FP7-SEC-2011-284725

SURVEILLE

Surveillance: Ethical Issues, Legal Limitations, and Efficiency
Collaborative Project

SURVEILLE Deliverable 4.2: Paper on legal issues related to the use of surveillance data for profiling

Due date of deliverable: 30.04.2013
Actual submission date: 30.04.2013

Start date of project: 1.2.2012 Duration: 39 months

SURVEILLE Work Package number and lead: WP04 Prof. Martin Scheinin (EUI)

Author(s): Jonathan Andrew (EUI)

DRAFT: D4.2 Legal issues relating to use of Surveillance data for profiling

Introduction

This paper attempts a detailed elaboration of specific concerns with respect to profiling activities by law enforcement and the intelligence services as regards behavioural profiling of open source data from online social networking activity. It examines inductive methods used to discern preemptively actions in anticipation of committing a crime. Whilst surveillance of online behaviour undoubtedly raised many important questions that may be framed in the context of privacy-related issues connected to the processing of this data, parallel concerns that arise from its use to profile and sort citizens, discriminating based on the analysis of communication and association between different entities, also requires scrutiny. Without sufficient oversight, distinctions may arise made through arbitrary decision-making.

The conceptual approach adopted reflects an interest in examining the implications inherent to an ongoing shift in profiling activities on the part of those agencies concerned with tackling serious crime. While the focus of this report is primarily grounded in observations drawn from a broadly European context, the analysis also reflects upon experiences in North America where this appreciation may afford useful insight. This evaluation underscores the criticality of acknowledging the value of applying an eductive approach to the application of human rights principles in response to technological change.

Defining behavioural profiling and surveillance data

This paper chooses as its focus the surveillance of the individual, rather than other entities that may be subject to monitoring such as physical objects or locations.[1] While the terms 'personal surveillance' and 'mass surveillance' are widely articulated, the two designations are frequently employed without further elucidation. Here, 'personal surveillance' is taken to mean the surveillance of an identified person. In the past the use of the term 'mass

[1] Lyon describes surveillance as "[A]ny focused attention to personal details for the purposes of influence, management, or control. Thus in addition to those who may be 'suspects' (because of alleged offences), ordinary persons in everyday life – workers, consumers, citizens, travellers -- find that their personal data are of interest to others." *See* D. Lyon, Surveillance, Power, and Everyday Life, Oxford University Press, New York, 2007, p.1. The working definition provided by SURVEILLE's Description of Work describes surveillance as: "Targeted or systematic monitoring of persons, places, items, means of transport or flows of information, in order to detect specific, usually criminal, forms of conduct, or other hazards, and enable, typically, a preventive, protective or reactive response, or the collection of data for preparing such a response in the future." See FP7-SEC-2011-1 SURVEILLE - Surveillance: Ethical Issues, Legal Limitations, and Efficiency, Description of Work, 19 September 2012, p.5

surveillance' has reflected the surveillance of groups of people[2], and most commonly large groups.[3] Customary distinctions such as these warrant reappraisal where recent developments throw into question how we distinguish and attribute activity to either collectives or individuals, especially where online technologies may render this delineation increasingly indeterminate.[4]

Furthermore, varying definitions of the term 'profiling' exist, reflecting competing notions of a practice that may constitute a diverse range of activities directed toward developing and utilizing models that delineate different traits and characteristics of persons. Indeed, the conduct of profiling as an activity is not limited to the security sector, but may also be pursued in a broad range of contexts; both of a commercial and non-commercial nature, and by a gamut of public and private actors.[5] It is necessary at this juncture to make certain

---

[2] Of critical importance then as regards the use of predictive analytics is how we frame the notion of group characteristics - the term may potentially be interpreted in a wider sense than that which corresponds to a more determinate elucidation.
See UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 29 January 2007, A/HRC/4/26, p.7 at para. 38.
"In the view of the Special Rapporteur, data-mining initiatives based on broad terrorist profiles that include group characteristics such as religion and national origin may constitute a disproportionate and thus arbitrary interference with the right to privacy, guaranteed by article 17 of the International Covenant on Civil and Political Rights (ICCPR)." The ICCPR defines group only in the context of the "family" (Article 23) and "ethnic, religious or linguistic minorities" (Article 27). Article 26 of the ICCPR prohibits discrimination and outlines a non-exhaustive list of proscribed grounds for such treatment - including language, religion, political or other opinion (amongst other criteria), affirming that all persons "are equal before the law and are entitled without any discrimination to the equal protection of the law." Increasingly however 'group' may be interpreted more expansively. Thus, the point at issue is how in this particular context we are to determine the criteria for establishing which group characteristics might prove disproportionate in their application to distinguishable associations in the context of profiling.
[3] *See*, for example: Roger Clarke, Information Technology and Dataveillance, November 1987, Available at: http://www.rogerclarke.com/DV/CACM88.html, Accessed: 19 January 2013.
[4] The somewhat nebulous and indefinite nature of certain association evolving through the discourse enabled by online social networks is discussed in more depth by Glassman in 'Occupying the Noosystem: The Evolution of Media Platforms and Webs of Community Protest'. *See* M. Glassman, Occupying the Noosystem: The Evolution of Media Platforms and Webs of Community Protest, Berkeley Planning Journal, 25(1), 2012, Available at: http://www.escholarship.org/uc/item/5ws9b7f5, Accessed: 19 January 2013.
[5] Accenture reported in early 2013 that the demand for predictive analytics vastly exceeds the supply, noting that in the public and private sectors: "[M]ore than twice as many organizations reporting that analytics is being used as a primarily predictive tool today than in 2009. *See* Accenture, Analytics in Action: Breakthroughs and Barriers on the Journey to ROI, 2013, Available at: http://www.accenture.com/SiteCollectionDocuments/us-en/landing-pages/analytics-in-action/accenture_analytics_in_action_survey.pdf, Accessed: 19 January 2013, p.4 *See also*, for example: J.A. Roberts, Profiling Levels of Socially Responsible Consumer

conceptual and practical distinctions for the purposes of clarifying the scope of this research piece. Profiling may be divided into different stages. Koops differentiates between the phases of developing a profile as: 1) Pre-profiling: the collection and storage of data; 2) Profile-making: the analysis of data collections in order to make profiles; 3) Profile use: the application of a profile in a specific case.[6] In this regard the scope of the analysis conducted reflects the latter two aspects for the purposes of attaining a more circumstantial understanding of the particular issues that pertain to the application of profiling in decision-making. This prioritization reflects the emphasis placed on the use of surveillance data for profiling rather than the technical means by which it is collected and retained.

This review provides a focus for the examination of evolving techniques and methodologies that pertain to behavioural profiling. Behavioural profiling involves collecting data (recording, storing and tracking) and searching in it for identifying patterns (with the help of data mining algorithms).[7] The greater efficacy of profiling based on behavioural aspects in relation to counter-terrorism investigations represents a reasonable standpoint from which to apply a narrower focus on aspects of behavioural profiling in relation to serious crimes as a whole, rather than adopt a wider purview.[8]

Behavioural profiling proves a fitting discipline for review in that recent technological and methodological developments portend an evolving paradigmatic shift in the way in which citizens' activities are monitored, measured and interpreted. Specific to this research is a focus on predictive modeling for the purposes of profiling.[9] Predictive profiling employs

---

Behavior: A Cluster Analytic Approach and Its Implications for Marketing, Journal of Marketing Theory and Practice, Vol. 3, No. 4 (Autumn, 1995), pp. 97-117

[6] Koops, Bert-Jaap, Some Reflections on Profiling, Power Shifts, and Protection Paradigms (June 2008), p.1, Profiling The European Citizen, Hildebrandt & Gutwirth, eds., Springer, 2008. Available at SSRN: http://ssrn.com/abstract=1350584

[7] Claude Castelluccia, Behavioural Tracking on the Internet: A Technical Perspective, in S. Gutwirth et al. (eds.), European Data Protection: In Good Health?, Springer, 2012, p.21

[8] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 29 January 2007, A/HRC/4/26, p.7 at para. 60

[9] The 2007 report of the of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism provides a working description of the two principle types of profiling utilised by law enforcement and the intelligence services:

""Profiling" is generally defined as the systematic association of sets of physical, behavioural or psychological characteristics with particular offences and their use as a basis for making law-enforcement decisions. Profiles can be either *descriptive*, i.e. designed to identify those likely to have committed a particular criminal act and thus reflecting the evidence the investigators have gathered concerning this act; or they may be *predictive*, i.e. designed to identify those who may be involved in some future, or as-yet-undiscovered, crime." *See* UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 29 January 2007, A/HRC/4/26,

probabilities-based analysis in order to identify suspects and target them for surveillance, noting that this practice constitutes an actuarial approach (in contrast to that of the explicitly heuristics-based method of descriptive profiling) as the method does not rely entirely on an evaluation of probabilities. The predictive method is contingent on the establishment of statistical correlations between group membership defined by certain traits and the prevalence of criminal activities for the purposes of extrapolating where future crimes may be committed.[10] In this context, the European Code of Police Ethics requires consideration in respect of the guidance given in relation to police action/intervention, whereby "Police investigations shall, as a minimum, be based upon reasonable suspicion of an actual or possible offence or crime." It is questionable therefore, even at this early juncture, as to whether broader use of social network analysis may meet this condition; in particular, the use of the investigatory technique in respect of predictive modeling for preemptive purposes may require exceptional review so as to discern whether it meets this standard.[11]

The distinction between *descriptive* and *predictive* profiling has to date evolved in accordance with established differentiations made between anticipatory or preparatory acts and, contrastively, criminal actions having already been committed. Descriptive profiling relies upon information and evidence in connection to a specific occurrence or set of pre-existing circumstances, and is intended to distinguish parties likely to have engaged in specific acts of a criminal nature connected with these scenarios, whereas predictive profiling resolves to identify, in advance of a specific criminal act occurring, those who may be predisposed toward engaging in unlawful activities for the purposes of prevention.[12]

Interestingly, the conceptual contradistinction between these two processes is rendered ever more conspicuous where rapid advances in computing augur increasingly elaborate endeavors to forecast actions based on extrapolating trends and patterns from assembled data. These advances conceive of an ability

---

p.7 at para. 33. See also: Moeckli, Daniel, Human Rights and Non-discrimination in the 'War on Terror' (July 22, 2008). Daniel Moeckli, HUMAN RIGHTS AND NON-DISCRIMINATION IN THE 'WAR ON TERROR', Oxford University Press, 2008. Available at SSRN: http://ssrn.com/abstract=1161103, pp.197-215 and Moeckli, Daniel, Terrorist Profiling and the Importance of a Proactive Approach to Human Rights Protection (December 16, 2006). Available at SSRN: http://ssrn.com/abstract=952163 or http://dx.doi.org/10.2139/ssrn.952163, pp.1-6

[10] Harcourt, B. E. (2003). The shaping of chance: Actuarial models and criminal profiling at the turn of the twenty-first century. The University of Chicago Law Review, 70, p.109

[11] *See* the Appendix to the Recommendation Rec(2001)10 of the Committee of Ministers to member states on the European Code of Police Ethics, adopted by the Committee of Ministers 19 September 2001. The Appendix to Recommendation Rec (2001)10 on the European Code of Police Ethics states under Section V. 'Guidelines for police action/intervention', (B,1 -47:) "Police investigations shall, as a minimum, be based upon reasonable suspicion of an actual or possible offence or crime."

[12] D. Harris, Profiles in Injustice: Why Racial Profiling Cannot Work (2003), pp. 10, 19-20, 26.

to predict future behaviour based upon prior observation; qualifying and characterizing behavioural attributes and, in turn, construing potentialities based upon ostensibly rational criteria. The inductive approach, when applied to behavioural profiling, to an extent depends upon the acceptance of the presumption that there exist a consistency of, and a correlation between, the behaviour of individuals; thus that there exists a homogeneity of 'types'; and, finally, that their exists a reliability and stability in the data.[13]

Clarke describes surveillance as:"[T]he systematic investigation or monitoring of the actions or communications of one or more persons. Its primary purpose is generally to collect information about them, their activities, or their associates. There may be a secondary intention to deter a whole population from undertaking some kinds of activity."[14] While the aforementioned distinction heretofore outlined indeed narrows to an extent the scope the review of this research, the breadth of surveillance data to which behavioural profiling techniques and methodologies may be applied further necessitates a degree of constriction. Both purposes of the surveillance Clarke identifies are pertinent to this research. Rather than attempt to address the multiplicity of diverse monitoring techniques available to law enforcement and intelligence services I choose to focus on the nascent challenges presented by the use of surveillance data in relation to the monitoring the Internet's social network sites. The pertinence of this particular focus of enquiry is highlighted by the findings of a 2011 report by the research division of the European Court of Human Rights, which noted that:

> "Questions of secret surveillance are all the more relevant in the context of the Internet, as the ongoing evolution of Internet technology has included the rapid development of equipment and techniques to monitor online communications."[15]

Social network site analysis can provide a powerful set of tools for describing and modeling the relational context in which behaviour takes place, as well as the relational dimensions of that behaviour.[16]

While conducting preliminary enquiries into the use of behavioral profiling the author identified a relative deficiency in the extent to which research had to date tackled in greater depth the specific questions that arise from its application to

---

[13] Sean Hammond, Offender Profiling Of Sexual Offences, Broadmoor Hospital, 2007, p.3, Available at: http://www.ramas.co.uk/offender_prof.pdf, Accessed: 22 January 2013.
[14] Roger Clarke, Information Technology and Dataveillance, November 1987, Available at: http://www.rogerclarke.com/DV/CACM88.html, Accessed: 19 January 2013.
[15] COE, Internet: case law of the European Court of Human Rights, 2011, p.8, Available at: http://www.echr.coe.int/NR/rdonlyres/E3B11782-7E42-418B-AC04-A29BEDC0400F/0/RAPPORT_RECHERCHE_Internet_Freedom_Expression_EN.pdf, Accessed: 19 January 2013.
[16] C.T. Butts, Social network analysis: A methodological introduction, Asian Journal of Social Psychology (2008), 11, 13–41, p.13

data collated from the analysis of online social networks.[17] This paper therefore attempts to address this discrepancy and provide a detailed analysis of the issues that arise in respect of the use of data collected by parties conducting surveillance monitoring of web-based social network sites. [18]This review necessarily takes a forward-looking approach in the sense that many of the issues it highlights reflect an evolving paradigm of surveillance, which, the author portends, augurs a likely manifestation of citizens increasingly challenging government monitoring of citizens' online activities.[19]

Scholars from disparate disciplines have appraised social network sites to discern the practices, implications, cultures, and significance of the sites, as well as users' engagement. Citizens today interact with online social network sites and transfer large quantities of their personal information in a manner that is unprecedented.[20] Some indeed submit that citizens have been subject to a

---

[17] Scholars such as Rubinstein et al have approached the question of behavioural profiling in broader terms, referring to the rather indeterminate notion of "internet profiling". *See* Rubinstein, Ira, Lee, Ronald D. and Schwartz, Paul M., Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches. University of Chicago Law Review, Vol. 75, 2008; UC Berkeley Public Law Research Paper No. 1116728. Available at SSRN: http://ssrn.com/abstract=1116728, Accessed: 22 January 2013 p.261

[18] Boyd and Ellison underscore the importance of furnishing a tangible and workable definition where confusion may arise from overly broad application of a term that could conceivably stretch to encompass online services such as social software, social media, collaborative software, or anything that enables any interaction with another human being on the Internet. Boyd and Ellison define social networks sites (SNS) thus: "We define social network sites as web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site." *See* Boyd DB & Ellison NB (2007) Social Network Sites: Definition, History, and Scholarship. Journal of Computer-mediated Communication. 13, 1, article 11. Available at: http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html, Accessed: 22 January 2013.

[19] A 2011 report by the research division of the European Court of Human Rights noted: "The monitoring of Internet use and telephone calls by national authorities could well be the focus of further litigation brought before the European Court of Human Rights in the future." COE, Internet: case-law of the European Court of Human Rights, 2011, p.8, Available at: http://www.echr.coe.int/NR/rdonlyres/E3B11782-7E42-418B-AC04-A29BEDC0400F/0/RAPPORT_RECHERCHE_Internet_Freedom_Expression_EN.pdf, Accessed: 19 January 2013.

[20] Membership of social network sites such as Facebook, Google+ and MySpace have experienced exponential growth in recent years - a phenomenon that to date has evidenced few indications that an increasing reliance on the utility of these sites will wane. Nielsen, State Of The Media: The Social Media Report 2012, April 2012, p.2 Available at: http://www.nielsen.com/us/en/reports/2012/state-of-the-media-the-social-media-report-2012.html, Accessed: 22 January 2013.
See also: S. Lohr, How privacy vanishes online, March 17 2010, Available at: http://www.nytimes.com/2010/03/17/technology/privacy.html. Accessed: 23 February 2013.

significant transformatory process in recent years, perhaps of an irreversible nature, as a result of our utilising the technology to communicate and forge relationships.[21]

The scope and capabilities of social media and social network sites are constantly evolving, and thus unless one actively engages in researching their potential one cannot veritably proffer a candid assessment of their impact. In particular, knowledge and practical experience are essential for the research community to comprehend the extent to which these capabilities may be reoriented and transformed by adept and inventive users of the technology.[22]

Whilst the surveillance of online social networks to counter the complex and asymmetrical nature of certain threats presented to security and public order by their misuse[23] has motivated substantial research into the use of advanced information technology to analyse and counter these threats, the risks the use of these techniques may pose to fundamental rights remains inadequately explored. In addition, this analysis is especially opportune insofar as more complex interactive services are anticipated to appear, which will further harness the power of the social connection and personal information provided by online social networks.[24]

In recent times, advances in communication technologies, coupled with a widening availability of networked devices, have further encouraged citizens to

---

[21] Tene asserts: "This new generation of users consists of individuals who post and search for personal, often intimate, information online; communicate with friends and colleagues on social networks." *See* Tene, Omer, Privacy: The New Generations (November 17, 2010), International Data Privacy Law, 2010, p.17 Available at SSRN: http://ssrn.com/abstract=1710688, Accessed 13 March 2012

[22] For example, social media applications were utilised by individuals engaged in mobilising criminal activity during riots in Athens in 2008 and 2010. In these instances certain individuals utilised social media and exploited capabilities for the purposes of command, control and communication; information was shared between parties so as to allow rioters to target damage to particular properties. See J. J. Stepien, "The Greek Riots and Twitter: Lessons for First Responders," The Counter-Terrorist (11/2010), pp. 58–67.

[23] A report prepared for the Research and National Coordination Organized Crime Division for Law Enforcement in Canada affirms: "Online social media sites can be used to coordinate criminal activities among networks of people who have never met each other offline, to identify criminal opportunities and to defraud." *See* R. Frank, C. Cheng, V. Pun, Social Media Sites: New Fora for Criminal, Communication, and Investigation Opportunities, Research and National Coordination Organized Crime Division Law Enforcement and Policy Branch Public Safety Canada, Report No. 021, 2011, 2011, p.22, Available at: http://www.sfu.ca/iccrc/content/PS-SP-socialmedia.pdf, Accessed: 22 January 2013.

[24] *See* Claude Castelluccia, Behavioural Tracking on the Internet: A Technical Perspective, in S. Gutwirth et al. (eds.), European Data Protection: In Good Health?, Springer, 2012, p.27

share information.[25] Kim affirms that online communication relates not only to expression, but also to associational activity:

> "The proliferation of online communities demonstrates that people participate in online communication not only for the content but also to interact with other communicators, especially those who share their interests or concerns."[26]

Increasingly, civil society engages in political activity not by traditional face-to-face associations but through online acquaintances such that campaigns and coalitions can less easily be defined by way of organized membership, policies and objectives.[27] Social media platforms thrive on both sharing causes and establishing causes to rally around.[28]

Strandburg highlights the complexity of characterising these relationships where their formation demonstrates "decentralized, often transient, networks of individuals associating primarily electronically and with policies and goals defined synergistically with the formation of the emergent association itself."[29] Furthermore, the emergence of online discussion fora and social networking has enabled the development of an exceptionally diverse range of online communities.[30] These associations represent a profuse range of different interest

---

[25] In alluding to the complexity of the challenges associated with an increasing array of disparate communications technologies, the US Subcommittee on Crime, Terrorism, and Homeland Security reported: "There has been a dramatic increase in the volume of communications, the types of services that are offered, and the number of service providers. It is no longer the case that the technology involved in communications services is largely standard. Now, communications occur through a variety of means, including cable, wireline, and wireless broadband, peer-to-peer and VOIP services, and third party applications and providers." *See* United States House of Representatives. Committee on the Judiciary. Subcommittee on Crime, Terrorism and Homeland Security. Hearing on: the 'going dark: Lawful electronic surveillance in the face of new technologies''. Available online http://judiciary.house.gov/hearings/printers/112th/112-59_64581.PDF, February 2011. Serial No. 112-59. U.S. Government Printing Office. Washington, p.5

[26] M Kim, "The Right to Anonymous Association in Cyberspace: US Legal Protection for Anonymity in Name, in Face, and in Action", (2010), p.52, Available at: http://www.law.ed.ac.uk/ahrc/script-ed/vol7-1/kim.asp, Accessed: 19 March 2013

[27] D. Runtzen and J. Zenn, Association and Assembly in the Digital Age, The International Journal of Not-for-Profit Law, Volume 13, Issue 4, December 2011, Available at: http://www.icnl.org/research/library/files/Transnational/Assoc%20Assemb%20Digital%20Age.pdf, Accessed: 19 January 2013.

[28] Robin Thompson, Radicalization and the Use of Social Media, Journal of Strategic Security Volume 4 Issue 4 2011, p.176.

[29] Katherine J. Strandburg, Surveillance of Emergent Associations: Freedom of Association in a Network Society, December 2007, p.1 Available at: http://works.bepress.com/katherine_strandburg/11, Accessed: 22 January 2013.

[30] Acquisti and Gross assert: "At the most basic level, an online social network is an Internet community where individuals interact, often through profiles that (re)present their public persona (and their networks of connections) to others." *See* Alessandro Acquisti and Ralph Gross, Imagined Communities: Awareness, Information Sharing, and

groups and affiliations, and indeed reflect the diversity and the plurality of opinions, convictions and beliefs that are represented in modern societies.[31] Online social network sites have made collective activity more accessible at lower cost, while at the same time diminishing the importance of parties' geographical proximity to one another. [32]

Associations may develop and achieve growth at a pace heretofore deemed unthinkable prior to the advent of social media applications. Gelman uses the term "blurry-edged social networks" to describe those associations where individuals cannot at any given moment list those people who comprise their social network.[33] These characteristics afford traditionally smaller groups less able to influence political decision-making the ability to exercise more influence via the effective exploitation of social media via Internet-based communication.[34] Glassman asserts that this mobilization reflects a significant change whereby these capabilities:

> "Offer unique possibilities for the development of autonomous online communities capable of generating meaning and knowledge while holding together disparate populations in pursuit of shared goals", and that these communities "emerge to address common concerns and work

---

Privacy on the Facebook, Privacy Enhancing Technologies Workshop (PET), 2006, Available at: http://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf , Accessed: 23 February 2013. p.2

[31] Parsell notes, for example, that: "Web 2.0 resources and tools encourage active participation in and identification with communities. Active participation is vividly demonstrated by the democratization of information dissemination." *See* M. Parsell, Pernicious virtual communities, https://www.hci.iastate.edu/REU09/pub/Main/CraftOfResearch/Parsell.pdf, p.3 Ethics and Information Technology (2008) 10:41–56 Ó Springer 2008 DOI 10.1007/s10676-008-9153-y , p.43

[32] *See* M.D. Slater, Reinforcing Spirals: The Mutual Influence of Media Selectivity and Media Effects and Their Impact on Individual Behavior and Social Identity, Communication Theory, Volume 17, Issue 3, pp. 281–303, August 2007

[33] Gelman provides an interesting elucidation of the construct where she remarks on the fact that in using online social network sites an individual develops a matrix comprising of a finite set of nodes linked by discoverable interdependencies. These linkages cannot, however, be accurately enumerated by the individual him/herself. Persons in one category of association may feel a kinship with another similarly situated, but they cannot list everyone with whom they are thus connected by sharing a certain quality or attribute. This illustrates how social networks generate associations that both impersonate but also deviate from those in the offline world. *See* Gelman, Lauren Amy, Privacy, Free Speech, and 'Blurry-Edged' Social Networks (November 1, 2009). Boston College Law Review, Vol. 50, No. 5, 2009, p.1329, Available at SSRN: http://ssrn.com/abstract=1520111, Accessed: 19 January 2013.

[34] Katherine J. Strandburg, Surveillance of Emergent Associations: Freedom of Association in a Network Society, December 2007, p.3, Available at: http://works.bepress.com/katherine_strandburg/11, Accessed: 22 January 2013.

> together in a multilateral, non-linear manner with shifting decision-making structures."[35]

Acquisti and Gross underscore how the increasing confidence in digital technologies, coupled with the self-reinforcing tendency of those utilizing online social networks to encourage ever greater transparency and disclosure, has magnified the effects of social network sites' information sharing utility - which in turn renders familiar conceptions between public and private increasingly redundant, noting:

> "Yet, online social networks' security and access controls are weak by design - to leverage their value as network goods and enhance their growth by making registration, access, and sharing of information uncomplicated. At the same time, the costs of mining and storing data continue to decline. Combined, the two features imply that information provided even on ostensibly private social networks is, effectively, public data, that could exist for as long as anybody has an incentive to maintain it. Many entities - from marketers to employers to national and foreign security agencies - may have those incentives."[36]

Social network sites prove especially efficient in allowing individuals to communicate with previously unacquainted individuals.[37] This transfiguration represents a significant shift in terms of the ubiquity of our interconnectedness toward others.[38] While online social networks have evolved into global platforms by which we can share, disseminate, and communicate ideas, their ubiquity, low access cost and ease of use all contribute in their appeal to parties wishing to exploit their effectiveness for the purposes of crime. [39]

---

[35] Glassman, Michael. (2012). Occupying the Noosystem: The Evolution of Media Platforms and Webs of Community Protest, Berkeley Planning Journal, 25(1). ucb_crp_bpj_11730. Available at: http://www.escholarship.org/uc/item/5ws9b7f5, p.3

[36] Alessandro Acquisti and Ralph Gross, Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook, Privacy Enhancing Technologies Workshop (PET), 2006, Available at: http://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf, p.1, Accessed: 23 February 2013.

[37] *See* Boyd DB & Ellison NB (2007) Social Network Sites: Definition, History, and Scholarship. Journal of Computer-mediated Communication. 13, 1, article 11. Available at: http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html, Accessed: 22 January 2013.

[38] Boyd and Ellison note how social network sites differ in their user bases, noting certain networks appeal to a particular audience: "As of this writing, there are hundreds of SNSs, with various technological affordances, supporting a wide range of interests and practices. While their key technological features are fairly consistent, the cultures that emerge around SNSs are varied… Some sites cater to diverse audiences, while others attract people based on common language or shared racial, sexual, religious, or nationality-based identities." *See* Boyd DB & Ellison NB (2007) Social Network Sites: Definition, History, and Scholarship. Journal of Computer-mediated Communication. 13, 1, article 11. Available at: http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html, Accessed: 22 January 2013.

[39] *See* S. Nelson, J.Simek and J.Foltin, The Legal implications of Social Networking, 22 Regent U. L. Rev. 1 (2009-2010), p.2

In particular, attributes such as the capacity to identify and connect individuals also serve individuals or groups wishing to facilitate communications, promote or publicize unlawful activities and recruit others. In an allusion to this tendency the European Court of Human Rights noted as: "[B]eyond dispute that the fight against crime, and in particular against organised crime and terrorism, which is one of the challenges faced by today's European societies, depends to a great extent on the use of modern scientific techniques of investigation and identification."[40]The further tendencies that Acquisti and Gross highlight in terms of the powerful networking effects of social network sites also, however, hint at its utility for those wishing to subvert its capabilities for illicit purposes.[41] The Appendix to the Recommendation of the Committee of Ministers to member states on the European Code of Police Ethics outlines as an objective of the police the detection of crime; surveillance activity of social network sites for the purposes of profiling thus falls within this remit.[42]

Surveillance activity monitoring the use of online social networks has been classed as constituting a novel form of 'open source intelligence'; in effect asserting that the method reflects an extension of established practices that simply take advantage of newly available conduits for communication and information transfer.[43] This assertion discerns that a transition toward the surveillance of online social networks evinces a natural extension of a tradition of law enforcement seeking to appraise intelligence gathered from the growing number of overt, public information sources.[44]

---

[40] S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, § 105, 4 December 2008

[41] A report by the Criminal Intelligence Services (CISC) of Canada in 2010 reported that criminal organisations use the technology "to communicate securely, conceal their activities, target victims, and locate skilled labour and valuable goods, such as large caches of stolen personal and commercial data." The same report also noted that certain organised criminal networks "are exclusively virtual with illicit activities and communications occurring entirely online." *See* CISC, 2010 Organized Crime Report, May 2010, Available at: http://www.cisc.gc.ca/annual_reports/annual_report_2010/frontpage_2010_e.html, Accessed: 19 January 2013.

[42] Recommendation Rec(2001)10 of the Committee of Ministers to member states on the European Code of Police Ethics, adopted by the Committee of Ministers 19 September 2001

[43] *See*, for example, the promotional material of software developers Paterva, which describes open source intelligence (OSINT) thus: "Open source intelligence (OSINT) is form of intelligence collection management that involves finding, selecting, and acquiring information from publicly available sources and analyzing it to produce actionable intelligence. In the intelligence community (IC), the term "open" refers to overt, publicly available sources (as opposed to covert or classified sources)" See Paterva, If this is Open Source - where can I get the source? Available at: http://www.paterva.com/web6/documentation/faq.php, Accessed: 19 January 2013.

[44] The UK's Open Data Institute, for example, secured in early 2013 £10 million to research the use of 'open data' or 'open source intelligence' for the purposes of improving public security and the judicial system. March 2013 saw it launch the 'Crime and Justice' programme to leverage the use of data in this sector. The project aims to

The question therefore arises as to whether the fusion of surveillance monitoring of social networks with predictive analytics could represent a fundamental shift stemming from its intrinsic capacity to accurately elaborate interpersonal relationships, an achievement that has to date proven particularly elusive.[45] Thompson hints at the possible benefits to law enforcement of embracing social network analysis where "every person with a cell phone and a social media application is a ground sensor capable of collecting and distributing raw, real-time intelligence."[46]However, oversight of the means by which information is acquired and disseminated within a society is integral to ensuring accountability, and functions to empower citizens in a democracy.[47] Gibson highlights the pivotal nature of this interdependency, noting that a democratic society should allow for the intelligence function to perform reciprocally, reflecting a two-way relationship with the public:

> "The public trusts it and it creates trust in the collective mind of the public. The currency of exchange is information, in the broadest sense of the word. If that currency is restricted then trust diminishes with it."[48]

---

unite specialists and industry experts including police forces, government departments, private security companies and charities, noting: "Attendees will innovate using datasets that may include crime data, sentencing statistics, poverty measures and rates of re-offending." *See* Open Data Institute, Knowledge for Everyone - Open Data Immersion Programme, 2013, Available at: http://www.theodi.org/events/immersion-programme, Accessed: 19 March 2013.

[45] McCue, an authority on operational law enforcement and security analytics, argues that a significant amount of human engagement is required to ensure the accuracy of predictive analysis, casting doubt on the assertion that its use may always be less resource intensive than other means: "In general, analysts should expect to spend approximately 80% of their time preparing the data and 20% of their time analyzing it. While this sounds like a terribly unattractive prospect, if the data preparation is done well, huge benefits in the overall quality of the analysis can be reaped. Moreover, the analysts will gain additional insight into the data, which can further refine the analysis." C. McCue, Data Mining and Predictive Analysis - Intelligence Gathering and Crime Analysis, (Oxford: Elsevier), 2007, p.93

[46] Robin Thompson, Radicalization and the Use of Social Media, Journal of Strategic Security Volume 4 Issue 4 2011, p.176

[47] The "democratizing effects" effects of Internet discourse were highlighted in the judgment of the US case ACLU v. Reno in 1996: "It is no exaggeration to conclude that the Internet has achieved, and continues to achieve, the most participatory marketplace of mass speech that this country - and indeed the world - has yet seen. The plaintiffs in these actions correctly describe the "democratizing" effects of Internet communication: individual citizens of limited means can speak to a worldwide audience on issues of concern to them… [T]he Internet may fairly be regarded as a never-ending worldwide conversation." - ACLU v. Reno , 929 F.Supp. 825 (ED.Pa. 1996), aff'd, 521 U.S. 844 (1997).

[48] Stevyn Gibson, Open Source Intelligence An Intelligence Lifeline, RUSI Journal, February 2004, p.3, Available at: http://www.rusi.org/downloads/assets/JA00365.pdf, Accessed: 22 January 2013.

Crucially, the question thus arises as to whether or not profiling information pertaining to online social networking activity constitutes a profound transformation in terms of how society conceives of the parameters to which lawful surveillance may extend.[49]

Distinctions between the 'private' and 'public' may therefore risk being further obfuscated. Briggs highlights the extent to which citizens' social network site activity challenges the public-private dichotomy, noting that personal information may be made more accessible by a process of 'social appropriation':

> "Developments of this type are interesting because they significantly enhance our ability to predict patterns of behaviour and personal preference in a way which is context sensitive… private histories can become public by a process of social appropriation. The power to combine such personal histories with rich contextual data suggests a future in which our daily habits and preferences can become highly accessible to others."[50]

Similarly, Castelluccia forewarns of a danger whereby we drift unwittingly into a condition whereby surveillance of Internet activity is pervasive, and tacitly accept that all our online actions are recorded and correlated for the purpose of discerning whether our behaviour suggests a tendency to engage in inapposite pursuits.[51]

Social network sites: Profiling as relational surveillance

In *Klass and Others v. Germany* the European Court of Human Rights accepted that the existence of legislation allowing for the surveillance of telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime.[52]Online social networks therefore, as a form of telecommunication, may also serve this purpose to provide the police and law enforcement services with valuable intelligence to inform decision-making and prevent crime. Their increasing omnipresence and ubiquity are testimony to the value users accord them.

---

[49] Horvitz, a researcher at Microsoft Research, notes: "Large amounts of data are being collected in part because of the shift of many human activities to the Web – and that has made it easy to collect transactions and events of various kinds in stream with activities." *See* 'A Golden Era of Insight: Big Data's Bright Future', Microsoft Research, 15 February 2013, Available at: http://www.microsoft.com/en-us/news/features/2013/feb13/02-15BigDataHorvitz.aspx, Accessed: 22 January 2013.
[50] P. Briggs, Future Identities: Changing identities in the UK – the next 10 years, UK Government Office for Science, January 2013, p.5
[51] Claude Castelluccia, Behavioural Tracking on the Internet: A Technical Perspective, in S. Gutwirth et al. (eds.), European Data Protection: In Good Health?, Springer, 2012, p.22
[52] Klass and Others v. Germany, 6 September 1978, § 48, Series A no. 28

Recent events have further prompted debate as to whether the prospect of a further augmentation in the implementation of social network analysis in crime prevention augurs well for civil society. [53] Sandburg notes that this evolution reflects a maturation of existing practice vis-à-vis 'relational surveillance' to deliver deeper insight into suspect activity by investigating the membership and relational structures of online association.[54]Concerns have also been expressed that this evolution is intrinsically refractory; monitoring of social networks sites for profiling may furnish 'destabilizing' interpretative accounts of human interactions, thus describing a transformative process that risks societal disorientation.[55] Conversely, Cohen argues that a greater risk associated with such techniques is that they attempt rendering individual behaviors and preferences transparent by conforming them to preexisting frameworks: this approach may in turn distort and misrepresent: "And in seeking to mold the future, surveillance also shapes the past: by creating fixed records of presence, appearance, and behavior, surveillance constitutes institutional and social memory."[56]

The increasingly preeminent role social network sites play in communication necessitates careful deliberation as we consider allowing their surveillance for the purposes of crime prevention. CEPOL recently alluded to the criticality of determining the effective exploitation of the resource, noting:

> "Social media systems have become increasingly interwoven with people's everyday lives, be it work or private. Such a prominent social development cannot be ignored by police forces, which in increasing numbers follow the public to the net."[57]

As technology has evolved emphasis has shifted from data operations (storage, access and the processing of data) to the evolving sphere of data science;

---

[53] *See*, for example, the 2011 HMIC report discussing the role social network analysis might play in tracking disturbances in public protest following the London riots of 2010. HMIC, The rules of engagement - A review of the August 2011 disorders, 2011, Available at: http://www.hmic.gov.uk/media/a-review-of-the-august-2011-disorders-20111220.pdf, Accessed: 19 January 2013.

[54] Katherine J. Strandburg, Surveillance of Emergent Associations: Freedom of Association in a Network Society, December 2007, p.1, Available at: http://works.bepress.com/katherine_strandburg/11, Accessed: 22 January 2013.

[55] David M. Berry, The Computational Turn: Thinking About The Digital Humanities, Culture Machine, Vol 12, 2011, p.12, Available at: www.culturemachine.net, Accessed 2 February 2013.

[56] *See* Cohen, Julie E., Privacy, Visibility, Transparency, and Exposure. University of Chicago Law Review, Vol. 75, No. 1, 2008; Georgetown Public Law Research Paper No. 1012068, p.186, Available at SSRN: http://ssrn.com/abstract=1012068, accessed 13 March 2012

[57] European Police College (CEPOL), Cross-European Approaches to Social Media as a Tool for Police Communication, Issue 6 - Winter 2011/12, p.11, Available at: http://www.composite-project.eu/tl_files/fM_k0005/AB%20Downloads/Denef+Bayerl+Kaptein_6_Bulletin.pdf, Accessed: 19 January 2013.

reflecting a growing interest in the computation of data for the purposes of understanding, analysing and, most critically, forecasting crime.[58]The dynamics of this change suggest a steady transition from a research basis towards its operational deployment in law enforcement and intelligence services. That said a necessary additional factor to consider is undoubtedly the overt promotion by commercial operations of predictive analytics as a solution to threats to public safety.[59]Indeed, the security industry clearly has an interest in encouraging the uptake and deployment of surveillance systems. The political economy of surveillance should not be overlooked as technology companies constantly press for procurements.[60]

In part, social network sites constitute an extremely attractive source of open source intelligence for the construction of profiles precisely because of the level of trust placed in them by users. Consequently, both the quantity, and detailed granularity of, the information pertaining to an individual's exploits is significant.[61] However, the analysis of data from social network sites for the purposes of the prevention of crime is, however, no panacea.[62] Despite the

---

[58] *See* D. Smith, Real-time Big Data Analytics: From Deployment to Production, Revolution Analytics, Available at: http://www.revolutionanalytics.com/news-events/free-webinars/2012/real-time-big-data-analytics/, Accessed: 19 January 2013.

[59] *See*, for example: HMIC, The rules of engagement - A review of the August 2011 disorders, 2011, Available at: http://www.hmic.gov.uk/media/a-review-of-the-august-2011-disorders-20111220.pdf, Accessed: 19 January 2013, p.36

[60] D. Lyon, Surveillance, Power, and Everyday Life, Oxford University Press, New York, 2007, p.15. One industry analyst recently called on public security professionals to view social media as a solution to fighting organised crime, rather than as an enabler for criminals to more efficiently coordinate their trade: "[S]top seeing social media as the problem and start tapping into it as part of the solution. In the fight against anti-social criminals, organised crime and terrorists alike, social media can be the law enforcement professional's most powerful weapon." *See* SAS Institute Inc., How Social Media Can Help Win the Battle for Public Security, 13 July 2012, Available at: http://www.memex.com/content/how-social-media-analytics-can-help-win-battle-public-security, Accessed: 19 January 2013. Eric Horvitz, Co-director of Microsoft Research, also speaks enthusiastically of a "Golden era of insight" whereby effective large-scale data analytics for predictive modeling, visualization, and discovery are becoming central for success, claiming that "we can leverage data to make real-time predictions about a computer user's changing intentions or interests." See 'A 'Golden Era' of Insight: Big Data's Bright Future', Microsoft Research, 15 February 2013, Available at: http://www.microsoft.com/en-us/news/features/2013/feb13/02-15BigDataHorvitz.aspx, Accessed: 22 January 2013.

[61] R. Frank, C. Cheng, V. Pun, Social Media Sites: New Fora for Criminal, Communication, and Investigation Opportunities, Research and National Coordination Organized Crime Division Law Enforcement and Policy Branch Public Safety Canada, Report No. 021, 2011, 2011, p.22, Available at: http://www.sfu.ca/iccrc/content/PS-SP-socialmedia.pdf, Accessed: 22 January 2013.

[62] Analysts such as Coleen McCue, an operational law enforcement and security analytics specialist, suggest that experience underscores the limits to the utility of new surveillance technologies, and that predictive profiling has clear limits to its application: "If we have learned little else in the past few years, one thing that has become abundantly clear is that there probably is no Rosetta Stone of crime and intelligence

increasing recognition of social networking analysis as a concept, the medium remains poorly understood, both in terms of its practical applications and its theoretical basis.[63] As with any analytical tool, its use necessitates a studied approach, which requires comprehension of both its utility and, conversely, its risks and limitations.

Mining data for suspicious associations

Increasing computational capabilities make it possible to apply analytics to larger and larger sets of data and raise the possibility of employing data mining techniques to uncover 'suspicious' patterns of association.[64] A company supplying European law enforcement agencies with social network site analytics, SAS Analytics, recently described the capability to continuously monitor online and social conversation data (and, on the same note, spoke rather ominously of a "battle for public security":

> "[T]o identify key topics and to enable professionals to focus in on relevant content areas *without wasting time sifting through information that ultimately proves immaterial*. Equally, they give investigators the ability to link different types of information to understand how people are connected, the closeness of those connections and the *ring-leaders involved*."[65]

---

information." See C. McCue, Data Mining and Predictive Analysis - Intelligence Gathering and Crime Analysis, (Oxford: Elsevier), 2007, p.320

[63] Analysts at the Cyber Behavior and Defense Institute of Artis Research affirm their belief that too often the limitations of analytical models remains unacknowledged, noting: "Even data-driven network analysis misses the mark by concentrating too heavily on descriptions of network structures without making clear statements about why and how they matter to the collective behavior under inspection. Possibilities are generated, but probabilities cannot be. All too often, the individual human element is either missing or misconstrued in both the approach and application to understanding." *See* ARTIS Research, Network Analysis, Available at: http://artisresearch.com/?page_id=2337, Accessed: 19 January 2013.

[64] Ugander et al describe the relatively onerous and time-consuming nature of the analysis of social networks prior to the advent of their online counterparts, noting: "Historically, studies of social networks were limited to hundreds of individuals as data on social relationships was collected through painstakingly difficult means. Online social networks allow us to increase the scale and accuracy of such studies dramatically because new social network data, mostly from online sources, map out our social relationships at a nearly global scale." *See* J. Ugander, B. Karrer, L. Backstrom, C. Marlow, The Anatomy of the Facebook Social Graph, 18 November 2011, p.1, Available at: http://arxiv.org/abs/1111.4503, Accessed: 22 January 2013.

[65] SAS Institute Inc., How Social Media Can Help Win the Battle for Public Security, 13 July 2012, Available at: http://www.memex.com/content/how-social-media-analytics-can-help-win-battle-public-security, Accessed: 19 January 2013 – *Note: emphasis added*. *See* also, *supra*, note 45: whereby McCue notes, in distinct contrast: "In general, analysts should expect to spend approximately 80% of their time preparing the data and 20% of their time analyzing it. While this sounds like a terribly unattractive prospect, if the data preparation is done well, huge benefits in the overall quality of the analysis can be reaped." Thus there clearly exists a distinct difference of opinion as regards the

This use of social network site data to discern suspect activity and investigate individuals, their membership of groups, their structure and attempt to predict future behaviours brings to the fore questions as to the permissible boundaries of data mining. The application of data mining to social network analysis for the purposes of crime prevention constitutes a continuing development of the medium of relational surveillance.[66] While conceptually relatively well established, nonetheless the assimilation of social network analysis into a potentially more expansive form of relational surveillance, anticipating the delivery of compelling new insight into behavioural observation, presents hazards.

Relational surveillance, which aspires to resolve and elucidate the nature of interactions and their purpose, highlighting suspicious patterns of association, harbours inherent risks - particularly in respect of its propensity to interfere with associational activity and free expression. Established doctrine pertaining to the rights to freedom of association, developed with respect to the protection of traditional notions of freedom of association, potentially provide strong protection against overreaching relational surveillance.[67]Relational surveillance for the purposes of profiling may be regulated so as to ensure the necessary protection of the burgeoning role of emergent associations in civil society that develop through social network sites. These associations increasingly play a role in citizens' lives and encourage wider dialogue and engagement in society.

In particular, the immediacy and asynchronous nature of Internet communications render them an especially efficient and efficacious tool in connecting the once disassociated; allowing parties to organise, mobilise and recruit others through highly connective social networks in a process that frequently obviates the need for either hierarchy or refinement of a strategy.[68]Ugander et al have observed the growing influence of social network sites in online communication, asserting: "As individuals bring their social relations online, the focal point of the internet is evolving from being a network of documents to being a network of people, and previously invisible social

---

precision of the technologies concerned; presenting obvious concerns as regards the ramifications for citizens subject to monitoring should these issues not be satisfactorily reconciled so as to ensure the necessary acuity required of agencies' criminal investigatory work using these techniques.

[66] *See*, for example: A.L. Barabasi, Linked: The New Science of Networks, Perseus Group, 2002, and Carrington, P.J., Scott, J. Wasserman, Models and Methods in Social Network Analysis, Cambridge University Press, New York, 2005.

[67] K. Strandburg, Surveillance of Emergent Associations: Freedom of Association in a Network Society, p. 1, in 'Digital Privacy: Theory, Technologies, and Practices' (Alessandro Acquisti, Stefanos Gritzalis, Costas Lambrinoudakis and Sabrina De Capitani di Vimercati, eds., Auerbach Publications, 2008)

[68] In 2002 Rheingold wrote with startling prescience of a techno-cultural shift empowering collective action and reinvigorating mobilisation and association through consumer devices that enabled greater connectivity between citizens. *See* Rheingold, Howard, Smart Mobs: The Next Social Revolution, Basic Books, 2002.

structures are being captured at tremendous scale and with unprecedented detail."[69]

Especially significant in our consideration of social network sites is their ability to originate associations that emerge and develop with unparalleled celerity, affording scope for citizens to interact and mobilise at a rate that corresponds to the speed at which the Internet facilitates and encourages the rapid interchange of information. Strandburg highlights the heterogeneity of emergent associations generated by interaction on social network sites, noting:

> "They can remain loosely connected or coalesce into more traditional forms of organization with paid staff, centralized decision making, and so forth. In an emergent association, strategies, issues, and positions can be selected democratically or imposed by a central leadership, but can also self-organize out of the independent actions of individuals. The low cost and many-to-many structure of modern communication technology facilitates experimentation and cooperation between different groups."[70]

A benefit of social network sites' abilities to facilitate association is its inherently egalitarian capacity to enable and embolden those who are otherwise unempowered or marginalized, lacking capacity to leverage influence or resources. Surveillance may therefore jeopardize equality. Protection from discrimination is enshrined in the International Covenant on Civil and Political Rights (ICCPR). Articles 2(1) and 26 may be engaged where profiling-related activity relating to associations between parties constitutes towards a discriminatory practice on the part of a State agency based on grounds, for example, of gender, religion, political or other opinion.[71]

---

[69] J. Ugander, B. Karrer, L. Backstrom, C. Marlow, The Anatomy of the Facebook Social Graph, 18 November 2011, p.1, Available at: http://arxiv.org/abs/1111.4503, Accessed: 22 January 2013.

[70] K. Strandburg, Surveillance of Emergent Associations: Freedom of Association in a Network Society, p. 3, in 'Digital Privacy: Theory, Technologies, and Practices' (Alessandro Acquisti, Stefanos Gritzalis, Costas Lambrinoudakis and Sabrina De Capitani di Vimercati, eds., Auerbach Publications, 2008)

[71] *See* UN International Covenant on Civil and Political Rights (ICCPR). Article 2(1) affirms: "Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status." Article 26 states: "All persons are equal before the law and are entitled without any discrimination to the equal protection of the law. In this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status." In addition, Article 14 of the European Convention for the Protection of Human Rights and Fundamental Freedoms states: "The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status." The Charter

Mobilization of citizens encourages aggregation, fostering and melding a collective effort that enfranchises and capacitates those whose persuasions reflect minority identities or opinions. In this regard the provision within the UN Code of Conduct for Law Enforcement Officials should also be considered with respect to the guarantee furnished by Article 2 and its commentary, 2(a), with regard to the duty of law enforcement officials to respect and protect human dignity and maintain and uphold the human rights of all persons.[72] Also relevant in this respect is the Council of Europe Convention of 1981 for the protection of individuals with regard to automatic processing of personal data, in which the limitations to which this processing is subject are outlined. The Convention provides, *inter alia*:

> "Article 5 – Quality of data
> c. adequate, relevant and not excessive in relation to the purposes for which they are stored;
> Article 6 – Special categories of data
> Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. (...)."[73]

The relevance of the above-cited provision relates to data collected by social network site monitoring that may pertain to information connected with an individual's political opinions or other beliefs, for example.

In addition, social network sites' facilitation of pseudonymity and anonymity emanates and encourages the development of associations that would less likely exist where participants feel deterred should their affiliation court attention.[74]

Of Fundamental Rights Of The European Union also stipulates within Article 21 of the treaty that: "Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited."

[72] The commentary refers also to, inter alia, the ICCPR and the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD), both of which contain provisions outlining the prohibition of discrimination. See UN Code of Conduct for Law Enforcement Officials, General Assembly resolution 34/169, adopted 17 December 1979.

[73] COE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted Strasbourg, 28.1.1981

[74] In an illustrative parallel Millbank notes, for example, that refugee decision-makers in the United Kingdom and Australia have been slow to fully appreciate the fact that sexual minorities are secretive about their sexuality and relationships as a result of oppressive social forces rather than by 'choice'. Millbank cites a change in precedent where, in Appellants S395/2002 and S396/2002 v. Minister for Immigration and Multicultural Affairs, the High Court of Australia was the first ultimate appellate court to consider a claim to refugee status based upon sexual orientation. By majority the court rejected the notion prevalent in earlier cases that decision-makers could 'expect' refugee applicants

Kim notes: "The Internet has become a communication medium of intense group interaction, and individuals with marginalised identities have used anonymity as a tool with which to participate in online interaction."[75]Research has shown that participation in online associations is more highly valued by people with marginalised, concealed or stigmatised identities (for example, by those who may not feel able to disclose their sexual orientation publicly, or those with extreme political beliefs).[76]Monitoring, in any form, may engender amongst those observed an agitation as to the judgment of those overseeing the monitoring. As such, those being watched may develop anxieties as to whether their exchanges with others may be misunderstood, their associative behaviours misinterpreted.[77] Merely being conscious of scrutiny by another party, then, can create unease. Kang argues that we invariably feel inhibited where we sense undesired observation:

> "... We have the capacity to reflect upon and choose personal and political projects and how best to further them... knowledge of observation "brings one to a new consciousness of oneself, as something seen through another's eyes. Simply put, surveillance leads to self-censorship."[78]

Furthermore, we might reflect too as to whether indeed apprehension should constitute the threshold by which we challenge the necessity of an encroachment.[79] When cognizant of an interference one may feel restrained, encumbered or inhibited: even absent any anxiety, this intervention may nonetheless evince subtle changes to our mental state (for instance, our sense of seclusion) and prompt adequate contemplation as to its necessity. Others have

---

to 'co-operate in their own protection' by concealing their sexuality. This precept, if accepted, could be interpreted as more broadly acknowledging the limitations for a in which sexual identity may be expressed, thus providing some substantiation for the premise that discreet online association could provide a haven for those who feel their identities to be suppressed. *See* Millbank, Jenni, From Discretion to Disbelief: Recent Trends in Refugee Determinations on the Basis of Sexual Orientation in Australia and the United Kingdom (January 19, 2009), International Journal of Human Rights, Vol. 13, No. 2/3, 2009. Available at SSRN: http://ssrn.com/abstract=1330175, p.2

[75] M Kim, "The Right to Anonymous Association in Cyberspace: US Legal Protection for Anonymity in Name, in Face, and in Action", (2010), p.1, Available at: http://www.law.ed.ac.uk/ahrc/script-ed/vol7-1/kim.asp, Accessed: 19 March 2013

[76] *See*, for example: S Watt, M Lea, and R Spears, "How Social is Internet Communication? A Reappraisal of Bandwidth and Anonymity effects" in S Woolgar (ed) Virtual Society?: Technology, Cyberbole, Reality (2002) 61-62; K McKenna and J Bargh, "Coming out in the Age of the Internet: Identity 'Demarginalization' through Virtual Group Participation" (1998) 75 Journal of Personality and Social Psychology, 681-694.

[77] *See:* Solove, Daniel J., Reconstructing Electronic Surveillance Law. George Washington Law Review, Vol. 72, 2004, p.1708 Available at SSRN: http://ssrn.com/abstract=445180 or http://dx.doi.org/10.2139/ssrn.445180, accessed 13 March 2012.

[78] Kang, Jerry, Information Privacy in Cyberspace Transactions, Stanford Law Review, Vol. 50, p.1260, 1998. Available at SSRN: http://ssrn.com/abstract=631723, accessed 12 May 2012

[79] Parker indeed emphasizes the significance of sensory oversight over a party's activity in defining privacy; he interprets privacy as constituting "control over who can sense us." *See*: Richard B. Parker, A Definition of Privacy, 27 RUTGERS L. REV. (1974), p.281

expressed concern based in part on the inability of citizens to apprehend[80] both the extent and significance of their online activity being tracked, which underscore the possible ramifications of a move toward a more prevalent or pervasive monitoring.[81]The surveillance of social network sites potentially carries therefore the very real risk of disrupting the inceptive period of associations, challenging one of the clear benefits the technology affords.

Communication and association on the Internet through social networks sites may develop in a manner that is all but invisible outside of the Web. That said, we should reflect and ponder the meaning of 'invisibility', and consider whether such a notion prove an exaggeration in the sense that it appears defensive – suggestive of a clandestine nature, of secrecy.[82] Society may unwittingly neglect to heed attention to subtle revisions by actors in the demarcation of the observed and the imperceptible, precipitating a vicissitude that induces an invasive role for surveillance.

Data mining activities for the purpose of predictive behavioural profiling may pose a risk where they expose and reveal nascent relationships and interactions that would otherwise remain undetected. Recognizing this risk Rachels posits that the requisite measure for privacy protection should assure individuals "…the important power to share information discriminately, which in turn enables them to determine not only how close they are to others, but the nature of their relationships."[83] Uteck argues that circumstances - interpreted in accordance with given contextual considerations - establish the conditions by which we anticipate protection from intrusive interference, and notes that this

---

[80] Lockwood notes that while most mobile phone users are generally aware that calls send and receive information via a network of cellular towers, only a minority will appreciate the express precision of the location data the technology may impart to service providers and other parties to whom access is granted. *See:* S. Lockwood, Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators, 18 HARV. J.L. & TECH (2004), pp.313-314

[81] Uteck notes: "Individuals are not always aware of what is being observed, even if they are aware of the installed technology. Apart from hiding the existence of surveillance, the embedded technology also makes it difficult to know what exactly is being observed and monitored. This creates, in effect, an embedded panopticon—pervasive surveillance hidden in the environment. *See* Uteck, Anne, Ubiquitous Computing And Spatial Privacy (March, 2009), p.89, Lessons From The Identity Trail: Anonymity, Privacy And Identity In A Networked Society, New York: Oxford University Press, 2009; Available at: idtrail.org/content/view/799, accessed 13 March 2012

[82] When using online social networks it is becoming increasingly challenging to maintain a profile that segregates disclosures. *See:* Gelman, Lauren Amy, Privacy, Free Speech, and 'Blurry-Edged' Social Networks (November 1, 2009). Boston College Law Review, Vol. 50, No. 5, 2009, p.1329, Available at SSRN: http://ssrn.com/abstract=1520111, Accessed: 22 January 2013.

[83] Rachels, J., Why Privacy Is Important, in Philosophical Dimensions of Privacy: An Anthology, Ferdinand D. Schoeman, ed., Cambridge: Cambridge University Press, (1984), p.294

expectation is a nuanced, contextual and fundamentally normative exercise.[84] Thus we might surmise that surveillance activity that may unearth such relationships warrants more nuanced oversight. The exposure of nascent consortia to wider critical examination and inspection may constitute a chilling effect that serves to stymie critical debate in a democratic society.

A particular concern therefore is the ostensible 'discovery' of associational patterns that may be in turn be classified in accordance with certain designations of behaviour. Exceptional care is needed where the analysis undertakes to resolve whether the constitution of associations may herald proclivity toward future engagement in unlawful activities. In these circumstances, the application of predictive profiling techniques proves predeterminate, and risks evidencing emergent associations before members even recognize or comprehend their own affiliation. Should surveillance of this nature impose upon the individuals connecting with one another and imparting information for fear of attracting unsolicited attention, citizens might well moderate their level of engagement and enquiry where they anticipate possible exploratory forays by the State. This hesitancy to participate in discourse and debate would likely prove the more consequential where topics may be perceived by some as reflecting seditious or subversive tendencies. The repercussions of an overly intrusive approach are therefore considerable. In *Klass and Others v. Germany* the European Court of Human Rights stressed that States must exercise caution in their exercise of surveillance lest its use risk undermining the very democracy it use is intended to protect."[85]

Knowledge that social network site activity may be subject to an extensive regime of monitoring interactions with other parties could foster a growing reticence amongst users to debate. Individuals may feel inhibited and constrained by such a development, particularly where the degree of engagement (in terms, for example, of the level and frequency of interaction with another party) likely to invite suspicion and the advent of a more comprehensive mode of surveillance remains opaque.

Crime prevention, link analysis and patterns of association

Law enforcement and intelligence officers may employ data mining techniques to the analysis of activity on social network sites for various purposes connected

---

[84] Uteck, Anne, Ubiquitous Computing And Spatial Privacy (March, 2009), p.89, Lessons From The Identity Trail: Anonymity, Privacy And Identity In A Networked Society, New York: Oxford University Press, 2009; Available at: idtrail.org/content/view/799, accessed 13 March 2012

[85] "Nevertheless, the Court stresses that this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate." Klass and Others v. Germany, 6 September 1978, § 49, Series A no. 28

with the prevention of crime, depending upon context. For example, the use of predictive analytics software may allow associational patterns within an identified network to distinguish between differences in the participatory engagement of different individuals.[86] Another practice, link analysis, may be used to extract underlying information pertaining to an individual's subsidiary associations with less proximate groups.[87] Lastly, the review of social network sites may also incorporate data mining activity that ventures to recognize patterns that may aid in the identification of further groups that may share heretofore-unidentified association.[88] A primary objective then of the use of metrics to analyse activity on social network sites is to allow those conducting the analysis to compare different attributes of the interactions of users and the inferred associative networks.[89] A person's function in relation to others may be qualified by tallying the various connections made with different users, while their role may also be measured and determined by the degree to which interconnections between unassociated parties pass via an individual acting as a conduit. Furthermore, analytics may also attempt to qualify the value of an association by characterizing reciprocity (i.e. discerning the extent to which connections are either mutual or otherwise only unidirectional).

We need consider therefore the impact that the implementation of this use of data for profiling online associations may have on citizens. Interestingly,

---

[86] McCue notes: "Predictive analytics encompasses a variety of model making tools or algorithms that can be employed to characterize historical information, which then can be used to predict the nature and likelihood of future events or occurrences." *See* C. McCue, Data Mining and Predictive Analysis - Intelligence Gathering and Crime Analysis, (Oxford: Elsevier), 2007, p.117

[87] De Rosa notes that subject-based link analysis mines data sets to determine links between a subject and other people, places, or things. De Rosa further affirms that this technique is already being used for background investigations and as an investigatory tool in national security and law enforcement investigations. *See* M. De Rosa, Data Mining and Data Analysis for Counterterrorism, March 2004, Center for Strategic and International Studies (CSIS), p.6, Available at: http://csis.org/files/media/csis/pubs/040301_data_mining_report.pdf, Accessed: 22 January 2013.

[88] A concern arises as regards the extent to which correlations may be drawn between associations and groups, or indeed to parties sharing a similar background. The notion of background, in particular, may in the context of profiling reflect a broad conceptualisation. Data mining by way of pattern-based analysis for the purposes of profiling individuals manifestly operates on the basis of determining a shared background of some sort. Thus, recognising this fact, more specifically a review of the permissibility of distinctions drawn on the basis of 'background' need be refined so as to effectively explicate which classifications of 'background' allow for non-discriminatory profiling. *See* UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 29 January 2007, A/HRC/4/26, p.7 at para. 40, which states: "The Special Rapporteur is concerned that profiling based on stereotypical assumptions may bolster sentiments of hostility and xenophobia in the general public towards persons of certain ethnic or religious background."

[89] Seifert, J. W., Data Mining And Homeland Security: An Overview, CRS Report RL31798, 2006.

research on human relationships has shown that our traditional offline social networks are perhaps surprisingly less complex than we might imagine.[90] In fact, this realization curiously reflects the common observation that 'we live in a small world' - whereby we frequently seem to make acquaintances with others that happen to know another party with whom we share some sort of a connection.[91] Strandburg warns that: "Targeted link analysis and pattern analysis, which rely on entire networks of communications patterns, thus have the potential to sweep in a very large number of individuals and their associations in short order."[92]

Where law enforcement officials suspect an individual may be inclined to embark in an unlawful activity they may use link analysis in a predictive context to pre-empt criminal activity by mining existing data not just of the individual under suspicion but also, crucially, that of his or her contacts, the acquaintances of these contacts, and so on.[93] This approach undertakes to identify a more extensive web of interrelationships in which the individual of primary concern is embedded. In doing so the agent engaged in the data mining activity identifies subsidiary individuals who may not in fact play any supporting or auxiliary role in unlawful activity.[94] The analysis therefore aims as its objective a more extensive and illustrative relief of context of the initial, narrower conditions of an

---

[90] *See*, for example: Bakhshandeh, Reza, et al. "Degrees of separation in social networks." Fourth Annual Symposium on Combinatorial Search, May 2011, p.18, Available at: http://www.aaai.org/ocs/index.php/SOCS/SOCS11/paper/viewFile/4031/4352, Accessed: 19 January 2013. *See* also: Newman M (2010) Networks: An Introduction. Oxford University Press; Easley D, Kleinberg J (2010) Networks, crowds, and markets: Reasoning about a highly connected world. Cambridge University Press.

[91] Additional research in computational statistics validates the assertion that this clustering effect on social network sites can be substantiated empirically. Ugander et al note the predominance of clustering on the Facebook social network site, which underscores the potentiality of even limited use of data mining capabilities in online social network site analysis to subject a disproportionately large number of citizens to surveillance activity. *See* J. Ugander, B. Karrer, L. Backstrom, C. Marlow, The Anatomy of the Facebook Social Graph, 18 November 2011, p.13, Available at: http://arxiv.org/abs/1111.4503, Accessed: 22 January 2013.

[92] Katherine J. Strandburg, Surveillance of Emergent Associations: Freedom of Association in a Network Society, December 2007, p.6, Available at: http://works.bepress.com/katherine_strandburg/11, Accessed: 22 January 2013.

[93] C. McCue, Data Mining and Predictive Analysis - Intelligence Gathering and Crime Analysis, (Oxford: Elsevier), 2007, p.119

[94] For example, a person communicating with others via a social network site that is suspected of involvement in extremist activity may communicate with groups of people whose characteristics and behaviours vary considerably. Besides maintaining contact with members of an extremist group, she may also use the same mode of communication to liaise with family members and associates in a religious organization. Here, links analysis could be utilised to discern how a broader profile of the suspect and their association with others. While belonging to one group does not necessarily preclude membership in the other (for example, in the aforementioned case, being both a member of an extremist group and being a fellow believer in a religious sect) the use of links analysis is intended to adequately differentiate and discriminate such that the qualities of an association, its nature, be made evident within a wider context.

association. The use of link analysis in profiling activity with respect to social network site data thus presents significant concerns as regards the extent to which this profiling can potentially expose a disproportionate number of legitimate, innocent associations. Hence it harbours the potential to inhibit and curtail free association especially insofar as it may expose a suspect's relations with other individuals and groups that are perhaps marginalized or in some other way socially or politically disfavoured.

The accuracy of the profiles created, which may be subject to further data processing using predictive analytics to model future behaviour, is a further important issue that need be considered. The results of link analysis, in particular, may obscure underlying inaccuracies pertaining to the relationships depicted by the qualification of different associations. For example, where assumptions are made as to how user accounts are utilised (that there be a presumption that a login is used by a single individual being a very real and relevant exemplar in this context, for instance) there exists a discernible risk that the analysis will render inapposite models of associations and related behavioural activity.

The repercussions of misconstruing and misinterpreting data thus imperil law-abiding citizens who may be subject to unwarranted suspicion. This example (that of several individuals using the same login - perhaps for reasons that are perfectly irreproachable - such as for efficiency or other rationales based on the manageability of a limited resource e.g. Internet connectivity, access to computing resources, financial cost, etc.) reflects a reality that cannot simply for the purpose of expediency. Ignoring these complications and impediments to modeling associations and developing insight into behaviour results in an analysis that is far less propitious and limited in its subsequent utility.

The ramifications for individuals incriminated and enmeshed in associations erroneously may seriously infringe upon their personal liberty. For example, should a suspect associate with several contrastive and unrelated groups (again, we might take consider a targeted individual who maintains relations with an extremist group, a moderate political organization and a religious sect) profiling may manifest a categorization of an associate belonging to a legitimate parliamentary lobbying group as an extremist - the delineation between extremist group/political activist organization/religious sect having been obfuscated.

Profiling via 'patterns': intrinsic risks

Pattern-based approaches to identifying and qualifying the nature of associations seek first to identify associated groups using an algorithm that identifies cluster-types. Then, in a second stage, the method probes for potential signatures attributable to the types of group that are of interest (such as an extremist group, terrorist network or organised crime syndicate).[95]Where

[95] J. Millar, Core Privacy - A Problem for Predictive Data Mining (March, 2009), p.104, Lessons From The Identity Trail: Anonymity, Privacy And Identity In A Networked

specific signatures are confirmed the known networks can be examined to discern whether any matching associations may be exposed.

Thus of crucial importance in determining the suitability of this technique is the precision of the clustering algorithm implemented to chart and depict the associational groups within the wider body of data collated and examined; ultimately the exactitude and validity of each search being a reflection of the accuracy of the model utilized to identify groups of interest.[96] The 2007 report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism notes: "Detailed profiles based on factors that are statistically proven to correlate with certain criminal conduct may be effective tools better to target limited law-enforcement resources." [97] Whether in this context the correlations established meets the requirement for being "statistically proven" remains subject to conjecture and resolution.

Exceptional prudence is required when conducting profiling of behaviour using pattern-based network analysis, especially where the inferences drawn are then utilised to extrapolate ensuing behaviour via a predictive approach.[98] Data mining that applies pattern-based searches to elaborate sequences and arrangements from large datasets attempt to discover implicit correlations. Efforts to pinpoint and prevent future criminal activity through the application of pattern-based data mining must acknowledge the limitations of this method in this distinct context.[99] In conducting profiling to uncover these associations, and

---

Society, New York: Oxford University Press, 2009; Available at: On the Identity Trail - Lessons From the Identity Trail
idtrail.org/content/view/799, Accessed 25 February 2013

[96] Strandburg argues that the algorithms developed for the clustering of associations with large networks are inappropriate when analysing social network sites, venturing to proclaim that they are "not particularly accurate" and "computationally expensive" and slow. Strandburg further notes: "To some extent these difficulties are inherent in the closely connected structure of social networks, which renders associations difficult to disentangle and mistaken identifications inevitable." See K. Strandburg, "Surveillance of Emergent Associations: Freedom of Association in a Network Society," in Digital Privacy: Theory, Technologies, and Practices (Alessandro Acquisti, Stefanos Gritzalis, Costas Lambrinoudakis and Sabrina De Capitani di Vimercati, eds., Auerbach Publications, 2008), p.8

[97] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 29 January 2007, A/HRC/4/26, p.7 at para. 33

[98] Boyd notes the perils of becoming too reliant on an unfailing belief in the authenticity of trends extrapolated from data: "It is the kind of data that encourages the practice of apophenia: seeing patterns where none actually exist, simply because massive quantities of data can offer connections that radiate in all directions." See Boyd, Danah and Crawford, Kate, Six Provocations for Big Data - A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, September 2011, p.5 Available at SSRN: http://ssrn.com/abstract=1926431, accessed 25 March 2012

[99] Rubinstein et al note the large data sets needed to make pattern-based analysis viable, hinting at its possible intrusiveness in requiring data generated by the lawful activities of citizens: "Because terrorists do not 'stand out,' intelligence and law enforcement

then parse the multitude of interconnections that are revealed, one may disclose and give prominence to an array of lawful and permitted groups in addition to those that potentially harbour a disposition toward criminality.

Certain groups that are identified in this manner may legitimately desire to minimise their exposure. With justification, such associations may affirm that this differentiation and identification constitutes interference. The impact of this discovery and disclosure cannot be deemed as necessary in a democratic society in the interests of public safety. The notion that a legitimate association would not fear its exposition and subsequent elucidation, regardless of the narrowness of the confines by which this information is divulged, is unreasonable: to otherwise suggest to the contrary would be to affirm that any interaction between two parties, however honourable, might permissibly be subject to unnecessary scrutiny.

Determining the significance of respective associative groups for the purpose of applying predictive methods is therefore problematic. An appreciable difficulty is developing coherent strategy that appreciates the novelty of forecasting scarce and highly sporadic acts (such as those associated with atypical events linked to serious crimes) that be applied with the requisite discrimination in conjunction with the acumen acquired from the identification of associations. Fung however reminds us that that our associations with one another are highly contextualized, and thus the interpretation of the information attributable to these interactions may be especially involute:

> "Responses to information are inseparable from their interests, desires, resources, cognitive capacities, and social contexts. Owing to these and other factors, people may ignore information, or misunderstand it, or misuse it. Whether and how new information is used to further public objectives depends upon its incorporation into complex chains of comprehension, action, and response."[100]

A critical issue is thus how profiling activities appositely discern the appropriate paradigm to comprehend the relational structure (or structures) of divergent groups implicated in serious criminal activity. In order that profiling activity reduces any predilection that it unfairly identifies legitimate associations, it must

---

agents want to do more than rely exclusively on investigations of known suspects. The new goal is to search "based on the premise that the planning of terrorist activity creates a pattern or 'signature' that can be found in the ocean of transaction data created in the course of everyday life. Accordingly, to identify and preempt terrorist activity, intelligence agencies have begun collecting, retaining, and analyzing voluminous and largely banal transactional information about the daily activities of hundreds of millions of people." *See* Rubinstein, Ira, Lee, Ronald D. and Schwartz, Paul M., Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches. University of Chicago Law Review, Vol. 75, 2008; UC Berkeley Public Law Research Paper No. 1116728. Available at SSRN: http://ssrn.com/abstract=1116728, p.261

[100] Fung, Archon, Mary Graham, and David Weil. Full Disclosure: The Perils and Promise of Transparency. New York: Cambridge University Press, 2007, p.187

clearly make distinctions between the relational structures of a group implicated in criminal activity and that of a law-abiding clique. However, such a presumption proves simplistic and untenable. A trait such as a disposition toward communicating in a covert or surreptitious manner could manifest in both types of association.

Those who may be subject to disfavour or discrimination (for example, based on ethnicity, sexual orientation, immigration or employment status or political opinion) could also favour seemingly clandestine modes of conferral. In this regard, Article 49 of the European Code of Police Ethics stipulates that investigations made by law enforcement officials prove impartial and be suitably sensitive to citizens' requirements, stating: "Police investigations shall be objective and fair. They shall be sensitive and adaptable to the special needs of persons, such as children, juveniles, women, minorities including ethnic minorities and vulnerable persons."[101]

Pattern analysis must therefore evidence sensitivity toward these distinctions. An indiscriminate use, and reliance upon, the application of data mining techniques to data collated from social network sites results in the monitoring of a broad range of persons not suspected of any wrongdoing. When combined with other factors influencing the motives for profiling activities, some of these people will be further subject to intrusive surveillance merely on the basis of the profiling itself, again without any suspicion of wrongdoing on their part. Indeed, of key importance here is whether the distinctions drawn are suitably specific, or rather reflect broader "profiles that reflect unexamined generalizations," such that this practice reflects a disproportionate interference.[102] Relevant to this context is Recommendation No. R(87)15 on regulating the use of personal data in the police sector places on the collection of personal data. The appendix to the recommendation affirms that this activity should be limited to reflect the intention of suppressing a specific criminal offence, rather than reflect a broader preventative mandate of an unspecified description. The Appendix to Recommendation No. R(87)15 regulating the use of personal data in the police sector (adopted on 17 September 1987) states, *inter alia*:

> "Principle 2 – Collection of data
> 2.1 The collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence. Any exception to this provision should be the subject of specific national legislation. …"[103]

---

[101] Recommendation Rec(2001)10 of the Committee of Ministers to member states on the European Code of Police Ethics, adopted by the Committee of Ministers 19 September 2001.
[102] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 29 January 2007, A/HRC/4/26, p.7 at para. 34
[103] Council of Europe, Committee of Ministers Recommendation No. R(87) 15 to the Member States on regulating the use of personal data in the police sector, 17 September 1987

Placing an unwavering faith in the capacity of any novel method to deliver unprecedented insight is seldom a wise tactic: it frequently proves premature.[104] Should law enforcement err by injudiciously identifying legitimate association between individuals as constituting malevolent ambitions, one can quickly sow mistrust. Mistrust generates suspicion and augurs unfavourably for the sustainable use of a surveillance practice in a democratic society.

Interference in a person's freedom of association can in turn foster a broader ambivalence in society that undermines minority groups' entitlement to acceptance and equal treatment at the hands of public authorities. Fallacious investigatory actions that expose undisclosed associations, however discretely conducted, are not without their injured parties. The 2007 report of the Special Rapporteur also highlighted the process of profiling practices that single-out persons for enhanced law enforcement attention may contribute to the social construction of groups to whom which suspicion may more generally be applied, noting: "This stigmatization may, in turn, result in a feeling of alienation among the targeted groups."[105]Public security agencies cannot simply internalize the resultant costs and externalities. Rights infringements resulting from false positives (reflecting poor inferential decisions based on either inaccurate depictions of associations or biased characterization of their significance) bare tangible costs, both to those immediately concerned in a specific instance, and more broadly to communities in the longer term.

Profiling activity in general has an appreciable impact on both individuals and communities. Earlier discussion in this paper has highlighted the positive enabling and empowering role that online interaction can play, particularly as regards the disfavoured, and those that feel impeded or at risk from expressing themselves in more traditional fora.[106] Knowledge that interaction and associative behaviour is subject to monitoring can therefore perform a potentially damaging role in allowing individuals to explore and express their identities, thereby constituting an infringement of human dignity. It would be lamentable should society embrace the misuse of a surveillance technique that burdens an injured party with the detrimental impact. Furthermore, one should

---

[104] McCue notes the manifest deficiencies in much of the data used in the context in question: "Regardless of how perfect a data set might seem to be, it almost always has some shortcomings. In law enforcement and intelligence analysis, the data and information generally are anything but perfect." *See* C. McCue, Data Mining and Predictive Analysis - Intelligence Gathering and Crime Analysis, (Oxford: Elsevier), 2007, p.82

[105] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 29 January 2007, A/HRC/4/26, p.7 at para. 57

[106] *See* Redfearn v The United Kingdom, no. 47335/06 §56, where the European Court of Human Rights affirms the protections afforded by Article 11 of the Convention also pertain to the safeguard of associations based on less appealing views or opinions: "the fact remains that Article 11 is applicable not only to persons or associations whose views are favourably received or regarded as inoffensive or as a matter of indifference, but also those whose views offend, shock or disturb."

remain mindful that the disfavoured, especially those whose views and opinions reflect insubstantial minority positions in a pluralist society, are frequently the least empowered in their ability or inclination to protest any such violation of their rights.[107] Recognising this risk, convincing action is needed to preemptively counter the danger that parties seek to conceal an occurrence that constitutes such an infringement. Therein lies an appreciable risk to society that the distress and injury caused vulnerable groups may not prove of sufficient interest or concern to the general public that the implementation of a defective method of surveillance be deemed inexpedient.

Analytical errors, such as the erroneous labeling of association as reflecting suspect activity, or the designation of a group as being illegitimate or, worse still formerly proscribed, possess the capacity to seriously inhibit free association. As discussed earlier, new technologies may materialize unconventional and neoteric forms of associations that are less likely to emerge and be nurtured in other spheres of interaction. In this context it is especially important that we understand how limitations on free association may hinder and restrict a burgeoning milieu in which the exchange of discourse and the imparting of ideas can prove facilitative in a society facing rapid change.

Fundamental rights are indivisible. The nexus of free expression with the freedom to associate and assemble acknowledges their interdependence.[108] Paradigmatic shifts, brought about by innovations in technology, however challenge the supposition that extant constitutions of the rights vis-à-vis association remain cogent and conceptually viable. A hallmark of the evolution social network sites has been their ability to incorporate a plethora of features that enable and facilitate the exchange of ideas. Indeed, it has been argued that this is one of online social networking's greatest achievements.[109]

The evolving functionality of social network sites also however increasingly challenges traditional distinctions made in delineating the notions of 'expression'

---

[107] The value of fora in which groups that represent minority interest can interact was highlighted in an International Civil Liberties Monitoring Group report, which noted that a minority group had experienced "alienation, marginalization and ... a sense of psychological internment." The value of fora in which groups that represent minority interest can interact was highlighted in an International Civil Liberties Monitoring Group report, which noted that a minority group had experienced "alienation, marginalization and ... a sense of psychological internment." *See* International Civil Liberties Monitoring Group, Anti-Terrorism and the Security Agenda: Impacts on Rights, Freedoms and Democracy, February 17, p.5, 2004, Available at: http://quakerservice.ca/wp-content/uploads/2011/05/ReportICLMGPublic_Forum.pdf, Accessed: 22 January 2013.

[108] *See*, for example: Vogt v. Germany (1996) 21 EHRR 205, (17851/91) §64, where the Court notes: "The protection of personal opinions, secured by Article 10 (art. 10), is one of the objectives of the freedoms of assembly and association as enshrined in Article 11 (art. 11)."

[109] *See*, for example: J. Ugander, B. Karrer, L. Backstrom, C. Marlow, The Anatomy of the Facebook Social Graph, 18 November 2011, Available at: http://arxiv.org/abs/1111.4503, Accessed: 22 January 2013.

and 'association'. At this juncture we might perhaps explore an alternative to this conventional distinction; a conception that reflects an approach whereby the two are conjoined. The synthesis of the two elements represents a right to expressive association. Associations do not have to associate for the purpose of disseminating a certain message in order to be entitled to protection rather, as the US Supreme Court adroitly elucidated: "An association must merely engage in expressive activity that could be impaired in order to be entitled to protection."[110]

Expressive association can be seen in two regards. The notion may appear to some as a rather enigmatic formulation derived from a nuanced interpretation of the broader right to free association; or otherwise it appears innate: an entirely uncontrived elucidation.[111] These contrasting distinctions in turn accentuate the difficulties inherent to our finding a reasonable entente. Preserving free association mandates a degree of deference toward parties' autonomy in discerning how they wish to express themselves and converse. We might also contemplate the significance of autonomy in development of our respective individual identities. The nurturing of autonomy is dependent upon the information we are exposed to that in turn shapes our behavior. Intervening action then would only therefore be considered appropriate where it serves compelling interests such that the interference on balance may be justified, as the employment of other less inhibitory means would fail to achieve the necessary objective.

There doubtless exist difficulties in forming a consensus as to how we determine the extent to which the association and interlocution that crystallize through social network sites be subject to protection under existing formulations of rights protection. These challenges stem from rival conceptual renderings as to the intrinsic substance of the relations and associations formed by this method of imparting and conveying ideas. Furthermore, we must afford due consideration to the notion that emerging associations, such as those that appear frequently to develop extemporaneously on social network sites in response to quotidian events, rarely exhibit determinable orders or hierarchies that condition who may protest an infringement of either their individual or collective right. Profiling activity places several constraints on the interchange of ideas on online social network sites. Firstly, in disclosing the existence and constitution of associations it inhibits and encumbers interaction. Second, it may chill association by mistakenly drawing inferences from pattern analysis that incorrectly construes lawful association as reflecting behaviours accredited to illegitimate activity. Finally, imprecision in profiling also harbors the potential to mistakenly render an individual an associate of a group or affiliation incorrectly.[112]

---

[110] Boy Scouts of America v. Dale, 530 U.S. 640 (2000).

[111] D. E. Bernstein, Expressive Association After Dale, George Mason University School of Law - Working Paper Series, 2005, Berkeley Electronic Press, Available at: http://law.bepress.com/, Accessed: 19 March 2013, pp.2-5

[112] The limitations of algorithms in predicting future behaviour was recently highlighted in a technology report by the New York Times, which affirmed: "The algorithms are

In these circumstances it must be considered whether the scope of profiling activity undertaken reflects the least invasive means by which the compelling interest of the party conducted the surveillance is served. Admittedly, in this context there exist recognizable difficulties in determining whether an allegation of a harm incurred by a party can be demonstrated. Nonetheless, scrutiny must be extended such that even where the purpose of surveillance may be deemed legitimate, that purpose cannot be pursued by methods that suppress the fundamental liberties of the individual where alternate, more narrow, means may be employed which manifest less risk of encroachment on these rights.[113]

Established legal precedent proves instructive where it may highlight the extent to which prior technological change has compelled courts to deliberate the adaptation of jurisprudence to novel scenarios.[114] The evolution of technology

---

getting better. But they cannot do it alone. "You need judgment, and to be able to intuitively recognize the smaller sets of data that are most important… to do that, you need some level of human involvement." The report further noted: The inherent difficulties computers face in discerning the nuances of human associations is alluded to in a recent New York Times technology report which noted the limitations of algorithms in parsing data from social network sites. The report noted: "Although algorithms are growing ever more powerful, fast and precise, the computers themselves are literal-minded, and context and nuance often elude them. Capable as these machines are, they are not always up to deciphering the ambiguity of human language and the mystery of reasoning. Yet these days they are being asked to be more humanlike in what they figure out." Indeed, Google Inc. has also noted the role of human curation in data analysis: "There has been a shift in our thinking," said Scott Huffman, an engineering director in charge of search quality at Google. "A part of our resources are now more human curated." The social network site Twitter also used humans rather than rely on algorithms alone for data analysis: "Twitter uses a far-flung army of contract workers, whom it calls judges, to interpret the meaning and context of search terms that suddenly spike in frequency on the service." *See* NYTimes.com, Web Site to Be Investigated for Posting Private Data, 13 March 2013, Available at: http://www.nytimes.com/2013/03/13/us/personal-data-on-well-known-people-is-posted.html?hpw, Accessed: 13 March 2013.

[113] *S. and Marper v. the United Kingdom* may provide some guidance in this respect; with regard to the retention of information where there exists no provision for independent review. The Court held in the *Marper* case that blanket and indiscriminate nature of the power of retention in this instance was not proportionate and did not strike a fair balance in respect of the rights of the individuals concerned. As such, this approach represents a serviceable precedent by which we might measure the likelihood that a resort to a similarly sweeping exercise of power of retention by a law enforcement agency in relation to Internet data, collated for the purposes of profiling, would likely prove disproportionate:
"…in particular, there is no provision for independent review of the justification for the retention according to defined criteria, including such factors as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances." S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, § 119, 4 December 2008

[114] *See*, for example, S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, § 71, 4 December 2008, where the Court notes: "Indeed, bearing in mind the rapid pace of developments in the field of genetics and information technology, the

with regard to the use of profiling in the context of social network site data unquestionably engages the review of the applicability of prior exemplars in relation to changing models of associational behaviour. Existing doctrine however provides us with substantial guidance as to how we may evaluate the permissibility of demands by law enforcement to acquire information pertaining to this associational behaviour, else it risk a breach of privacy.[115]

While the courts have frequently been required to resolve the quandaries presented by evolving surveillance techniques[116] to date case law has dealt almost exclusively with more conventional notions of membership and association; the emergent associations, the means by which groups form, and the technologies deployed by social network sites do not necessarily in each instance represent a replication of the type of activities to which the courts have thus far deliberated and expounded an opinion.[117] Of course, this is not to immediately suggest that prior precedent proves inflexible, or that existing doctrine be supplanted.

Legitimate Aim and Proportionality

Imperative to the assessment of whether the practice of applying predictive analytics to discern the existence of, and nature of, associations between individuals is the proviso that an interference resulting from the use of this surveillance technique should fulfill a legitimate aim. Where the use of this method of surveillance is pursued with a determined and definite purpose then it may be considered to constitute an activity that fulfills a legitimate aim. Should

---

Court cannot discount the possibility that in the future the private-life interests bound up with genetic information may be adversely affected in novel ways or in a manner which cannot be anticipated with precision today."

[115] *See* Amann v. Switzerland [GC], no. 27798/95, § 46, ECHR 2000-II, where the Court affirms: "Such interference breaches Article 8 unless it is “in accordance with the law”, pursues one or more of the legitimate aims referred to in paragraph 2 and is, in addition, “necessary in a democratic society” to achieve those aims."

[116] *See* Kopp v. Switzerland, no. 23224/94 (1998), p.iii. Where the European Court of Human Rights states with regard to the necessary precision of laws where they pertain to evolving technologies: "Law’s “foreseeability” as to meaning and nature of applicable measures: As interception constituted a serious interference with private life and correspondence, it had to be based on a “law” that was particularly precise, especially as the technology available for use was continually becoming more sophisticated."

[117] *See* Hasan and Chaush v Bulgaria, no 30985/96, 2000 [ECtHR] §62. Where the European Court of Human Rights affirms prior assertions that: "The Court recalls that religious communities traditionally and universally exist in the form of organised structures." The notion appears especially inflexible from the outset, particularly the premise that 'religious communities *universally* exist in the form of organised structures'. This affirmation therefore calls to question how the Court may apply such a precedent where future freedom of thought or conscience-related cases that are to be interpreted in the light of Article 11 will be decided where less typical associations are subject to review. The rights of freedom of expression, freedom of religious worship and freedom of association and assembly are interwoven but distinct. These freedoms may cultivate a pluralism that is congenitally sceptical of state orthodoxy.

the process be deployed lacking a specific, identified objective then it may be considered an arbitrary and therefore unlawful imposition on the fundamental rights of those subject to surveillance.

In essence, the determining factor in this consideration is whether profiling proves efficacious in its implementation, and is proportionate.[118] In the deliberation of a specific instance of its use, we need reflect as to the measure of any negative impacts its utilization may render.

The 2007 report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism provides guidance in the more specific context of countering terrorism.[119] However, its recommendations still prove pertinent where we consider other serious crimes, insofar as the methods employed would need to furnish a profile that is sufficiently focused so as to preclude those that do not represent a threat in relation to the pursuit of engaging in serious crime, and still however be sufficiently broad in scope so as to include those that do. Indiscriminate use of profiling for the purposes of substantiating a more general predisposition toward engagement in less serious crimes, or to ascertain more generalized information as regards a propensity for types of association that correlate with statistically significant tendencies or inclinations toward engaging in a broader spectrum of criminal activity, would be unlikely to meet this standard. Lowering the threshold proves problematic where it is suggestive of an acceptance that extensive and universal surveillance, such as that envisaged by the comprehensive use of social network site monitoring, would be justified. This postulation would effectively promulgate the notion that widespread pre-emptive monitoring of individuals' associations with each other would constitute a practice tolerable in a democratic society.

An interesting point arises with regard to the use of other forms of profiling in which ethnic appearance and national origin may be used as proxies for religion.[120] In this context, the use of data mining by way of either pattern-based techniques or links analysis for predictive purposes, to supposedly identify possibly malevolent associations linked with plots to engage in criminal activity,

---

[118] *See* Malone v. the United Kingdom, no. 8691/79 (1984), pp. 32-33, §§ 67-68. Where the Court states: "... Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference."

[119] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 29 January 2007, A/HRC/4/26

[120] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 29 January 2007, A/HRC/4/26, p.7 at para. 50

requires further consideration. Should analytical methods prove effective in identifying and mapping these associations, it might be argued by those wishing to deploy these techniques that it effectively eliminates issue of the proxy as a stand-in; such that religious affiliation more accurately be defined, thus answering the criticism advanced as to its purported inexactitude. This rationale might be applied more widely beyond a religious affiliation, and in turn be used to further the argument that associations sharing particular viewpoints deemed suspect for the purposes of preventing serious crime could also justifiably be subject to surveillance.

The immediate difficultly this prospect raises is the extent to which this mode of reasoning might easily jeopardise the protection of freedom of expression and freedom of association more widely. Were it to be embraced, the modus operandi of social network site analysis would effectively be to monitor all associations in which an identifiable belief or cause could be established. Undeniably, the effect of such an approach would be to seriously encroach on the fundamental rights of citizens, and would undermine the very foundations of a democratic society that fosters pluralism, free association and open debate. Furthermore, the aforementioned scenario, were it to be realised, would raise the issue of over-inclusive profiles. A strategy based on leveraging the data of social network sites to develop broad profiles would exhort law enforcement agencies to treat as suspect an expansive range of individuals' associations with another even while most would present no credible risk to public safety or security. Such an eventuality would struggle to win support where law enforcement resources are limited and need be deployed as effectively as possible.[121]

The jurisprudence in this context affirms that principles extend from existing conceptual approaches to elaborating the fundamental rights concerned where new technological circumstances dictate. Doctrine indeed proves adaptive in the light of change. The principles to which surveillance monitoring be adjudged ought to prove responsive to new circumstances brought about by technological change. This responsiveness necessarily includes recognizing that such change may comprise of relatively inconspicuous innovation such as modifications to existing algorithms applied to pattern or link analysis. Precepts formulated in this context must discern appropriate measures by which whether the technology achieves sufficient discrimination between permissible and illicit behaviour.

Contemplation of the consequence of the indiscriminate application of data mining to online social network sites may draw on an interesting analogy made with respect to the landmark US Supreme Court case *Kyllo v. U.S. in 2001*,[122] where a parallel is made corresponding to the similarities between the arguments thence as to thermal imaging's lack of specificity and the inherently

---

[121] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 29 January 2007, A/HRC/4/26, p.7 at para. 51

[122] *Kyllo v. United States, 533 US 27 - 2001.*

indiscriminate approach intrinsic to profiling of associative behaviour in this context.[123] The proximation references the argument that while the use of thermal imaging by law enforcement renders knowledge that is embedded in accessible data, this intelligence would otherwise not be discernible save by making use of the advanced technology. It corroborates the dictum that advances in surveillance capabilities may generally be categorized in two forms; either they allow for more data to be collected, or they furnish more information from the existing available data: both allow for overly intrusive monitoring.

The acceptability of a technology employed for the purpose of gathering intelligence must depend on the degree to which it is capable of delineating legitimate and non-legitimate activities; its capacity to differentiate is of foremost concern where an inability to adequately distinguish subjects citizens to a disproportionate risk of infringement of their fundamental rights.

The correlations that the analysis of social network sites may yield are quite unlike the type of associational information that may be extrapolated from data by more conventional means (that previously required human resources to laboriously sieve through data and identify connections). Contemporary data mining techniques afford efficiencies that render detailed depictions of implicit structures behind behaviours that differ considerably from prior benchmarks. Furthermore, data mining of social network site data promises to reveal relationships within associations that those within the loosely knit 'structure' (a term used in a rather indefinite sense in this respect) themselves are likely to be unaware. This eventuality cuts to the very heart of whether we continue to appreciate and uphold the constitutive values recognition of freedom of association inheres. A method that conspicuously advertises entirely legitimate associations proves burdensome.

The determination of the reasonableness of the surveillance of online social network sites must inhere an evaluation as to whether the monitoring serves a legitimate and compelling interest.[124] In conducting such a review, however, on must remain mindful of retaining a suitably objective standpoint in discerning the strain unwarranted monitoring places on citizens' inclination to freely share their thoughts and explore relationships with other parties. This is particularly the case where it threatens to expose intimate and expressive associations; the risk of chilling these interactions cannot be dismissed as a relatively imperceptible and acceptable consequence of such activity.

---

[123] K. Strandburg, "Surveillance of Emergent Associations: Freedom of Association in a Network Society," in Digital Privacy: Theory, Technologies, and Practices (Alessandro Acquisti, Stefanos Gritzalis, Costas Lambrinoudakis and Sabrina De Capitani di Vimercati, eds., Auerbach Publications, 2008), p.22

[124] *See* Malone v. the United Kingdom, no. 8691/79 (1984), pp. 32-33, §§ 67-68. The European Court of Human Rights asserts: "… Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power."

Notwithstanding these risks, the cognizance that the encroachment into individuals' personal lives nonetheless continues to be jeopardised by averments that entreat the population to disregard the ineffaceable value of confidentiality in our association with others: a diminution of this fundamental precept is indeed climacteric. In this context, a critical facet of the challenge to rights protection is therefore the notion that we allow the erosion of our imprescriptible entitlement to secure our personal communications from intrusion without fear that this be construed as attesting to a desire to conceal. Posner make the assertion that, indeed, this impulse is but a pretext; the real motive being subterfuge:

> "[W]hat they want, I think, is mainly something quite different from seclusion: they want more power to conceal information about themselves that others might use to their disadvantage."[125]

The quandary finds a suitable elision in the popular refrain that persons with nothing to hide may rest at ease, and relieve themselves therefore of any anxiety as to the possible attrition to their freedom that this indifference encourage.[126] At question, therefore, is the premise that one might wish to conceal discreditable facts. From this contention necessarily arises the question as to what might constitute the type of conduct tending to bring harm to one's reputation? Essentially the limits are possibly boundless. We should, therefore, accept the imperative that this is for the individual herself to freely discern, absent any coercion to justify their estimation; the foundation for this assumption being the simple premise that we presume an individual's behaviour to be law-abiding absent any grounds to suspect otherwise. The obverse approach would be to tacitly accept the notion that this mode of deploying surveillance achieves a requisite compromise between providing security for a population and ensuring that our rights are still to be respected. Should the latter proposition be accepted we face a worrying development whereby, if the same reasoning be applied to analogous circumstances, we risk instigating a shift in practice, and indeed convention, that irrefutably sanctions a

---

[125] R.A. Posner, The Economics of Justice, Cambridge, Mass., Harvard University Press, 1981, p.271

[126] Solove notes that when discussing whether government surveillance and data mining pose a threat to privacy, many people respond that they have nothing to hide - this argument permeates popular discourse on security issues, and is illustrated by one blogger's comment that: "I don't have anything to hide from the government. I don't think I had that much hidden from the government in the first place. I don't think they care if I talk about my ornery neighbour." See, Solove, Daniel J., 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. San Diego Law Review, Vol. 44, p. 745, 2007; GWU Law School Public Law Research Paper No. 289. Available at SSRN: http://ssrn.com/abstract=998565, Accessed: 23 February 2013. The citation references a May 2006 blog post of user 'annegb' on Solove's Concurring Opinions site at http://www.concurringopinions.
com/archives/2006/05/is_there_a_good.html#comments.

pervasive and penetrating role for the conduct of ubiquitous surveillance of associations.[127]

Individuals may foster associations they wish to conceal simply because they find them to be an embarrassment, or otherwise would rather others didn't know. Evidently, to accept this reality is not just to attest that certain persons have a hidden agenda of which society should genuinely be concerned, justifying a consequential suspicion that would warrant placing their interactions with others under observation. On the contrary, it suggests recognition that each of us must remain unfettered by an obligation to expose, explain or justify our every legitimate association. A similarly schematic approach to the review of personal associations in our online communication, based on a line of reasoning that contends no harm results where insentient entities (namely computers) are responsible for the profiling of social network site data, is again fallacious.[128]

Casady forewarns of the significant risks of 'differential policing' based on this type of analysis, whereby more invasive monitoring of activity by law enforcement may account to a recipe for deteriorating community relations between police and minority groups, reflecting a perceived lack of procedural justice, accusations of indiscriminate profiling, and thus threaten police legitimacy.[129]

Critically, whether a pattern-based analysis proves permissible remains contingent on the precision of the algorithm employed and its capacity to distinguish between those associations relevant to an investigation and those that are innocuous. At issue then is the algorithm's ability to discriminate sufficiently. Should it prove deficient in this regard, entirely innocent associations will be disclosed. Complicating this issue is the reality that the

---

[127] Lyon's appraisal also underscores the importance of our grasping the significance this shift mild herald, noting: "[C]omputers have become essential for so many everyday communications, analyses of networks of social relations cannot but include reference to them. This is the 'technoculture.' Frequently, however, the focus is on how fresh forms of relationship are enabled by the new technologies rather than on how power may also be involved in ways that limit or channel social activities and processes." *See* D. Lyon, Surveillance, Power, and Everyday Life, Oxford University Press, New York, 2007, p.15

[128] Calo, for example, offers a lucid articulation of the perils of such an approach: "[H]uman beings need not physically review personal information for that information to form the basis of an adverse action. There does not have to be a human observer who gathers and misuses information. Machines are perfectly competent to comb through private information and use it to make automatic decisions that affect us in tangible and negative ways." *See* M. Ryan Calo, The Drone As Privacy Catalyst, 64 STAN. L. REV. ONLINE 29 December 12, 2011, p.21, Available at: http://www.stanfordlawreview.org/, accessed 12 February 2012

[129] T. Casady, Police Legitimacy and Predictive Policing, March 2011, Available at: http://www.nij.gov/topics/technology/maps/gps-bulletin-v2i4.pdf, Accessed: 19 January 2013, p.1

analysis of social network data is still in its infancy.[130] Furthermore, the situation is made more complex still by the perpetual changes being made to the sites. One service is, for example, developing the capability to 'auto-degrade' online associations where a threshold for communication is not met: evolving functionality therefore represents a very real challenge to the credibility of any analysis, save a regular cycle of suitably responsive software updates.[131]

It is questionable whether pattern-based analysis in predictive analytics can at this point in time allow for sufficiently rigorous discrimination between different types of association based on the current state-of-the-art. In addition, a further decisive factor need be considered; the cognizance that, with respect to surreptitious associations such as those that may be attributable to extremist or terrorist groups, little acumen exists as to how these organisations effectively function in terms of their modes of association. Thus the task of delivery of plausible results from quantitative analysis is seriously hampered where pertinent data is acutely absent.

Mitigation of this paucity of information cannot simply be achieved by anticipating a more indiscriminate use of these tools in the hope that they will identify a broader range of associations from which one might 'pick' those that appear to warrant further examination. The result would reflect a wholesale and indiscriminate dragnet. In effect constituting an expansive and indeterminate search for any association between individuals however innocuous. To accept such an approach would be to agree to subject all online social network site interactions to review: an unfavorable proposition given the level of intrusion it would represent. The European Code of Police Ethics should in this context be considered in respect of its provision whereby "Police organisations shall be ready to give objective information on their activities to the public, without disclosing confidential information."[132] If pattern-based analysis is to be broadly implemented for the purposes of profiling, it efficacy must be made subject to review: transparency is essential in building public trust.

The use of targeted link analysis, based on data collated from social network sites for the purpose of analysing and predicting future behaviours, should also be approached with caution. Inferences drawn as to future behaviour of an individual, based on historical associations with other individuals and groups,

---

[130] *See* J. Ugander, B. Karrer, L. Backstrom, C. Marlow, The Anatomy of the Facebook Social Graph, 18 November 2011, Available at: http://arxiv.org/abs/1111.4503, Accessed: 22 January 2013.

[131] Fast Company, Path Explores Ways To End Awkward Friendships: It's Not You, It's My Bot, 15 march 2013, Available at: http://www.fastcompany.com/3007008/tech-forecast/path-explores-ways-end-awkward-friendships-its-not-you-its-my-bot, Accessed: 19 March 2013

[132] Recommendation Rec(2001)10 of the Committee of Ministers to member states on the European Code of Police Ethics, adopted by the Committee of Ministers 19 September 2001.

remains problematic.[133]As link analysis necessitates the review of a distance associations - mining data relating to connections of the second or third order, rather than immediate connections - it therefore represents a considerably more intrusive means of discovery than prior methods which would target more traditional lists and directories pertaining to membership or affiliation. Significantly, this form of analysis encroaches on the fundamental rights of those individuals who are themselves not directly subject to a specific search for information, but fall within the scope of enquiry simply for having established in some way a distant connection with those that have.

Thus one immediately discernible problem with these broad approaches to extrapolating malevolent plots is their extensive sweep, which constitutes a markedly disproportionate approach to addressing a distinct suspicion in relation to an individual's behaviour. The technique intends to furnish an elucidation of the wider context of a person's associations in relation to one another. However, this corollary proves problematic as it inexorably divulges the attributes of a large volume of innocent associations.[134] At issue here then is the relative proximity of different individuals i.e. the strength of the ties of the association. Whereas it may be considered reasonable to conduct an analysis that reveals the nature of those immediately in direct communication with a suspect, revealing the wider networks of association is clearly inapposite in most circumstances and reflects a disproportionate interference.

Conclusion

Any shift toward greater integration of predictive analytics in profiling populations in Europe should only occur where sufficient safeguards are implemented to protect fundamental rights. In addressing the concerns to which one has thus far alluded, we need reflect as to how we draw distinctions between and, indeed, conceptualize such rights. Advancements in technology herald novel capabilities that necessitate our contemplating how we distinguish the intersection of principles such as privacy, freedom of association, freedom of thought and conscience, and the prohibition of discrimination. The indivisibility,

---

[133] McCue argues that link analysis in profiling activity requires human intelligence to deliver meaningful results: "Link analysis tools can be used to identify relationships in the data… There are some limitations to link analysis; however, domain expertise and a good understanding of the concept behind link analysis can help the analyst interpret the results." C. McCue, Data Mining and Predictive Analysis - Intelligence Gathering and Crime Analysis, (Oxford: Elsevier), 2007, p.119

[134] Lyon argues that pervasive monitoring of social network sites raises fundamental questions as to social justice: "[O]rdinary people may feel that they are more vulnerable to intrusion, the use of searchable databases for categorizing and profiling means that deeper questions of power are involved… which means that such surveillance is implicated in basic questions of social justice, to do with access, risk distribution and freedom." *See* D. Lyon, Surveillance, Power, and Everyday Life, Oxford University Press, New York, 2007, p.15

interdependence and interrelatedness of rights evoke the criticality of our recognizing the intrinsic value of protecting human dignity.[135]

This recognition reflects an appreciation that impeding one right may in turn restrain the enjoyment of another, and hinder the fulfillment of providing the conditions under which a person may satisfy their developmental, physical, psychological and spiritual needs. Furthermore, we need also consider the role of participation and inclusion in society, in addition to the principle of equality between individuals - the prohibition of discrimination, as attributes a democratic society necessitates for its own continuance.

Absent this realization, there exists a heightened risk by which the conditions for rights infringement may develop. In this context the difficulties and exceptions the implementation of predictive profiling may present requires our anticipating how existing precedent may guide our formalizing a coherent, lucid response that effectively articulates the parameters which it may be utilised, and regulated. Our response therefore necessitates an appreciation as to how the individual rights are framed and delineated, and how one may reexamine these distinctions in the light of the novel scenarios we now apprehend.

Profiling which implements predictive modeling techniques based on the collation of data from social network sites risks infringing an individual's right to privacy. Enabling the enjoyment of this right places an incumbent duty upon states to prevent unlawful or arbitrary interferences with privacy.[136] Predictive profiling of social media by law enforcement proves especially problematic where its efficacy is largely dependent upon a broad, sweeping analysis of communications. Conceptually, a crucial distinction is that by which public authorities may determine that the use of 'open source intelligence' obviates the requirement to duly consider the right to respect for private life, including private communications.[137]The inception of a class of information and communication based the invariably nebulous and indefinite premise of 'open

---

[135] Regarding the interdependence of rights such as those pertaining to expression and association see, for example, UN Human Rights Committee General Comment 25. Whilst the UN Human Rights Committee General Comment 25 addresses more specifically Article 25 of the ICCPR (relating to the rights of individuals to participate in the public affairs), it nonetheless specifies that freedom of association "is an essential adjunct to the rights protected by article 25."[135] General Comment 25 also attests to the role of association in facilitating the conduct of public affairs where: "Citizens also take part in the conduct of public affairs by exerting influence through public debate and dialogue with their representatives or through their capacity to organize themselves. This participation is supported by ensuring freedom of expression, assembly and association." *See* UN Human Rights Committee, General Comment No. 25: The right to participate in public affairs, voting rights and the right of equal access to public service (Art. 25) (1996) at para. 26

[136] Article 17 of the ICCPR states: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, or correspondence…" and affirms "Everyone has the right to the protection of the law against such interference or attacks."

[137] Article 8, European Convention on Human Rights; Article 7, Charter Of Fundamental Rights Of The European Union

source information' is imprudent; in essence the concept represents an inherently indefinable and ambiguous notion. Reasoning that attempts to categorize and render essentially interpersonal communications as public dialogue, bereft of the privacy protections existing legal provisions furnish, are therefore unsound. Accepting such a shift would be to begin to institute a rationale that undermines a principle of the inviolability of our personal communications absent a sound, compelling justification.

Implementing the use of predictive analytics in the profiling of social network sites can be reconciled with respect to an individual's right to privacy where the interference proves necessary and proportionate. An expansive, wide ranging surveillance programme such as that which social network site monitoring may inhere risks a disproportionate intervention in, and an infringement of, a person's right to privacy where the public authority conducting the activity cannot satisfactorily articulate an explicit justification for the intervention with regard to its anticipated objective. In this regard, whilst it may be argued that the surveillance targets the prevention of disorder or crime, the interference must prove proportionate to the real benefit towards the objective pursued from which the infringement arises. Implementing social network site analysis to monitor and prevent crime based on a blanket and insufficiently selective method likely cannot constitute a proportionate response in certain circumstances. Should the surveillance target serious crime that poses a distinct threat to national security or public safety, for example, its implementation still requires that it be achieved in a measured way, incorporating steps to curtail and minimise the impact on human rights where appropriate. The focus of predictive analytics in discerning from seemingly disparate and unrelated data possible threats renders qualifying whether it represents a proportionate response particularly problematical. Further, it proves difficult to articulate whether it is reasonable and necessary in a democratic society to a implement a measure that characteristically provides its rationale only after having established a suspicion; an expansion of this principle would risk allowing for any monitoring activity should it eventually discern grounds upon which it could be justified (absent any initial foundation); the ramifications of such a precedent would clearly prove destabilizing of society where the dispensation may clearly be abused.

The potentiality for the surveillance of social network sites and the deployment of predictive analytics to overreach the prohibition on discrimination is, in certain regards, rather subtle where it may be perceived as constituting a sweeping and inclusive method (and thus be less inclined to exhibit a bias). The nuances and subtleties in the practice of surveillance are constitutive to discriminatory procedures. A particular risk arising in the utilization of predictive analytics is that those persons conducting monitoring fail to appreciate the decision-making processes integral to the application. Implicit in the acuity of an application or, conversely its imprecision, will be the quality of the decision-making inherent to its design and build. Several risks in this respect can be identified. A significant risk inherent to an over reliance in the reputed objectivity of software analytics is the notion that the algorithms upon which they manifestly depend are entirely impartial; reflecting a flawless capability to

interpret absent any predisposition or bias. To accept this assertion in fact proves misguided; the inherent value of a cogent analytical capacity assumes value judgments inform its competences. Thus we need remain mindful of the possibility that discriminatory practices may become embedded and perpetuated within the profiling activity. Crucially, care should be taken to ensure that interpretative modes integral to predictive analytics do not veil questionable practices that foster discriminatory actions. Absent a vigilant approach monitoring activity may in fact exacerbate and further magnify existing inequalities and thereby undermine a central tenet of human rights protection.

The use of predictive analytics to profile associations for the purpose of discerning a propensity to be involved in unlawful activity may furnish benefits, but also has discernible pitfalls. Greater transparency is needed with regard to the reliability, performance and operation of systems deployed by law enforcement and the intelligence services that integrate predictive analytics in operational decision-making. Further questions also arise as regards the capacity of public security agencies to fully leverage the capabilities of the systems and, at the same time, understand their inherent limitations. The hyperbole of predictive analytics vendors contrasts sharply with the understated rhetoric of those in data science that understand the inherent value of human decision-making in effectively rendering the requisite precision essential to these processes.

Central to this anxiety is a consternation that this form of surveillance engenders a genuine transfiguration in the extent to which monitoring of our associations and relations could permeate a society; this pervasiveness proving an unwelcome influence that engenders subtle changes in our behavior and in turn is highly disruptive to social interactions. The intrinsic value of free association in a democratic society is subject to interpretation, where different perceptions place a contrasting emphasis on the value of individual and shared identities. Our identities however are in part relational; meaning that they are shaped by social interactions and, crucially, by way of both the consciousness of ourselves, and our sentience toward others' observation. Surveillance therefore indubitably plays a role in shaping this dynamic.

Where the apparatus of the state adopts vast technologies of surveillance and classification our democracy may be gradually reordered in a way that we as yet appear only to have a cursory understanding. Improperly implemented, the use of predictive analytics in monitoring social network sites could prove extremely contentious owing to the harm it may inflict. Conflict and division may foster the conditions in which crime burgeons. If misused, it may precipitate a form of social control whereby influence is improperly exerted over individuals, with populations subject to segmentation based on the perceived threat its constituent associations may pose to public security.[138] Presaging this possible

[138]Rosen argues that pervasive monitoring, such as constituted by widespread use of social network site analysis by law enforcement, threatens values of equality in ways that could transform the relationship between citizens and their government. *See* J. Rosen, The Naked Crowd: Reclaiming Security And Freedom In An Anxious Age, 2003,

eventuality, a law enforcement officer recently averred: “Widely-available large data sets and new analytical tools are transforming policing. Our technological capabilities have grown faster than our capacity to understand and react to the ethical implications of these new capabilities.”[139]

All-important, then, is an appreciation of the magnitude this change reflects. Where data analysis intersects with behavioral analysis we see seismic shifts in terms of how everyday associations are interpreted. The implications are tremendous; the impact of this activity will potentially resonant across many facets of our lives. In essence, acquiescence to these practices absent meaningful public debate will foster a climate of opacity; fertile territory for mistrust and marginalization within society.[140] However, others contend that predictive policing strategies to ameliorate crime prevention can be achieved without participating in overzealous monitoring and unnecessary profiling.

Should the urge to press ahead with more routine use of predictive analytics prevail, those charged with its implementation consider need consider how best it can be employed to benefit and empower prevention strategies in the long term, while winning the confidence of the public by ensuring greater transparency as to how it is being implemented. In the opinion of the author there indeed exists an ambiguity as to how fears raised as to the negative impact of predictive profiling may be allayed.[141] Deployment of this evolving technology requires a coherent and unambiguous vision. Should the urge to press ahead

---

Available at: http://www.law.fsu.edu/faculty/2003-2004workshops/rosen.pdf, Accessed: 19 January 2013, p.27

[139]Casady's assiduous examination of the implicit challenges a predictive-oriented approach and underscores the fact that amongst certain law enforcement officers there exists the concern that when misemployed it represents a possible threat to peaceable relations in communities, noting: "As place-based policing, hot spot policing, intelligence-led policing, and information-based policing merge into the science and practice of predictive policing, police will confront increasingly complex ethical issues." T. Casady, Police Legitimacy and Predictive Policing, March 2011, Available at: http://www.nij.gov/topics/technology/maps/gps-bulletin-v2i4.pdf, Accessed: 19 January 2013, p.1

[140] Indeed, the Special Rapporteur highlighted in a 2007 report the crucial role intelligence gathering plays in preventative law enforcement operations, noting that the ongoing support of police activities would remain dependent upon their securing communities' support. *See* UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 29 January 2007, A/HRC/4/26, p.7 at paras. 58 & 62

[141] The possibility of predictive profiling playing a role akin to social engineering is not unfathomable. At the first Predictive Policing Symposium, held in November 2009 in Los Angeles, and attended by European law enforcement officials, it was noted that: "Police who engage in predictive analytics must keep safety, crime reduction, and quality of life in mind... In the future, panelists suggest it be used for managing budgets and personnel, monitoring offenders, and *planning safe* and *economical* neighborhoods.” Note: emphasis added. *See* T. Casady, Police Legitimacy and Predictive Policing, March 2011, Available at: http://www.nij.gov/topics/technology/maps/gps-bulletin-v2i4.pdf, Accessed: 19 January 2013, p.3

with more routine use of predictive analytics prevail, those charged with its implementation consider need consider how best it can be employed to benefit and empower prevention strategies in the long term, while winning the confidence of the public by ensuring greater transparency as to how it is being implemented. Absent any agreement as to what the technique should accomplish, or where the boundaries should lie as to its implementation, there will continue to be confusion as to its place in a broader strategy of providing security for our communities.

Bibliography

Accenture, Analytics in Action: Breakthroughs and Barriers on the Journey to ROI, 2013, Available at: http://www.accenture.com/SiteCollectionDocuments/us-en/landing-pages/analytics-in-action/accenture_analytics_in_action_survey.pdf, Accessed: 19 January 2013

A. Acquisti & R. Gross, Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook, Privacy Enhancing Technologies Workshop (PET), 2006, Available at: http://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf , Accessed: 23 February 2013.

ARTIS Research, Network Analysis, Available at: http://artisresearch.com/?page_id=2337, Accessed: 19 January 2013

Bakhshandeh, Reza, et al. "Degrees of separation in social networks." Fourth Annual Symposium on Combinatorial Search, May 2011, p.18, Available at: http://www.aaai.org/ocs/index.php/SOCS/SOCS11/paper/viewFile/4031/4352, Accessed: 19 January 2013

Barabasi, A.L., Linked: The New Science of Networks, Perseus Group, 2002, and Carrington, P.J., Scott, J. Wasserman, Models and Methods in Social Network Analysis, Cambridge University Press, New York, 2005

Bernstein, D.E., Expressive Association After Dale, George Mason University School of Law - Working Paper Series, 2005, Berkeley Electronic Press, Available at: http://law.bepress.com/, Accessed: 19 March 2013

Berry, D.M., The Computational Turn: Thinking About The Digital Humanities, Culture Machine, Vol 12, 2011, p.12, Available at: www.culturemachine.net, Accessed 2 February 2013

Bollier, D. (2010) 'The Promise and Peril of Big Data', Available at: http://www.aspeninstitute.org/publications/promise-peril-big-data, Accessed 12 January 2012

Briggs, P., Future Identities: Changing identities in the UK – the next 10 years, UK Government Office for Science, January 2013

Butts, C.T., Social network analysis: A methodological introduction, Asian Journal of Social Psychology (2008)

Boyd, Danah & Crawford, Kate, Six Provocations for Big Data (September 21, 2011). A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, September 2011. Available at SSRN: http://ssrn.com/abstract=1926431 or http://dx.doi.org/10.2139/ssrn.1926431

Calo, M.R., The Drone As Privacy Catalyst, 64 STAN. L. REV. ONLINE 29 December 12, 2011 , pp. 29-33, Available at: http://www.stanfordlawreview.org/, Accessed 12 February 2012

Casady, T., Police Legitimacy and Predictive Policing, March 2011, Available at: http://www.nij.gov/topics/technology/maps/gps-bulletin-v2i4.pdf, Accessed: 19 January 2013

Castelluccia, C., Behavioural Tracking on the Internet: A Technical Perspective, in S. Gutwirth et al. (eds.), European Data Protection: In Good Health?, Springer, 2012

Cisco Inc., Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2011–2016, Available at: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html , Accessed 22 February 2012

Citron, D. K., Technological Due Process. U of Maryland Legal Studies Research Paper No. 2007-26; Washington University Law Review, Vol. 85, pp. 1249-1313, 2007. Available at SSRN: http://ssrn.com/abstract=1012360

Clarke, R., Information Technology and Dataveillance, November 1987, Available at: http://www.rogerclarke.com/DV/CACM88.html, Accessed: 19 January 2013

Cohen, Julie E., Privacy, Visibility, Transparency, and Exposure. University of Chicago Law Review, Vol. 75, No. 1, 2008; Georgetown Public Law Research Paper No. 1012068, p.186, Available at SSRN: http://ssrn.com/abstract=1012068, Accessed 13 March 2012

De Rosa, M., Data Mining and Data Analysis for Counterterrorism, March 2004, Center for Strategic and International Studies (CSIS), p.6, Available at: http://csis.org/files/media/csis/pubs/040301_data_mining_report.pdf, Accessed: 22 January 2013.

Manuel Egele, Christopher Kruegel, Engin Kirda, and Giovanni Vigna. PiOS: Detecting Privacy Leaks in iOS Applications. In Network and Distributed System Security Symposium, NDSS 2011, San Diego, CA, USA, 2011

European Police College (CEPOL), Cross-European Approaches to Social Media as a Tool for Police Communication, Issue 6 - Winter 2011/12, p.11, Available at: http://www.composite-project.eu/tl_files/fM_k0005/AB%20Downloads/Denef+Bayerl+Kaptein_6_Bulletin.pdf, Accessed: 19 January 2013

Fast Company, Path Explores Ways To End Awkward Friendships: It's Not You, It's My Bot, 15 march 2013, Available at: http://www.fastcompany.com/3007008/tech-forecast/path-explores-ways-end-awkward-friendships-its-not-you-its-my-bot, Accessed: 19 March 2013

Gelman, L.A., Privacy, Free Speech, and 'Blurry-Edged' Social Networks (November 1, 2009). Boston College Law Review, Vol. 50, No. 5, 2009, p.1329, Available at SSRN: http://ssrn.com/abstract=1520111, Accessed: 19 January 2013.

Gibson, S., Open Source Intelligence An Intelligence Lifeline, RUSI Journal, February 2004, Available at: http://www.rusi.org/downloads/assets/JA00365.pdf, Accessed: 22 January 2013.

Glassman, M., (2012). Occupying the Noosystem: The Evolution of Media Platforms and Webs of Community Protest, Berkeley Planning Journal, 25(1). ucb_crp_bpj_11730. Available at: http://www.escholarship.org/uc/item/5ws9b7f5, Accessed: 19 January 2013.

Guzik, K., Discrimination by Design: Data Mining in the United States's 'War on Terrorism', Surveillance & Society, Vol 7, No 1 (2009), Available at: http://www.surveillance-and-society.org/ojs/index.php/journal/article/viewArticle/design , Accessed 1 February 2012

Hammond, S., Offender Profiling Of Sexual Offences, Broadmoor Hospital, 2007, p.3, Available at: http://www.ramas.co.uk/offender_prof.pdf, Accessed: 22 January 2013

Harcourt, B. E. (2003). The shaping of chance: Actuarial models and criminal profiling at the turn of the twenty-first century. The University of Chicago Law Review, 70

HMIC, The rules of engagement - A review of the August 2011 disorders, 2011, Available at: http://www.hmic.gov.uk/media/a-review-of-the-august-2011-disorders-20111220.pdf, Accessed: 19 January 2013

Kim, M., "The Right to Anonymous Association in Cyberspace: US Legal Protection for Anonymity in Name, in Face, and in Action", (2010), p.52, Available at: http://www.law.ed.ac.uk/ahrc/script-ed/vol7-1/kim.asp, Accessed: 19 March 2013

Koops, Bert-Jaap, Some Reflections on Profiling, Power Shifts, and Protection Paradigms (June 2008), p.1, Profiling The European Citizen, Hildebrandt & Gutwirth, eds., Springer, 2008. Available at SSRN: http://ssrn.com/abstract=1350584

Lewis, D. K., (1986). On the Plurality of Worlds. Blackwell Publishers.

Lohr, S., How privacy vanishes online, March 17 2010, Available at: http://www.nytimes.com/2010/03/17/technology/privacy.html. Accessed: 23 February 2013

Lyon, D., Surveillance, Power, and Everyday Life, Oxford University Press, New York, 2007

McCue, C., Data Mining and Predictive Analysis - Intelligence Gathering and Crime Analysis, (Oxford: Elsevier), 2007

Frank, R., C. Cheng, V. Pun, Social Media Sites: New Fora for Criminal, Communication, and Investigation Opportunities, Research and National Coordination Organized Crime Division Law Enforcement and Policy Branch Public Safety Canada, Report No. 021, 2011, 2011, p.22, Available at: http://www.sfu.ca/iccrc/content/PS-SP-socialmedia.pdf, Accessed: 22 January 2013

Fung, Archon, Mary Graham, & David Weil. Full Disclosure: The Perils and Promise of Transparency. New York: Cambridge University Press, 2007

Jerry, K., Information Privacy in Cyberspace Transactions, Stanford Law Review, Vol. 50, p.1260, 1998. Available at SSRN: http://ssrn.com/abstract=631723, Accessed 12 May 2012

Lockwood, S., Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators, 18 HARV. J.L. & TECH (2004)

Microsoft Inc. Research, 'A Golden Era of Insight: Big Data's Bright Future', 15 February 2013, Available at: http://www.microsoft.com/en-us/news/features/2013/feb13/02-15BigDataHorvitz.aspx, Accessed: 22 January 2013.

Millar, J., Core Privacy - A Problem for Predictive Data Mining (March, 2009), p.104, Lessons From The Identity Trail: Anonymity, Privacy And Identity In A Networked Society, New York: Oxford University Press, 2009; Available at: On the Identity Trail - Lessons From the Identity Trail
idtrail.org/content/view/799, Accessed 25 February 2013

S. Nelson, J.Simek 7 J.Foltin, The Legal implications of Social Networking, 22 Regent U. L. Rev. 1 (2009-2010),

Nielsen, State Of The Media: The Social Media Report 2012, April 2012, p.2 Available at: http://www.nielsen.com/us/en/reports/2012/state-of-the-media-the-social-media-report-2012.html, Accessed: 22 January 2013.

Newman, M., (2010) Networks: An Introduction. Oxford University Press; Easley D, Kleinberg J (2010) Networks, crowds, and markets: Reasoning about a highly connected world. Cambridge University Press

NYTimes.com, Web Site to Be Investigated for Posting Private Data, 13 March 2013, Available at: http://www.nytimes.com/2013/03/13/us/personal-data-on-well-known-people-is-posted.html?hpw, Accessed: 13 March 2013

Parker, R.B., A Definition of Privacy, 27 RUTGERS L. REV. 275, 280 (1974)

Parsell, M., Pernicious virtual communities, Ethics and Information Technology (2008) 10:41–56, Springer Available at:
https://www.hci.iastate.edu/REU09/pub/Main/CraftOfResearch/Parsell.pdf, Accessed: 19 January 2013.

Posner, R.A. "Privacy, Surveillance, and Law." 75 University of Chicago Law Review 245 (2008).

Rachels, J., Why Privacy Is Important, in Philosophical Dimensions of Privacy: An Anthology, Ferdinand D. Schoeman, ed., Cambridge: Cambridge University Press, (1984

Roberts, J.A., Profiling Levels of Socially Responsible Consumer Behavior: A Cluster Analytic Approach and Its Implications for Marketing, Journal of Marketing Theory and Practice, Vol. 3, No. 4 (Autumn, 1995), pp. 97-117

Rosen, J. The Naked Crowd: Reclaiming Security And Freedom In An Anxious Age, 2003, Available at: http://www.law.fsu.edu/faculty/2003-2004workshops/rosen.pdf, Accessed: 19 January 2013, p.27

Rubinstein, Ira, Lee, Ronald D. and Schwartz, Paul M., Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches. University of Chicago Law Review, Vol. 75, p. 261, 2008; UC Berkeley Public Law Research Paper No. 1116728. Available at SSRN: http://ssrn.com/abstract=1116728

D. Runtzen & J. Zenn, Association and Assembly in the Digital Age, The International Journal of Not-for-Profit Law, Volume 13, Issue 4, December 2011, Available at: http://www.icnl.org/research/library/files/Transnational/Assoc%20Assemb%20Digital%20Age.pdf, Accessed: 19 January 2013.

Ryan, M.R., The Boundaries of Privacy Harm (July 16, 2010). Indiana Law Journal, Vol. 86, No. 3, 2011. Available at SSRN: http://ssrn.com/abstract=1641487

SAS Institute Inc., How Social Media Can Help Win the Battle for Public Security, 13 July 2012, Available at: http://www.memex.com/content/how-social-media-analytics-can-help-win-battle-public-security, Accessed: 19 January 2013

Seifert, J. W., Data Mining And Homeland Security: An Overview, CRS Report RL31798, 2006.

Slater, M.D., Reinforcing Spirals: The Mutual Influence of Media Selectivity and Media Effects and Their Impact on Individual Behavior and Social Identity, Communication Theory, Volume 17, Issue 3, pp. 281–303, August 2007

Smith, D., Real-time Big Data Analytics: From Deployment to Production, Revolution Analytics, Available at: http://www.revolutionanalytics.com/news-events/free-webinars/2012/real-time-big-data-analytics/, Accessed: 19 January 2013

Solove, Daniel J., Reconstructing Electronic Surveillance Law. George Washington Law Review, Vol. 72, 2004, p.1708 Available at SSRN: http://ssrn.com/abstract=445180 or http://dx.doi.org/10.2139/ssrn.445180, Accessed 13 March 2012

Solove, Daniel J., 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. San Diego Law Review, Vol. 44, p. 745, 2007; GWU Law School Public Law Research Paper No. 289. Available at SSRN: http://ssrn.com/abstract=998565, Accessed: 23 February 2013

Strandburg, K., "Surveillance of Emergent Associations: Freedom of Association in a Network Society," in Digital Privacy: Theory, Technologies, and Practices (Alessandro Acquisti, Stefanos Gritzalis, Costas Lambrinoudakis and Sabrina De Capitani di Vimercati, eds., Auerbach Publications, 2008)

O. Tene & J. Polonetsky, Privacy In The Age Of Big Data: A Time For Big Decisions, 64 STAN. L. REV. ONLINE 63, February 2, 2012

Tene, O., Privacy: The New Generations (November 17, 2010). International Data Privacy Law, 2010. Available at SSRN: http://ssrn.com/abstract=1710688

Thompson, R., Radicalization and the Use of Social Media, Journal of Strategic Security Volume 4 Issue 4, 2011

J. Ugander, B. Karrer, L. Backstrom & C. Marlow, The Anatomy of the Facebook Social Graph, 18 November 2011, p.1, Available at: http://arxiv.org/abs/1111.4503, Accessed: 22 January 2013

UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 29 January 2007, A/HRC/4/26

Uteck, A., Ubiquitous Computing And Spatial Privacy (March, 2009), p.89, Lessons From The Identity Trail: Anonymity, Privacy And Identity In A Networked Society, New York: Oxford University Press, 2009; Available at: idtrail.org/content/view/799, Accessed 13 March 2012

S Watt, M Lea, & R Spears, "How Social is Internet Communication? A Reappraisal of Bandwidth and Anonymity effects" in S Woolgar (ed) Virtual Society?: Technology, Cyberbole, Reality (2002)