police *personnel*, the European Commission against Racism and Intolerance (ECRI), the European Commission for Democracy through Law (Venice Commission) and the Declaration on the Police¹²². These are reflected in the Principles.

National framework

The international framework and the various individual rights nested within it are given further effect by a range of national instruments enacted by the relevant legislatures of the sovereign party States¹²³. These domestic regulations in the jurisdictions represented on the Group cover a very wide range of policing activities, from the use of force against people and their property, processing of citizens' biometric and other personal data to the management of covert human intelligence sources and the disclosure of material in advance of prosecution. These detailed measures in primary and secondary legislation are supported by codes of ethics and conduct in each of the jurisdictions considered by the Group¹²⁴ along with statutory and professional guidance emanating from such bodies as the National Police Chiefs' Council and the College of Policing.

¹²² Resolution 690 (1979) adopted by the Parliamentary Assembly of the Council of Europe in 1979

¹²³ The Human Rights Act 1998 being a good example

¹²⁴ <https://www.garda.ie/en/about-us/publications/policy-documents/code-of-ethics-english-1-5-18.pdf>; <https://www.scotland.police.uk/about-us/code-of-ethics-for-policing-in-scotland/>; https://www.college.police.uk/What-we-do/Ethics/Documents/Code_of_Ethics.pdf accessed 24 June 2019

In each of the police services within the Group’s jurisdiction police officers are required to attest or make a solemn declaration the wording of which expressly binds them to upholding the rights of citizens and to observing the standards of professional behaviour set out in some of the legislative instruments *supra*.

The existence and composition of these standards support the notion of the police *using* rather than merely enforcing the law (Waddington1999:94). The development of the legal frameworks, their application within communities and their interpretation by the courts has followed a sort of ‘constitutional titration’ by the legislative, executive and judicial arms of the State, an incremental process of trial and error in an effort to achieve an acceptable balance between the democratic answerability of policing and the independent application of professional discretion. The efficacy and impact of that process is well and richly documented in a vast volume of literature only a very small part of which can be rehearsed here. The Principles are set against the context of the framework and accompanied by some key references which are included to highlight the specific issues considered by the Group

Governance, Regulation and Oversight

Viewed from the vantage points of governance mechanisms, regulators and oversight bodies (Stenning 2009) policing accountability can become an unwieldy and amorphous concept¹²⁵. Using its best endeavours the Group created the Principles in a way that took account of these overlapping aspects. In doing so the Group heard from a number of invited experts in these three forms of accountability, beginning with Rick Muir who noted that police accountability can be grouped under three broad governance paradigms (Muir 2016):

- Bureaucracy
- Markets
- Democracy

Paradigm	Descriptor	Pros	Cons
Bureaucracy	Top-down hierarchical governance setting structures	Produces standardised solutions. Works for simple problems	Can be too rigid and unresponsive for complex challenges = demoralising for lower tier staff. Strategic decision makers too distant from issues/realities and <i>vice versa</i>

¹²⁵ A recent report that helpfully separates some of these component parts is *The Future of Policing in Ireland* September 2018 [http://policereform.ie/en/POLREF/The%20Future%20of%20Policing%20in%20Ireland\(web\).pdf/Files/The%20Future%20of%20Policing%20in%20Ireland\(web\).pdf](http://policereform.ie/en/POLREF/The%20Future%20of%20Policing%20in%20Ireland(web).pdf/Files/The%20Future%20of%20Policing%20in%20Ireland(web).pdf) accessed 10 June 2019

Market-based	Seeks to contract-out certain aspects of policing	<p>Creates a 'reputational' competition to drive efficiency</p> <p>Transfers risk associated with overhead and responsibility for maintaining stable resource base</p>	<p>Too much focus on market-based targets can affect public trust. Relies on assumption that people make rationally informed choices</p> <p>Funding arrangements can cause disconnect between local and national policing and blur lines of responsibility/accountability</p> <p>Contracts can be too rigid & costly to refine during life of agreement</p> <p>Who manages the contract can blur lines of operational irresponsibility/accountability – Chief Constable or local elected policing body?</p> <p>Affluent areas can pay for additional constables bringing role of the public police into question</p>
Democratic	Elected representatives on governance body	<p>Offers direct accountability through e.g. complaints or indirectly via electoral process, surgeries etc.</p> <p>Opportunities to unify other emergency services e.g. FRS</p>	<p>Appointed boards too far removed from public - directly elected commissioners might provide a necessary balance of power and encourage collective participation <i>but</i> risk of crude majoritarianism and politicisation¹²⁶</p> <p>Electoral cycle too long e.g. 4 years between Police and Crime Commissioner elections</p>

¹²⁶ see e.g. Sampson (2012); Neyroud (2013)

--	--	--	--

Table 1

The Group considered Muir’s input on how some of the complexities around implementing the various mechanisms of police accountability are highlighted by the following tensions and need to be resolved through a ‘balancing’ approach:

Silos vs Complexity: Complex problems require negotiated order; different agencies need to work together to produce common solutions.

Experts vs People: Public priorities often relate to very local issues affecting different communities not necessarily reflecting issues of wider importance such as hate crime, human trafficking etc.

Trust vs Deference: There is a trend towards risk aversion. There is a need to manage public expectations and adopt a realistic approach to tolerating risk – bad things may and can happen.

Accountability vs Innovation: Too much accountability has a tendency to stifle progress and originality in processes.

Measurement vs Obscurity: The management aphorism what gets measured gets done demands a more holistic approach to what is measured.

Policy vs Practice: Policy is being made daily; through implementation it can change and affect practice. Sometimes it can be difficult to identify whether there is a relevant policy in action and, if so, who bears responsibility for that policy.

Next the Group considered accountability from the perspective of *regulation* of looking at lessons from the financial and charitable sectors. In this context Franklin Ngwu presented the three basic forms of regulatory accountability:

- Systemic: Top down using hierarchical sets of rules
- Prudential: Bottom-up supervision of the sector and
- Conduct of business: Regulation of how institutions conduct their business.

The Group heard how proper mechanisms of regulation can increase confidence in the sector and its institutions, that there is a need to ensure regulators themselves understand what they are supposed to do and that they have proper training to carry out their duties. There is also a need for an all-inclusive, robust regulation mechanism as a proliferation of

light touch regulatory models can have an adverse effect on the overall effectiveness.

The limitations of regulation were noted, such limitation including:

- The Government 'safety net' particularly if organisations are considered too big or too important to fail.
- Political considerations make regulation complex.
- 'Agency capture' whereby those regulating come from the same background as those who are being regulated tend to take a sympathetic approach.

The Group also heard from Emeritus Professor Gareth Morgan of Sheffield Hallam University on the regulatory issues within the charitable sector (Morgan 2016). They noted how the relationship between regulated and regulatory needs to be clearly explained and how, paradoxically, *too much* regulation can affect reputation and public confidence. Professor Morgan indicated the many layers of governance and accountability and opined that charities regulation is an over-populated field.

It was agreed that clearly defined targets for regulation are needed, selectively based on what is worthy of having a target. It was noted how Minister's priorities can often lead to reluctance in the implementation of regulatory policies and how a *constitutional purpose* for the public police may aid in accountability in the same way as the 'charity model' where the accountability is focused on whether the bodies are serving their *purpose*. The Group noted how, in certain regulatory sectors, those who are regulated make financial contributions to a regulatory authority such as the FRSB or health and social care; this has the tendency to change the dynamic between a regulatory authority and a regulated body. The Group were clear that *purpose* should not be just about 'straplines' as these are open to interpretation; the question would be how all styles of policing could be justified in relation to community well-being and the accountability focus should include cost-effective ways of achieving the purpose part of which would involve delivering Best Value and thus require partnership working between different agencies.

The Group accepted the inherent difficulty of defining a single role /purpose of the police who are the first and last resort in most circumstances that require an immediate response and accepted that inevitably the purpose of the public police would remain broad, postulating that an ideal situation might be that emergency services are restructured in such a way that when a member of the public makes a call, the nearest service responds. Ultimately however, policing needs to be accessible and transparent.

Finally, the Group considered accountability and governance in health and social care, noting the following features:

- Healthcare is the responsibility of Westminster and devolved administrations (not local government)
- It is a highly complex and closely regulated environment similar to policing
- The medical profession also has a political influence and can affect discourses (for instance junior doctors' strikes).
- Social care is the responsibility of the local government and is funded by both public and private sector
- Accountability generally means answerability to external to organisations both horizontally and vertically. Governance is more about internal processes and procedures but also includes internal accountability (Wakefield and Fleming 2009) for things such as financial probity and administrative regularity.

One central feature in the comparative context of health and social care was the important role for lay people and it was noted that patients have a right to be involved in discussions affecting clinical care. For example the Scottish Medicines consortium includes lay people who serve on their committees. While the police engage with communities often it is not for the purposes of operational decision-making and the group were clear that this needed to change, accepting as it did that lay people are well equipped to ask questions about operational decision making just as they are about medical treatment and intervention. The Group queried but remained undecided as to whether true accountability is possible without sanctions.

They were clear however that Ombudsmen should come from a lay, non-professional background with access to expert advice to focus on the substance decisions.

Other cross-sectoral similarities were seen in staffing matters such as low morale owing to austerity and capacity, the evidence-based correlation between public satisfaction and job satisfaction and the need for significant steps to be taken to increase the involvement of staff in partnerships.

Lines of accountability – vertical and horizontal – were considered thus:

- Electoral: Ministers and councillors are accountable through the electorate.
- Scrutiny: Health and Care Scrutiny Committees, public scrutiny in Parliament, local authorities, Audit bodies, Ombudsman, user bodies and community health wards.
- Managerial: Performance management and KPIs.

- Contractual: Commissioning and monitoring between public bodies and independent sector.
- Regulation: Standards-based inspections with or without powers of enforcement.

The Group stressed the importance of highlighting examples of successful intervention and acknowledged the tests of these accountability mechanisms to be:

- What are the processes of external-internal and horizontal-vertical accountability?
- What role should the non-executives play? What is the proper role for lay people?
- Is the focus on improvement?

At the same time, expectations should be defined in advance, linked to outcomes, close staff engagement helps to promote effectiveness and sustainability and avoid perverse, defensive behaviour, while oversight should be manifestly constructive.

The Principles

Principle 1: Universality – all policing must be accountable

The Group began the compilation of the Principles by agreeing the need for universality. For policing to be truly accountable the Principles ought to be evident across the whole spectrum of policing activity including statutory undertakers having national policing functions (such as British Transport Police and the Civil Nuclear Constabulary), national agencies like the National Crime Agency and also the regulators and auditors of those bodies such as HM Inspectorate of Constabulary, Fire and Rescue Services. It was thought that these different agencies are competing with each other in various jurisdictions and there are no clear lines of accountability between what Loader calls Policing Above Government, Below Government and Beyond Government (Loader 2000). It was recognised that the mechanisms for accountability – particularly local accountability - would be more complex than those envisaged for conventional geographically-defined police services. However the importance of clarity in articulation of policy, particularly in terms of the nature and scope of national agencies, was critical if complete accountability of *policing* was to be achieved.

The distinction between the lines and levers of accountability as between the police and their *governance* bodies (police authorities, board, elected commissioners etc.) and those operated by independent police complaints bodies (IPCB) such as ombudsmen or complaints commissioners was noted. For example in the latter the requirements

for other principles such as independence (*infra*) are more acute. However, the Principle of universality provides that *all* relevant manifestations of policing should be potentially within the jurisdictional reach of the relevant IPCB. This Principle is needed if the others are not to be circumvented by off-shoring policing functions and putting the decision makers and actors beyond the ordinary levers of accountability. Universality therefore extends the Principles' applicability to those carrying out policing activities under contract. This element is entirely consistent with the development of legislation, for example, around the law in England & Wales needed to bring the conduct of non-police employees such as private custody staff under the jurisdiction of the Independent Police Complaints Commission¹²⁷; it also reflects the approach of the Human Rights Act 1988 which extends the justiciability of protected rights and freedoms to private delivery of some public services¹²⁸ and which is, the group believed, particularly important as policing treads a seemingly 'inexorable path' (Dupont, 2003: 43) towards 'privatisation' (Jones & Newburn 1998; Mulone 2016).

In inculcating this Principle the positive benefits of scrutiny and oversight need to be highlighted. Asymmetries in accountability of national level security and enforcement bodies and the police means there is a governance and accountability gap and the Group believed that comprehensive principles of accountability can help establish a common ethos that is currently absent.

The Principle also extends to technical developments such as the use of security drones, body worn cameras and the consequences of decisions to deploy them as they bring new interfaces of accountability (Doyle, 2003)

Principle 2: Independence

The Principle of independence raises questions of governance, oversight and operational discretion. Independence of the police from other State agencies and from political interference is a recurrent theme throughout the international legal framework. The Group were clear that those bodies responsible for holding the police to account must be sufficiently distinct from policing to enhance public trust and confidence in them. Independence is also a key feature of some of the other Principles particularly those relating to the regulation of conduct and also the legal safeguards around operational discretion.

¹²⁷ **THE INDEPENDENT POLICE COMPLAINTS COMMISSION (COMPLAINTS AND MISCONDUCT) (CONTRACTORS) REGULATIONS 2015 (SI 41/22015)**

¹²⁸ s.6 which extends the Act's provisions to persons 'certain of whose functions are of a public nature' - see *Yarls Wood Immigration Ltd. & Ors v Bedfordshire Police Authority* [2009] EWCA Civ 1110

The Group agreed that governance and accountability should not be reliant solely on mutual trust and confidence, believing that formal mechanisms should be strong enough to withstand overreliance on relationships and personalities (particularly relevant in models such as the police and crime commissioners in England and Wales where the elected body and the chief constable are corporations sole¹²⁹. Where police complaints and misconduct matters are engaged the existence of an Independent Police Complaints Body (IPCB)¹³⁰ was felt to be essential.

In terms of governance arrangements the Group saw tension arising in relation to the appointments of board members and queried the extent to which these ought to be Ministerial or Parliamentary appointments. It was noted how, in NI, the Republic of Ireland and Scotland board members on police authorities are appointed by ministers while the Chair is also likely to have their own preferences “rubber stamped” by the Minister. While this element of sign-off is a necessary consequence of wider RACI¹³¹ models applicable within public bodies generally, *quaere* the effect that this link with the executive administration may have on the public perception of independence. Moreover, where the accountability is exercised by an IPCB, the recommended model is for each police ombudsman or complaints commissioner to be appointed by and answerable to a legislative assembly or a committee of elected representatives that does not have express responsibilities for the delivery of policing services.¹³² More specifically, if a board member has a specialist background, there is a risk of generating tensions between the board and the executive, particularly if the board members become intrusive in the day-to-day functioning of the executive; people bringing their own perspectives can skew the governance and oversight. Further, in terms of board composition, it was agreed that members with political knowledge or ex-police officers may be justified in certain cases where they complement the knowledge requirements of a given area but whether it is reasonable – or even possible - to expect people who are inherently partial or partisan to act impartially while serving on a board was left undetermined.

Insofar as democratic governance arrangements are concerned, the Group noted that they can offer direct accountability through, for example, elected police and crime commissioners through the electoral process although there is a risk of partisan politicization (see Table 1). It is important to note the distinction between democratic accountability

¹²⁹ Police Reform and Social Responsibility Act 2011, s.1 and sched 2

¹³⁰ the definition used in the Opinion of the European Human Rights Commissioner Concerning Independent and Effective Determination of Complaints Against the Police 12 March 2009 CommDH (2009)4

¹³¹ an accepted model whereby roles are identified within a decision-making process as being Responsible, Accountable, Consulted, Informed

¹³² Opinion of the Human Rights Commissioner *loc cit*

and simple *electoral* accountability and the Group noted the fact that, while in the initial police and crime commissioner (PCC) elections in England and Wales in 2012 the second preference¹³³ vote mostly went to independent candidates not representing a particular political persuasion, these were all but wiped out in the second election cycle some three years later¹³⁴. Although the Police Reform and Social Responsibility Act 2011 and secondary legislation¹³⁵ expressly provides for the locally elected policing bodies and their constabularies to be separate legal entities with distinct areas of responsibility, the local bodies rely on their police forces for functional staples such as ICT systems, HR and payroll with many sharing offices in the police headquarters. The Group noted how such dependencies in an IPCB would offend fatally against this Principle but, even after considering cross-sectoral accountability, did not go so far as some in suggesting a model oversight agency to ensure accountability across all public services by use of investigative, executive and prosecutorial powers (Prenzler & Faulkner 2010: 259).

Principle 3: Compellability

It is axiomatic that, if an accountability body is to discharge its functions effectively it will need access to the relevant information, data sets, individuals and other sources of evidence; it will also need to have some *original* (as opposed to derivative) legal authority to act. The Group agreed that uncontested policing can lead to insufficient governance and accountability and increase the likelihood of scandal. Therefore any governance and accountability regime must have the capacity, capability, authority and opportunity to interrupt, interrogate and, if necessary, compel. Such a participative approach raised further questions as to the composition of the participants, their backgrounds and skills but the Group were clear that there needs to be an element of *compellability* in any effective oversight arrangements.

While there are practical arrangements in place for governance bodies such as police authorities and PCCs to require access to policing information these will necessarily be subject to wider considerations of public interest, operational sensitivity and the legitimate expectations of those providing the original data. There are also clear powers available to oversight bodies such as the Independent Office for Police Conduct (IOPC), the PIRC and the Office of the Police Ombudsman for Northern Ireland by which to obtain – if necessary by compulsion – relevant information from the police. However, compulsion ought to be a measure of last resort, the need for which arises in inverse proportion to

¹³³ the elections used a preferential voting system

¹³⁴ The electoral response to mainstream parties post Brexit experience will be interesting in May 2020 when the PCCs are elected for a third time.

¹³⁵ See the Policing Protocol Order 2011 (SI 2011/2744)

the existence of transparency - one of the hallmarks of true accountability (Principle 8).

Principle 4: Enforceability and redress

Accountability bodies must be able to effect change which means they require powers of redress. This element of accountability was neatly described by Congressman Kucinich in the context of the Patten Commission's report as "*something that tolerates the calling of where the system falls short*"¹³⁶.

Given the different types of policing accountability that might arise – local and central (see Godfrey, 2007) – together with the different types of body exercising the relevant functions, the Group believed that it was appropriate for different oversight bodies to have different powers. For example a PCC in England & Wales has statutory powers to suspend the chief constable and even to require them to retire or resign in the interests of efficiency and effectiveness. Such powers are consistent with the function of quasi-employer that sits with these local elected policing bodies and they are subject both to the professional opinion of HMICFRS and the supervision of the High Court which has been prepared to intervene in cases where the elected official has acted unlawfully¹³⁷. There are also powers to bring the relevant chief officer before a misconduct hearing and to implement any sanctions determined by the panel. These are very different from the investigative powers of IPCBs which are enacted in the various jurisdictions under consideration in order to meet the requirements of the international legal framework and, in particular, those elements that are essential components of 'effective investigation (see Conduct).

The Group saw this Principle as bringing with it a correlative need for capacity and autonomy, partly on the basis of independence as set out *supra*, but also as a result of pragmatism. In order to be equipped to pursue enforcement and redress the relevant accountability body must have adequate training to enhance its capability, supported by sufficient capacity to undertake its functions; it must also offer procedural justice (see Sunshine & Tyler 2003). The Group believed that current arrangements tend towards too great a focus on national strategy and not enough attention on training and capacity of local bodies and observed that there is very limited resource deployment locally under this head.

¹³⁶ Open Meeting before the House of Representatives sub committee on international operations and human rights Friday 24 Sept 1999 Serial No. 106-103, p.33

¹³⁷ *R (on the application of Rhodes) v Police and Crime Commissioner for Lincolnshire* [2013] EWHC 1009 (Admin);
R (on the application of Crompton) v Police and Crime Commissioner for South Yorkshire[2017] EWHC 1349 (Admin);

Principle 5: Legality

Much of the foregoing addresses this fundamental Principle. The policing organisations considered here are creatures of the law and must operate within the legal frameworks discussed in the Introduction. The European Code of Police Ethics identifies how this principle flows in two directions:¹³⁸

“The police objective of upholding the rule of law encompasses two distinct but interrelated duties: the duty of upholding the properly enacted and constituted law of the state, including securing a general condition of public tranquillity, and the related duty of keeping strictly within prescribed powers, abstaining from arbitrary action and respecting the individual rights and freedoms of members of the public.”

Overlapping with and underpinning many of the other Principles, this first aspect of the legality principle is focused partly on performance, effectiveness and efficiency. As such it is more allied with what have previously been discussed as governance-type accountability. In actions against the relevant policing bodies – including the governance bodies if appropriate - there may be a range of legal redress available under the international framework and its domestic enactments under this principle – common topical examples would include alleged cases of unlawful interference with a citizen’s right to private life by the police misusing CCTV, collating and retaining surveillance data, accessing and processing social media files etc.

The Code goes on to identify the second aspect of legality:-

“Above all, the rule of law requires that those who make, adjudicate and apply the law should be subject to that same law. In other words, the police should be subject to the self-same law that they apply and uphold. It is the mark of the police in a fully-fledged and mature democracy that they bind and subject themselves to the very law that they are pledged to uphold.”

This part is concerned primarily with the areas engaged by oversight and regulation, those falling within the jurisdiction of IPCB and the Principles under Conduct (*infra*). It is important to note that there is, within the jurisdictions considered by the Group, no equivalent of ‘Law Enforcement Officers’ Bills of Rights’ such as exist in a number of States in the USA (Keenan & Walker, 2005) and the law applies to police personnel in the same way as it does to anyone else. In short this Principle apprehends the levels of accountability (democratic, personal and criminal) identified by the House of Representatives sub committee on international operations and human rights in 1999¹³⁹ which leads neatly into the next Section.

¹³⁸ P.18

¹³⁹ *loc cit.*

CONDUCT

“The police role in upholding and safeguarding the rule of law is so important that the condition of a democracy can often be determined just by examining the conduct of its police.”¹⁴⁰

This is a powerful excerpt. The conduct of the police - and the extent to which that conduct is overseen, investigated and its actors answerable - is probably the touchstone of accountability in the mind of the citizen. It was the experience of the Group that people do not complain if they are insufficiently aware of what merits a legitimate complaint or if they believe that to make such a complaint is futile. To this end the international legal framework identifies 5 principles of effective investigation of complaints against the police¹⁴¹ (see Smith 2010):

- **Independence:** there should not be institutional or hierarchical connections between the investigators and the officer complained against and there should be practical independence;
- **Adequacy:** the investigation should be capable of gathering evidence to determine whether police behaviour complained of was unlawful and to identify and punish those responsible;
- **Promptness:** the investigation should be conducted promptly and in an expeditious manner in order to maintain confidence in the rule of law;
- **Public scrutiny:** procedures and decision-making should be open and transparent in order to ensure accountability; and
- **Victim involvement:** the complainant should be involved in the complaints process in order to safeguard his or her legitimate interests.

Principle 6: Constructiveness

Conduct is often the first point of reference for internal and external audiences when considering principles of policing accountability, with the focus invariably fixing on the complaints, powers-and-sanctions end of the continuum. The Group however believed that the pre-eminent feature of an effective accountability arrangement would be its *constructiveness*. All levels of accountability need to be constructive and there needs to be clarity of expectation on all sides (see Principle 7). The Group believed that this constructiveness needed to take account of the lessons from other regulated sectors, for example making it apparent why people should complain, why the time and effort were worth it and assigning sufficient resources to complaints (Morgan, 2016). It was felt that the Principles should help enhance confidence in policing, increasing engagement with the criminal justice system and encouraging people to

¹⁴⁰ European Code of Police Ethics at p.18

¹⁴¹ Human Rights Commissioner’s opinion concerning independent and effective determination of complaints against the police 2009

participate on the basis of trust, trust that someone will listen, that something will be done and that something will change. The Group queried whether the responsibility for conduct matters should therefore sit within the same functional area that deals with compliments and recognition. In any event it was clear that policing accountability should be enabling rather than disabling.

This approach is reflective of the European Police Oversight Principles¹⁴² drafted after the EPAC Annual Conference in Budapest, Hungary in 2006 by a working group to develop minimum standards for organisations involved in the *independent oversight* of policing. While the European principles' primary frame of reference is of that element of accountability concerned with effective mechanisms for addressing cases of alleged misconduct, they seek generally to promote the highest standards in policing and bring about¹⁴³:

- greater public confidence in policing;
- effective redress for those who are victims of police misconduct;
- greater openness and understanding of policing by citizens;
- greater respect for the law, policing and as a consequence reductions in criminality and disorder.

Principle 7: Clarity

For accountability to be effective the Group believed it required clarity about many things, starting with whose demands are being addressed i.e. the public, media, victims, families, politicians, etc., and addressing the question “accountable to whom?” (Adams, 2010: 234). The Group also believed that accountability systems and structures needed to be sufficiently comprehensive to address and balance different levels of demands from different stakeholders.

As has already been seen, accountability means different things to different people in different settings. The Group noted “a conflation of confusion between performance management and accountability”. Whether described as governance, oversight or regulation, the facets of accountability and the extent to which they constructively balance democratic answerability against the necessary direction-and-control freedoms of chief officers (Waddington, 1999) need to be clear – to everyone.

More specifically, there is a need for clarity in the notion of police “operational independence” and the remit of accountability bodies. Recently the High Court in England and Wales has made it clear that, not only are locally elected policing bodies permitted to hold their chief

¹⁴² The European Police Oversight Principles

<https://igp.gouvernement.lu/dam-assets/service/attribution/police-oversight-principles.pdf>

¹⁴³ para 1.1.2

officers to account over operational policing matters on behalf of their constituencies, they are *obliged* to do so¹⁴⁴. Debates about the legal parameters of operational independence are unlikely to provide the clarity required for accountability purposes and it seems much more practicable to adopt the approach of the Patten Commission¹⁴⁵ by focusing on operational *responsibility* and to explode once and for all the myth that the police are accountable solely to the courts which has its roots more in folklore than common law (see Stenning, 2011).

From a regulatory perspective the difference between a self-regulatory framework and a statutory regulatory framework needs to be defined clearly and the Principles should help create a shared clarity of understanding between public services about what accountability means.

Reflecting on the experience of other sectors the Group recognised that the growing emphasis on wellbeing and security within policing can detract from the core responsibilities and that clarity in identifying the respective roles and responsibilities of *all* the different stakeholders was a critical aspect of accountability.

Principle 8: Transparency

A cornerstone of responsive and responsible public service in democratic societies, this Principle was regarded by the Group as a *sine qua non* for accountable policing. Transparency includes the availability and ready accessibility of relevant information and data sets. In some ways it is the corollary of Principle 3 (Compellability). A good example of these two Principles in action can be seen in the report setting out a future for An Garda Síochána.¹⁴⁶ That report highlights how the Minister for Justice and Equality receives a large number of Parliamentary Questions about the police, often seeking substantial amounts of detailed information. The report notes that, “while it is right and proper that the Minister is questioned in the Oireachtas [Legislature] on matters relevant to the Department’s direct responsibilities”, the use of this mechanism to elicit routine information needed for holding the police to account is inefficient and unnecessary and that such information should be readily available directly from the police without resort to parliamentary procedures.¹⁴⁷

In describing this Principle the Group believed that there had been a discernible ‘declining faith in experts, shifting trends in the politics of crime coupled with a growing cynicism about politicians and elites’. This had led to low and unrepresentative attendance at police-public consultation forums (see Participation) but also a generally low level of available information. In contradistinction to their counterparts in the

¹⁴⁴ R (OTAO) *Crompton loc cit.*

¹⁴⁵ Report of The Independent Commission on Policing for Northern Ireland *loc cit.* para 6.19-6.20

¹⁴⁶ *The Future of Policing in Ireland* September 2018 *loc cit.*

¹⁴⁷ pp 40-41

USA, policing bodies in the UK have been reluctant to share datasets such as street level crime mapping (Sampson and Kinnear, 2010) and have an unedifying history in relation to data processing¹⁴⁸. While there is some evidence of this trend being incrementally reversed, this has been partly in response to legislation expressly requiring publication of governance data such as expenditure, contracts and personal interests and partly as a result of litigation by citizens.

Plainly there are aspects of policing where confidentiality is required, so too are there similar situations in the areas of health, education and social care and it was thought that there ought to be a presumption (rebuttable) in favour of disclosure. The Group also noted how disclosure can lead to a series of events and changes within policing such as stop and search practice (see e.g. Murray, 2014) that can aid governance and accountability.

It was recognised that performance data are acutely context dependant and simply being transparent about data without more would often not meet the rationale of this Principle. Changing the context can modify the criteria for interpreting and utilising data sets, for example management information, and there are many dependant variables when dealing with data that straddle the criminal justice system. Information solely based around e.g. crime statistics is dominated by the idiosyncrasies of governmental ‘counting rules’ and does not always account for or reflect ‘actual crime rates’ or take account of subtleties such as the differential impact of certain types of crime (e.g. vehicle theft) in rural and urban settings. The Group affirmed that holding accountability meetings in public and making reports available was not enough; transparency requires a clear understanding of what is being scrutinised. The absence of global transparency in this way can lead to the perception of “smoke and mirrors” sleight of hand by the police (Coliandris, Rogers & Gravelle, 2011:204) which undermines public confidence and participation.

PARTICIPATION

In terms of governance bodies it is difficult to achieve the right balance between experts and democratically elected representatives with the

¹⁴⁸ See *S & Marper v. United Kingdom* [2008] ECHR 1581 (police retention of DNA samples of individuals arrested but later acquitted); *R (on the application of GC & C) v. The Commissioner of Police of the Metropolis* [2011] UKSC 21 (successful challenge of policy indefinite retention of biometric samples);

“*Caught red handed: Why we can’t count on police recorded crime statistics*” Report of the Public Administration Select Committee 13th session 2013/14 HC 760, The Stationery Office, London; Report of HM Inspector of Constabulary into the reliability of crime recording data created and maintained by the police forces of England and Wales May 2014

<http://www.justiceinspectorates.gov.uk/hmic/programmes/crime-data-integrity/>; See also <http://www.telegraph.co.uk/news/uknews/crime/11117598/Criminals-could-appeal-after-Home-Office-admits-potentially-misleading-DNA-evidence-presented-to-juries.html>

perennial challenge that is always the ‘usual suspects’ who are elected or appointed with similar experiences, age and membership. Similarly, in a regulatory or oversight sense, there is a risk of ‘agency capture’ where those regulating come from the same background as those who are being regulated, producing a tendency to take a sympathetic approach. (Ngwu 2016). This homogeneity does nothing to reflect pluralism and diversity, can reinforce ‘groupthink’ (Janis 1982) and undermines public confidence. Mirroring Principle 2, the Principles that follow endeavour to take account of these tensions and challenges.

Principle 9: Pluralism and multi-level participation

If police accountability is for the public good then the public has to be engaged throughout the accountability processes. This truism was put at the heart of the following Principles by the Group; it is reinforced by the wider utilitarian observation within the European Code of Police Ethics: that policing is largely carried out in close cooperation with the public and police efficiency is dependent on public support.¹⁴⁹ This indivisibility between the police and their citizens is, of course, a quintessential ingredient of the policing models in the jurisdictions considered by the Group (Lustgarten, 1986; Uglow, 1988; Morgan, 1989a; Reiner, 1993; Oliver, 1997; Mawby, 1999; Loader, 2016)

There was recognition however that a degree of expertise was needed, supported by a skills matrix that highlights the most important skills and expertise; the institutional design of the relevant accountability body should reflect this.

Having regard to other sectors the Group considered how medicines consortia included lay people who serve on their committees. While noting that the police frequently engage with communities, the Group recognised that this was not for the purposes of operational decision-making and were clear that this needed to change, accepting as they did that lay people are well equipped to ask fundamental questions about operational decision making just as they are about medical treatment and intervention. Conventional public participation through surveys and local civil society infrastructure was found to be limited and not representative, either of the prevailing concerns within communities or of the people living with them, falling a long way short of the powerful concept of “Citizen Oversight” (Walker, 2000).

It was agreed that public consultation could be significantly improved through deliberative approaches, and through the use of digital and social media, although it was acknowledged that some barriers to public participation in policing policy were probably permanent. The difficulties in involving marginalised groups (Jones & Newburn, 2001)

¹⁴⁹ p23

and those who have come to the UK and Ireland from jurisdictions where the relationship with the police is fundamentally different were identified.

The Group also identified a mismatch between the rhetoric of wanting local people to be “involved in” decision making while, in reality, highly centralised processes and bodies were dominant concluding that, if local input is being promised, local people need to be listened to and recognising the ‘catharsis of co-production’ and its power in generating a community voice. However the Group accepted that public participation and consultation needs to yield concrete results, and that too often the police priorities remain the same even after consultation. Police officers and staff engaged in public consultation also need to be trained on how to hold a meeting, conduct consultation and give confidence to the public rather than dominating the agenda. That agenda, so approached, should evolve into the identification of community needs rather than priorities and true consultation can empower local citizens and allow local communities to take more ownership of their policing.

Principle 10: ‘Recognition’ and ‘Reason’

Building on elements in Principles 2 (Independence) 3 (Compellability) and 4 (Transparency) and the Group’s determination that uncontested policing is unaccountable policing, this Principle aims to facilitate ‘participatory space’ and inculcate authentic public scrutiny (*per* Loader and Walker¹⁵⁰). As such it raised further questions as to the composition of the participants, their backgrounds and skills. The strong element of ‘agency capture’ (*supra*) in current police governance arrangements was noted. In particular the fact that PIRC and HMICS both consist of experienced ex-police officers. The SPA is the only truly ‘civilian’ body but it too has ex-police officers serving on its board. It was noted that the scrutiny reviews carried out by HMICS carried more weight and influence in comparison to the reviews carried out by the SPA. While PIRC were undergoing a process to train people with a non-policing background to undertake investigations, it was accepted that this was a gradual process. It was also accepted that, to a certain extent, the efficacy of the *regulatory* or *oversight* arrangements required the ‘spine’ to be provided by those with policing knowledge and expertise as most investigations involve an understanding of the standard operating procedures (SOPs) and internal policies and regulations. The relevant legislation allows for a secondment of serving police officers to PIRC which it was noted can cause a potential conflict of interest and perception of bias, offending against Principle 2. The role of the Lord Advocate’s Office as having complete oversight prosecutions and investigations was recognised as adding an important extra dimension to policing oversight. By contrast the arrangements for the Police Service

¹⁵⁰ *loc cit.*

of Northern Ireland (PSNI) offer independent oversight through a combination of political and independent members and at the time of writing consideration was being given to recruiting former police officers from other countries to bring in policing expertise. The Group noted how agency capture also carries a risk of an oversight/regulatory body replicating police culture.

Nevertheless, the Group were of the view that agency capture can work if the process of investigation and oversight is transparent and that correct procedures are followed. In the health sector there is an element of lay involvement and at least two members of the public are involved at every stage, every inspection and investigation. However there needs to be a balance between experts and lay people and frameworks should be developed following consultation.

Another facet of this Principle is responsiveness; service delivery needs to reflect the views of the public thus:

- The Principles need to be contextual and need to be adapted and applied in different contexts to reflect the dynamic nature of policing.
- How people react to inspection and reports needs to be reviewed.
- Regulators need to be properly trained. Mere disclosure of information to fulfil a legal obligation is not sufficient - the 'regulators' need to be able to understand the information that is being presented.
- At the moment the different agencies within the criminal justice system seem to be working in silos; there needs to be an integrated approach as that is what the taxpayers are concerned with. Boundaries lead to gaps between problem identification and problem resolution. In NI, the Criminal Justice System Inspection provides that holistic oversight.
- There needs to be proactive regulation and clear rules of engagement between the police and the regulatory body with complete transparency.

IMPLEMENTATION AND EVALUATION

The Group concluded that deliberations of oversight bodies need to be informed by robust evidence and rigorous, independent evaluation of policing – in what is really an extension of evidence-based policing (Sherman 1998) and that policing must show that it proactively seeks learning opportunities in order to improve.

Principle 11: Commit to Robust Evidence and Independent Evaluation

The Group believed that, for it to be effective and reliable, any evaluation needs to be an independent analysis of 'what works' and 'what doesn't'.

This allows an assessment of the extent to which policies, practices and these Principles themselves have been implemented and whether this has led to expected or unanticipated outcomes. It will also allow assessment of the influence of context on the effectiveness of the *Principles*, for example, in relation to the impact of pre-existing institutional structures, norms, values and relationships. An example would be an evaluation of the effect of these Principles on public confidence (Goldsmith, 1991; Reiner, 1991) and on the answerability and responsiveness of complaints outcomes (Maguire, 1991).

The Group identified that this Principle encouraged greater emphasis on insight and learning rather than competition and performance, recognising that there was an urgent need to de-conflate performance management from accountability generally but particularly under this head. While performance review is about choosing what to do with resources, accountability review is about explaining and justifying those choices. It was also consonant with the wider view that this required review not 'inspection' and that all accountability reports should be shorn of adjectival biases, being based solely on evidenced fact.

In taking forward this Principle the political risk of an evidence-driven approach and the barriers to independent evaluation in public bodies generally should be noted (Rutter, 2012), such barriers include:

- Timeliness of research
- Suitability of issues to rigorous testing and policies often not being designed in a way that allows proper evaluation
- Lack of usable data.

But the most stubborn areas of resistance might be the 'demand barriers' (Rutter¹⁵¹) emanating from both incentives and culture among senior decision-makers.

Principle 12 Be a Learning Organisation

If a 'cycle of enlightenment' with regard to the Principles is to be attained then both oversight/regulatory bodies and the police themselves need to develop the skills to create, acquire and transfer knowledge, not just *inter se* but across and between partnerships and collaborations. The relevant organisations also need to be prepared to modify their behaviour in response to the relevant feedback, to reflect what has become known in light of the new evidence and to use these assets of new knowledge and insight to improve outcomes. This Principle requires embedded formal systems to ensure that lessons are learnt from incidents and errors systematically rather than from *ad hoc* reviews of single instances that attract critical attention.

The Group noted that being a learning organisation complements and reinforces Principle 6 and the corollary – being a closed and uninquiring

¹⁵¹ *ibid*

organisation - would damage public confidence. The Group also took account of the different approaches in other public services, particularly Defence in which 'lessons' are sub-divided into stimulation, identification and implementation (see Lloyd, 2005).

References

Adams, R. (2010). Police Corruption, Deviance, Accountability and Reform in Policing. *Policing – A Journal of Policy and Practice* Vol 4 No 4 pp. 322 – 325.

Banton, M (1964) *The Policeman in the Community*, London: Tavistock

Bovens, M. (2005). Public Accountability in Ferlie, E., Lynn, L.E. & Pollitt, C., *Oxford Handbook of Public Accountability*. (pp. 182-208). Oxford: Oxford University Press.

Bowling, B (2007) Fair and Effective Policing Methods: towards 'good enough' policing, *Scandinavian Studies in Criminology and Crime Prevention* Vol 8, sup 1 pp 17-32

Brown, J. Loader, I. Neyroud, P. and Muir, R. (2013). Independent Police Commission (2013), *Independent Police Commission; an independent enquiry focusing on the future of policing in England and Wales*, Available from www.independentpolicecommission.org.uk . Published on-line 25th November 2013. Accessed November 2014

Coliandris, G., Rogers, C. & Gravelle, J. (2011). Smoke and Mirrors, or a Real Attempt at Reform? *Policing – A Journal of Policy and Practice*, 5(3), pp. 199-209.

College of Policing *College of Policing analysis: estimating demand on the police service* (2015)

Doyle, A., (2003) "Arresting Images: Crime and Policing in Front of the Television Camera" University of Toronto Press, Toronto

Dupont, B. (2003). The New Face of Police Governance in Australia. *Journal of Australian Studies*, 27(78), 43-51

Ellison, G (2007) A Blueprint for Democratic Policing Anywhere in the World?: Police Reform, Political Transition, and Conflict Resolution in Northern Ireland
Police Quarterly 1 Sept Volume: 10 issue: 3, page(s): 243-269

Godfrey, J (2007) "Who is to Guard the Guards Themselves? A Contribution to the Current Debate on the Accountability of Policing", *Policing: A Journal of Policy and Practice*, Volume 1, Issue 4, 2007, Pages 495–500 Oxford University Press

Goldsmith, A. J. (1991). External Review and Self-Regulation. In Goldsmith (Ed.). *Complaints Against the Police: The Trend to External Review* pp. 13-61 Oxford University Press.

Holdaway, S. (1984) *Inside the British Police: A Force at Work*. Blackwell
Oxford

Jackson, J (2009) *Crime, Policing and Social Order; On the Expressive nature
of public confidence in policing*. British Journal of Sociology pp 493 – 521
Wiley LSE London

Jackson, J., Bradford, B., Stanko, E., & Hohl, K. (2011). Just Authority? Public
trust and police legitimacy Willan, Cullompton

Janis, I.L., (1982) *Groupthink* Wadsworth, Boston MA,

Jones, T., and Newburn, T., (2001) “Widening Access: Improving Police
Relations with Hard to Reach Groups” Police Research Series Paper 138
Home Office

Jones, T., & Newburn, T. (1998). Private Security and Public Policing
Clarendon Studies in Criminology, Oxford

Keenan, K., & Walker, S., (2005) Law Enforcement Officers Bills of Rights
(“LEOBORS”), Public Interest Law Journal vol. 14, pp 185-244.

Kleinig, J. (1996) *The Ethics of Policing* Cambridge University Press,
Cambridge

Lister, S and Rowe, M., (eds.) (2016) *Accountability of Policing* (Routledge
Frontiers of Criminal Justice) Routledge Oxford.

Lloyd, M (2005) *Lessons Identified; purpose and methodology* [Dstl] Ministry
of Defence paper #231 12 July
http://www.dodccrp.org/events/10th_ICCRTS/CD/presentations/231.pdf
accessed 12 June 2019

Loader, I. (2000). Plural Policing and Democratic Governance. *Social and
Legal
Studies*, 9(3), 323-345

Loader, I., (2016) In Search of Civic Policing: Recasting the ‘Peelian’ Principles
Crim Law and Philos (2016) 10:427–440

Lustgarten, L. (1986) *Governance of Police*. London: Sweet & Maxwell

Maguire, M. (1991). Complaints against the Police: The British Experience, in
Goldsmith, A. J., (Ed.), *Complaints Against the Police: The Trend to External
Review* (pp. 177-210). Oxford: Clarendon.

- Marshall, G., (1978) "Police Accountability revisited" in D. Butler and A.H. Halsey (eds) *Policing and Politics*, Macmillan, London 1978
- Mawby, R.I., (Ed.) 1999 *Policing Across the World: Issues for the Twenty-first Century* London: Routledge.
- Morgan, G., (2016) Sheffield Hallam University "*The State of UK Charity Regulation*" Presentation to Principles of Accountable Policing Group 11th and 12th February Scottish Universities Insight Institute
- Morgan, R. (1989a). *Policing by Consent: Legitimizing the Doctrine*. In: *Coming to Terms with Policing: Perspectives on Policy*. Eds. Morgan, R. and Smith, David J. London: Routledge.
- Morgan, R. (1989b). *Policing a Post-Modern Society*. *The Modern Law Review* November 1992; Vol. 55; No. 6 ;761.
- Muir, R., (2016) Police Foundation, Presentation to Principles of Accountable Policing Group 11th and 12th February Scottish Universities Insight Institute
- Mulone, M., (2016) *The Politics of Private Policing: No Force and No Legitimacy?*, in (ed.) *The Politics of Policing: Between Force and Legitimacy (Sociology of Crime, Law and Deviance, Volume 21)* Emerald Group Publishing Limited, pp.277 - 293
- Murray, K., (2014) *Stop and Search in Scotland: An Evaluation of Police Practice*, The Scottish Centre for Crime and Justice Research
https://www.sccjr.ac.uk/wp-content/uploads/2014/01/Stop_and_Search_in_Scotland1.pdf accessed 12 June 2019
- Newburn, T. (2008) "The future of policing." in Newburn, T (Ed.) *Handbook of Policing*,(pp. 824-840) Willan Publishing, Cullompton.
- Neyroud, P. (Ed) (2013) *Policing UK* Wittan Media, London Pp 24-27
- Ngwu, F., (2016) Glasgow Caledonian University, *The Financial Crisis and the Failure of External Regulators* Presentation to Principles of Accountable Policing Group 11th and 12th February Scottish Universities Insight Institute
- Oliver, I. (1997). *Police, Government and Accountability*. London: MacMillan.
- Prenzler, T. & Faulkner, N. (2010). *Towards a Model Public Sector Integrity Commission*. *The Australian Journal of Public Administration*, 69(3), 251-262
- Reiner, R. (1991). *Chief Constables; Bobbies, Bosses or Bureaucrats?* Oxford: Oxford University Press

- Reiner, R. (1992) *Policing a Post-Modern Society*. The Modern Law Review November 1992; Vol. 55; No. 6 ;761. Wiley
- Reiner, R. (1993). Police Accountability: Principles, Patterns and Practices, in Reiner, R., & Spencer, S., (Eds.). *Accountable Policing – Effectiveness, Empowerment and Equity* (pp. 1-23). London: Institute for Public Policy Research.
- Reiner, R. (2000). *The Politics of the Police*. Oxford: Oxford University Press.
- Reith, C (1952) *The Blind Eye of History: A Study of the Origins of the Present Police Era* (London: Faber).
- Rutter, J., (2012) *“Evidence and Evaluation in Policy Making; a problem of supply or demand?”* Institute for Government
https://www.instituteforgovernment.org.uk/sites/default/files/publications/evidence%20and%20evaluation%20in%20template_final_0.pdf accessed 13 June 2019
- Sampson, F & Kinnear, F (2010) *“Plotting Criminal Activity: Too True to be Good: Crime Mapping in the UK.”* Journal of Policing: Policy and Practice – Oxford University Press Vol 4 No. 1
- Sampson, F (2012) *“Hail to the Chief?: how far does the introduction of elected police commissioners herald a US-style of politicisation of policing for the UK?”* Journal of Policing: Policy and Practice – Oxford University Press Vol 6 No. 1 Pp 4 - 15
- Sampson, F., Lyle, A., *“Legal Considerations Relating to the Police Use of Social Media”* in Akhgar, B., Staniforth, A., Waddington, D (Eds) 2017, pp 171-188 in *Application of Social Media in Crisis Management: Advanced Sciences and Technologies for Security Applications*, Springer International Publishing, Switzerland
- Savage, S.P. (2007). *Police Reform: Forces for Change*. Oxford: Oxford University Press.
- Sherman, L. (1998) *Evidence-based Policing*, Police Foundation: Washington DC
- Simey, M. (1988). *Democracy Rediscovered: A Study in Police Accountability*. London: Pluto Press.
- Smith, G. (2010). *Every complaint matters: Human Rights Commissioner’s opinion concerning independent and effective determination of complaints*

against the police. *International Journal of Law, Crime and Justice*, 38, 59 – 74.

Stanko, E.A. & Bradford, B. (2009). Beyond Measuring 'How Good a Job' Police Are Doing: The MPS Model of Confidence in Policing. *Policing – A Journal of Policy and Practice*, 3(4), pp. 322-330. http://www.sccjr.ac.uk/wp-content/uploads/2009/12/Beyond_Measuring.pdf accessed 24 June 2019

Stenning, P. (Ed) (1995) *Accountability for Criminal Justice: selected essays* University of Toronto Press Toronto

Stenning, P. (2009) "*Governance and Accountability in a Plural Policing Environment – the story so far*" *Journal of Policing: Policy and Practice* – Oxford University Press Volume 3, Issue 1, 2009, Pages 22–33

Stenning, P. (2011) *Governance of the Police: Independence, Accountability and Interference* (2011 13 FLJ 241 - 267) <http://classic.austlii.edu.au/au/journals/FlinLawJl/2011/11.pdf> accessed 24 June 2019

Sunshine, J. & Tyler, T. (2003). The Role of Procedural Justice and Legitimacy in Shaping Public Support for Policing. *Law and Society Review*, 37(3), 513-47.

Uglow, S. (1988) *Policing Liberal Society* : Oxford University Press, Oxford.

Waddington, P.A.J. (1993) *Calling the Police; the interpretation of, and response to, calls from the public* Avebury

Waddington, P.A.J. (1999) *Policing Citizens*. UCL Press London

Walker, S. E., & Archbold, C. A., (2014) *The New World of Police Accountability* Sage Thousand Oaks, CA

Walker, S. (2000). *Police Accountability: The Role of Citizen Oversight*. Belmont: Wadsworth Professionalism in Policing Series.

References from Critical Analysis

Akhgar, B., Staniforth, A., Waddington, D (Eds) 2017, *Application of Social Media in Crisis Management: Advanced Sciences and Technologies for Security Applications*, Springer International Publishing, Switzerland

Arthurs, H.W., 1983 *Law and Learning: Report to the Social Sciences and Humanities Research Council of Canada by the Consultative Group on Research and Education in Law*, Information Division, Social Sciences and Humanities Research Council of Canada, Ottawa.

Babuta, A, 2017, "Big Data and Policing: An Assessment of Law Enforcement Requirements, Expectations and Priorities" 6 September, Royal United Services Institute.

Baburoglu, O.N. and Ravn, I. 1992 *Normative Action Research*. *Organization Studies* (13:1), pp. 19-34.

Belasen, A 2000 *"Leading the Organization"* State University of New York Press, Albany NY.

Bloom, B.S., (1956) *Taxonomy of Educational Objectives*, Longman, White Plains, NY.

Bransford, J.D., Brown, A.L., and Cocking, R.R. (Eds) 2000 *"How People Learn: Brain, Mind, Experience and School"*. National Academy Press, Washington DC.

Chynoweth, P., 2008 'Legal Research' in. Knight, A. & Ruddock, L. (eds.) *Advanced Research Methods in the Built Environment*, Wiley-Blackwell.

Duhon, B. 1998 *"It's All in Our Heads"* in *Inform* vol 12, no 8, pp 8-13 ISSN 0892-3876.

Feldman, D., *"The Nature of Legal Scholarship"* in *The Modern Law Review*, Vol 52, July 1989, pp497 - 518

Hart, H.L.A., 2003, *The Concept of Law*, Oxford University Press, Oxford.

Hermitage, P, Chief Constable 1998 Foreword in Sampson, F. *"Blackstone's Police Manuals"* Oxford University Press, Oxford.

Holsapple, C.W., and Joshi, K. D., 2002 *"Knowledge Management – A Threefold Framework"* in *The Information Society*, Taylor & Francis, Florence KY, pp 47-63.

Jost, G. & Bauer, M.W. 2003, *Organisational Learning by Resistance*, Institute of Social Psychology, London School of Economics.

Klein, D.A. (Ed) 1998 *The Strategic Management of Intellectual Capital* Butterworth-Heinemann, Woburn MA.

Langbroek, P., van den Bos, K., Thomas, S.M., Milo, M & van Rossum, W "Methodology of Legal Research: Challenges and Opportunities", Utrecht Law Review, Volume 13, Issue 3, 2017

Mann, T (ed), 2010, *Australian Law Dictionary*, Oxford University Press, Oxford

Rapoport, R. 1970 "Three Dilemmas of Action Research." Human Relations, 23 (6), 499- 513).

Sampson, F. "Blackstone's Police Manuals" 1998 Foreword by Hermitage, Oxford University Press, Oxford.

Riege, A. and Lindsay N. 2006, "Knowledge management in the public sector: stakeholder partnerships in the public policy development." Journal of Knowledge Management vol 10, no. 3 pp 24-39.

Tranfield D., Denyer, D & Smart, P.,. 2003 "Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review." British Journal of Management vol 14 pp 207-222.

Wang, C.L., & Ahmed, P.K., 2003, Organisational Learning: a Critical Review, *The Learning Organisation: an International Journal*, vol.10, no.1, pp. 8-17.