Ethics and Privacy in National Security and Critical Infrastructure Protection

Jennifer Betts and Sakir Sezer
School of EEECS
Queens University Belfast
Belfast, Northern Ireland
j.betts@qub.ac.uk

Abstract:

Protection of critical infrastructures has a growing role in national security issues. These include power and water supplies, traffic management systems, financial services and communication networks. Attacks on any of these can damage economies, cause disasters and may lead to loss of life. Dependence on critical infrastructures in modern societies makes them targets for organized crime and terrorism. Their protection is vital to national security and public safety. This paper highlights the importance of ethical principles in the design of critical infrastructure network protection systems, focusing on privacy and data protection. It introduces our research addressing privacy in the design of one such system funded by the European Commission's FP7 Programme. Debates surrounding national security and privacy involve policy makers, regulators, academics, security engineers and the public. A proposal from the designer of the Privacy by Design framework is discussed and the paper concludes by challenging policy makers, researchers and the technology industry to review and develop such proposals and enable the protection of national security and privacy.

I. INTRODUCTION

In 1949 George Orwell's novel "1984" depicted a fictional nation called Oceania ruled by a tyrannical government known as "Big Brother". This was a nation where privacy did not exist. Every action and word was recorded or filmed and used to identify and incriminate rebellious citizens. Fast forward to 2000 it was predicted that '…As the cost of storage continues to drop, enormous databases will be created, or disparate distributed databases linked, allowing data to be cross-referenced in increasingly sophisticated ways' [1]. This was not only seen to predict technical advances, but also would have political implications, '…Both collecting and collating personal information are ways of acquiring power, usually at the expense of the data subject.' (p1461) [1].

These visions of the future are now a reality since what have become known as *"the Snowden files"* were revealed by the Guardian newspaper in June 2013 [2]. They detail mass electronic surveillance and data mining programs carried out by the National Security Agency (NSA) in the U.S. and the Government Communications Headquarters (GCHQ) in the UK. Government surveillance is now a political issue and governments can no longer rely on a tacit acceptance that whatever they do relating to national security and surveillance is for the greater good and only impacts on criminals and terrorists.

Public knowledge and awareness has changed following the release of the Snowden files. Now politicians are accountable to their electorate concerning government activities once regarded as secret. Issues such as individual privacy and trust are to the fore in media and political debates, not only nationally, but extending to other democratic jurisdictions where the fundamental right to privacy is respected. In this work, we raise the ethical question of how governments can secure their national assets while respecting the rights of their citizens to individual privacy in their communications and

978-1-4799-4992-2/14/$31.00©2014IEEE

associations.

It may be the case that the debate cannot progress while privacy and national security are viewed as a dichotomy. Privacy by Design [3] is a framework for privacy enhancing technologies endorsed by European regulators [4]. Here we present an ethical challenge to politicians and the security industry. Where policy makers offer solutions [5], a corresponding commitment needs to be shown in the form of resources and implementation. For example, in European funded FP7 programmes [6], this is endorsed by a specification that privacy must be integral and demonstrated in methodology and design from inception to the implementation of security systems. We highlight one such project [7] and briefly outline how we intend to demonstrate and measure the impact of privacy protection. We believe such a challenge should be shared across policy makers and research disciplines to ensure systems enable privacy policies to be monitored and evaluated on an ongoing basis.

The paper is structured as follows: Section 2 shows how European legislation currently promotes national security over data protection. This does not, however, give providers of critical infrastructures permission to ignore data protection. European regulators are strengthening data protection throughout all Member States and the European Commission has given priority to issues of privacy and trust. Section 3 discusses what academics refer to as 'myths' that inform publicly held opinions on privacy and surveillance techniques; attitudes that the Snowden files have challenged. Section 4 describes a proposal [5] from the designer of the Privacy by Design framework [3] that could achieve data surveillance while safeguarding individual privacy. Finally, we raise an ethical question. If technical solutions are available, what reason would there be for failing to implement them?

This work has been partially supported by the project PRECYSE funded by the European Commission under the FP7 Framework Programme (www.precyse.eu)

II. EUROPEAN POLICY, NATIONAL SECURITY AND CRITICAL INFRASTRUCTURES

The rationale for data protection in Europe is about giving individuals more control over who has access to their data. The European Convention for the Protection of Human Rights (ECHR) [8] enshrines the right to privacy, but also includes specific instances when infringement of privacy by a public authority is permissible. Article 8(2) includes the exception *"...in a democratic society in the interests of national security"*. In line with current EU data protection, proposed EU General Data Protection Regulation on the *"processing of personal data wholly or partly by automated means"* [9] states in Article 2, 2(a): "*This Regulation does not apply to the processing of personal data: (a) in the course of an activity which falls outside the scope of Union law, in particular concerning national security."*

The legislation is clear that national security measures have precedence over data protection. Dependency on critical infrastructures in modern societies makes them a target for cyber warfare, organised crime and terrorism. Critical infrastructures include power and water supplies, traffic management systems, financial services and communication networks. Attacks on any of these can damage economies, cause natural disasters and lead to loss of life. Therefore their protection is vital to national security and public safety. Despite this, critical infrastructure providers are bound by data protection regulation in Europe as their administration networks store personally identifiable and financial information. Data protection for their service users and employees has a central role in designing security systems for critical infrastructure network protection.

A growing awareness of the vulnerability of industrial control systems means that their protection has become a global priority. An analysis of critical information infrastructure systems revealed how different priorities in critical infrastructure protection dictate different approaches. When

978-1-4799-4992-2/14/$31.00©2014IEEE

economic outcomes are the priority the main actors come from the private sector, with business continuity being the key consideration. In law and order, the main actors come from the law enforcement establishment to address issues ranging from technology enabled crime to crimes against individual computer users. Notably, where the issue is one of 'national security', the perception is that the whole of society and its core values are in danger due to their dependence on communication technology. In this case the main actors are from the security establishment with action taken at technical, legislative, organisational or international levels [10].

SCADA (supervisory control and data acquisition) industrial control systems are communication systems used in critical infrastructures including power, gas and water supplies and traffic control systems. Control system information is relayed to stations via the internet. The use of open networks makes them vulnerable to online criminal and terrorist targeted attacks. "PRECYSE" (Prevention, Protection and Reaction to Cyber Attacks to Critical Infrastructures) [7] is a European funded project to design an early warning intrusion detection system for SCADA industrial control systems. Pilot sites that will test and validate the PRECYSE system are a Traffic Control Centre and a company providing power and related services. The European Commission has stipulated that ethics in the form of privacy and trust must be a main focus for the system design to achieve successful delivery of the project.

"Operationalising" is a methodology used in social science research methodology. It involves translating abstract concepts, in this case privacy, into actions that can be measured and evaluated. In PRECYSE we evaluate the level of data protection by measuring the effectiveness of the system in protecting personal and company data. For example, in the deployment and testing of firewalls separating the SCADA and administration systems where personal data relating to service users and employees is stored. Data encryption and access restrictions provide additional technical solutions. Some areas require policies to be enforced by good management practices. For example, insider threat is a major issue that needs to be addressed through policies on staff training and awareness raising. Our privacy impact assessment tool is based on global standards and best practice to measure policy compliance. This will also serve to raise management awareness of privacy and trust issues. Our research methodology and outcomes will be presented in a future publication.

In parallel, at EU level, the NSA and GCHQ case has done a great deal to raise awareness of privacy and trust issues. Legal action by privacy lobbyists [11] has led to judges at the European Court of Human Rights (ECHR) demanding that UK Ministers provide submissions to them by the beginning of May 2014 justifying GCHQ surveillance in the light of the right to privacy under Art. 8 of the European Convention [8]. Within the UK public opinion is divided on whether surveillance by GCHQ is justified. Many believe reduced privacy is a fair exchange for their safety and that if they are doing nothing wrong they have nothing to fear from surveillance. This assertion has been debated in academia for some time, and is discussed in the next section.

III. CHALLENGING MYTHS

A. Public trust and public fear

Achieving a balance between individual privacy and national security is increasingly controversial and technically challenging; *"…the multiplication of databases and growth of new technologies raise new challenges to the protection of European's fundamental rights to personal data and privacy"* [12]. We would also argue that, prior to Snowden, the impact of data surveillance techniques were viewed as something affecting a minority of the population, and costs to privacy were regarded as reasonable when weighed against implications for public safety. Given the secrecy surrounding surveillance, it is not surprising that public opinion was neither particularly informed nor evident.

Referring to how society's beliefs are shaped in relation to critical infrastructure protection in particular, Burgess [13] conceptualises critical infrastructures and their protection in terms of 'social values'. In doing so, he shifts the emphasis

978-1-4799-4992-2/14/$31.00©2014IEEE

from the actual critical infrastructure to the effect its destruction has on the psyche of citizens, both in the areas affected and globally. His main argument is that a terrorist attack on a critical infrastructure has less to do with the disruption and even loss of life this may cause, but rather the loss of confidence of people in their critical infrastructures. The reality of future attack makes it easy to engender fear and uncertainty and the value for the terrorist is in the fear they create rather than the material value of the critical infrastructure [13].

Further explanations for the acceptance of surveillance techniques cite perceptions of risk that overestimate the risk of terrorism, while underestimating harms that might come from a reduction in privacy [14]. It is also argued that the way in which threats are presented to the public informs what security reactions are seen as acceptable [15]. For example, an internet virus corrupting thousands of computer systems, if viewed as a criminal attack prompts users to take measures to protect their individual online security. However, if the same attack is construed as an attack on the information network system of the nation it will be viewed as grounds for greater government surveillance. Different rationale leads to different technical design and, crucially, different levels of tolerance in a reduction of privacy protection. Motivated by how values influence the design and regulation of technologies, Nissenbaum argues for ethics and political values to be added to considerations and constraints in the design and regulation of systems [15].

B. The "nothing to hide" myth

The belief that "if I have done nothing wrong, I have nothing to hide" is common in public discourse [16] and confirmed by the UK's Foreign Secretary when he stated that law-abiding members of the public have "nothing to fear" [17]. Solove [18] dismisses this argument as a 'myth' that reduces privacy to one concept associated only with law and order and public protection. He argues that privacy is about more than concealment and secrecy. It involves the accumulation of information about an individual over time. It need not be connected with anything sinister, but may nevertheless involve embarrassment when matters the individual believed to be private are exposed. The aggregation of data is a concern for privacy advocates who claim it is impossible for people to manage their personal information due to the plethora of information that is collected by various entities [18].

The use of secondary data without the owner's consent illustrates an imbalance of power. Government surveillance involving data mining can introduce additional problems depending on the origins of the information. This includes information provided in different contexts for different purposes. The data subjects trust the information will only be used for particular and time-bound purposes. Precedent in the U.S. shows if information is collected from third parties, it invalidates individual privacy protection as there can be no 'reasonable expectation of privacy' in information that is freely given to others by the individual *(United States v. Katz, 389 U.S. 347, 360-61 (1967)).*

C. The metadata myth

A global survey conducted in January and February 2013, prior to Snowden's revelations, found that 62% of consumers reported being very, or somewhat concerned *"…the government or government agencies may obtain access to my personal data."* [19]. Government officials have defended the collection of 'metadata' claiming it does not contain personal communications or data that identifies individuals [16]. In June 2013 the media reported [20] that Verizon Communications was ordered to provide the NSA with all its customers' telephone metadata under section 702 of the U.S. FISA Amendments Act of 2008. This included local and international calls. The NSA, is also able to demand that major Internet companies, including Google, Apple and Yahoo hand over communications data that matches certain search terms. This includes the data of European citizens who use the services of these Internet service providers and involves a range of communications including emails, chat, video and social network posts. It also collects metadata identifying users of major internet companies.

978-1-4799-4992-2/14/$31.00©2014IEEE

Cavoukian describes metadata as *"...essentially information about other information, in this case, relating to our communications."* [21]. It reveals the time and length of a communication, the devices used, and the address or numbers contacted. Since every device has an address, they can be linked and traced to an individual. Government officials defended these activities by claiming that 'metadata' is not privacy invasive since it does not access the content of communications. However, privacy academics strongly contest this, arguing that metadata can actually reveal more information about an individual than their communications. Professor Daniel Weitzner, a researcher at MIT's Computer Science and Artificial Intelligence Laboratory is quoted as saying that metadata can be more revealing since it is easier to analyse patterns in vast amounts of data than to carry out analysis of individual emails [22].

President Obama has announced reforms stemming from a report from the surveillance review panel established in August 2013 [23]. In a White House Briefing on 17 January 2014, he announced changes to the system for collecting metadata on all US phone calls under Section 215 of the Patriot Act. This will be amended later in the year to reflect the recommendation that rather than government holding the repository of data it will either be left to the phone companies or handed to a third party for storage. In addition, and starting immediately, analysts will no longer be able to search phone records without a court order. President Obama also said that the standards for conducting state surveillance needed to be higher and that it was not enough for leaders to ask the public to trust them that they would not abuse the data they collect. This is an issue of public trust.

Proposals for third parties to store information rather than government is part of Cavoukian's Privacy-Protective Surveillance [5] outlined in section 5 of this paper. We would have some concerns regarding third parties retaining and storing data for several reasons. Firstly, the third party, rather than government would be responsible for the security of the data. Is it to be stored in the cloud with any attendant security risks? What data protection issues might arise if there are different legal jurisdictions involved? If data is stored in disparate locations, security issues will emerge that will need to be addressed during the development and design stage.

D. Prism has given privacy centre stage in debates about national security. Public awareness is raised, and ethical questions require responses. Are governments prepared to review and resource the necessary research and development stages for proposals that may provide opportunities to allow people to feel protected from attack, but not to have to fear indiscriminate mining of their personal communications? Privacy-Protective Surveillance is outlined below. The authors acknowledge the need for further technical research and development and therein present an ethical challenge to industry.

IV. Privacy-Protective Surveillance: A Viable Solution?

Privacy by Design [3] is well documented and was recognised in October 2010 as the global standard at the International Conference of Data Protection and Privacy Commissioners. Its developer has co-authored a paper outlining Privacy-Protective Surveillance (PPS) [5], a privacy protective alternative to current counter-terrorist surveillance. Based on the Privacy by Design framework, it utilises current technology tools combining cryptography with machine learning techniques.

PPS [5] has three main technological components. Firstly, 'intelligent virtual agents' search online and transactional databases for suspicious activities. If suspicious activity is detected, any associated personal information associated with it would be encrypted and flagged up for further investigation. Secondly, a system using "Secure Multi-Party Computation methods" would interrogate the encrypted data searching for links between activities and individuals. "Homomorphic encryption" is the suggested encryption method. This would be valuable in allowing data to be analysed while still encrypted, although it is an area requiring technical expertise to decide on its practicality for this purpose. Finally,

978-1-4799-4992-2/14/$31.00©2014IEEE

"probabilistic graphical models", Cavoukian gives the example of Bayesian networks, would perform inferential analysis on the anonymised data to calculate the likelihood of a terrorist threat from the previous analysis of suspicious linked activities. It is only at this point that a warrant would be sought to decrypt any personally identifiable information.

The reputation of internet companies such as Google and Facebook have been damaged by the release of the Snowden files. Public trust has been further eroded following media reports that they accepted sums of money from the NSA for their co-operation [24]. Cavoukian believes PPS could improve public perception if, ultimately, internet companies were able to use the methodology to carry out anti-terrorist surveillance on their users' data without having to hand it over to the government. PPS avoids the mining of vast sums of data looking for previously unknown patterns of behaviour. While this can be useful for marketing and profiling for targeted advertising, it produces too many false positives for mass surveillance. The specifically targeted nature of the PPS data analysis technique could therefore help to restore public trust.

The proposed methodology attempts to address the ethical area of privacy and trust. Well designed and developed "probabilistic graphical models" could achieve targeted data analysis that would minimise the risk of false positive results and the data of innocent internet users being exposed. Analysis has only been conducted on encrypted data up to the point where there is sufficient suspicion for a warrant to be requested. At the stage where a warrant is issued and data unencrypted, further privacy safeguards could restrict access to the data. The model enables a minimisation of human contact with personally identifiable information that could be further developed.

V. CONCLUSION

The release of the Snowden files have moved ethical concerns in relation to privacy and trust to a new political level. The ethical concerns of society today shape the policies and legislation of tomorrow, although the events of 2013 have produced a political urgency not generally associated with the slow progress of policy and legislation normally the subject of prolonged consultation and debate. Privacy concerns related to mass data surveillance cannot be fully addressed by politicians and governments. Nor, we believe, should they be. Our paper presents an ethical challenge to researchers and the technology industry. We highlight how a privacy impact assessment tool can be used in critical infrastructure protection to measure the effectiveness of technical security solutions. We also identify the PPS solution with which it is possible to develop policies and technologies that can prevent mass data surveillance violating the privacy a majority of law-abiding citizens have a right to expect. The availability of these solutions challenges policy makers, researchers, engineers and industry to progress their implementation with the objective of promoting and protecting both national security and privacy. If there is not a willingness to do this, we have to ask ourselves why?

A. REFERENCES

[1] Froomkin Michael A. (2000) The Death of Privacy; Stanford Law Review, Vol. 52, No:5 Symposium: Cyberspace and Privacy: A New Legal Paradigm? (May 2000), pp. 1461-1543.

[2] The Guardian World News "Edward Snowden and the NSA files – timeline" [Online]. Available: http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline

[3] Privacy by Design [Online]. Available: http://www.privacybydesign.ca/

[4] COM/2007/228 on Promoting Data Protection by Privacy Enhancing Technologies (PETs); Brussels. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0228en01.pdf

[5] Cavoukian A. and El Emam K. (September 2013) Introducing Privacy-Protective Surveillance: Achieving

Privacy *and* Effective Counter-Terrorism; Information and Privacy Commissioner, Ontario, Canada.
[6] European Commission Research and Innovation 7th Framework Programme for Research and Technological Development [Online]. Available: http://cordis.europa.eu/home_en.html
[7] Precyse [Online]. Available: https://ssl6.ovh.net/~precyse/
[8] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols 11 and 14, 4 November 1950, ETS 5, Art. 8.
[9] COM(2012)11 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [Online]. Available: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
[10] Myriam Dunn, 'The socio-political dimensions of critical information infrastructure protection (CIIP)'; *Int. J. Critical Infrastructures, Vol. 1, Nos. 2/3, 2005 (pp. 258-268).*
[11] European Court of Human Rights, App. No. 58170/13 Joint Application under Article 34.
[12] CIPHER Integrated cyber-security frameworks for privately held information systems and European Roadmap", D1.2 Diagnosis of legal, ethical and political situation.
[13] J. Peter Burgess (2007) Social values and material threat: the European Programme for Critical Infrastructure Protection in Int. J. Critical Infrastructures, Vol. 3, Nos. 3/4, 2007.
[14] Jennifer A. Chandler, "Personal Privacy versus National Security: Clarifying and Reframing the Trade-off" in Kerr, Lucock and Steeves, eds. *On the Identity Trail: Anonymity, Privacy and Identity in a Networked Society,* Oxford University Press, 2009) pp. 121-138.
[15] H. Nissenbaum, "Where Computer Security Meets National Security", *Ethics and Information Technology,* Vol. 7, No. 2, June 2005, 61-73.
[16] BBC 7 June 2013 US spy-chief Clapper defends Prism and phone surveillance, Comments [Online]. Available: http://www.bbc.co.uk/news/world-us-canada-22809541
[17] Guardian 24 January 2014 "Justify GCHQ mass surveillance, European court tells ministers" [Online]. Available: http://www.theguardian.com/uk-news/2014/jan/24/justify-gchq-mass-surveillance-european-court-human-rights
[18] Solove, Daniel J., 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. San Diego Law Review, Vol. 44, p. 745, 2007.
[19] Privacy Uncovered Can Private Life Exist in the Digital Age? (2013) A report from The Economist Intelligence Unit; Beazley [Online]. Available: https://www.beazley.com/privacy_uncovered.html
[20] Glenn Greenwald, Thursday 6 June 2013 Guardian World News, 'NSA collecting phone records of millions of Verizon customers daily' [Online]. Available: http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order
[21] Cavoukian, A. (July 2013) A Primer on Metadata: Separating Fact from Fiction; Information and Privacy Commissioner's Office, Ontario, Canada.
[22] E. Nakashima, "Metadata reveals the secrets of social position, company hierarchy, terrorist cells". The Washington post, June 15, 2013 [Online]. Available: http://www.washingtonpost.com/world/national-security/metadata-reveals-the-secrets-of-social-position-company-hierarchy-terrorist-cells/2013/06/15/5058647c-d5c1-11e2-a73e-826d299ff459_story.html
[23] Liberty and Security in a Changing World (12 December 2013) Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies [Online]. Available: http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf
[24] Ewen MacGaskill, New York, NSA paid millions to cover Prism compliance costs for tech companies, Friday 23 August 2013. [Online]. Available: http://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid

978-1-4799-4992-2/14/$31.00©2014IEEE