This project has received funding from the European Union's Seventh Framework Programme for research; technological development and demonstration under grant agreement n: 607480

LARGE SCALE INFORMATION EXPLOITATION OF FORENSIC DATA

The Contested Semantics of 'Security' and the Curious Case of Privacy Impact Assessments applied to National Security Initiatives

LASIE Project

FP7 - SEC-2013.1.6-1 - Framework and tools for (semi-) automated exploitation of massive amounts of digital data for forensic purposes – Integration Project

Grant Agreement n°: 607480

Start date of project: 1 May 2014

Duration: 42 months

Document. ref.:

Peace Research Institute Oslo (PRIO)

Oslo, 29 August 2016

The Contested Semantics of 'Security' and the Curious Case of Privacy Impact Assessments applied to National Security Initiatives

A breakfast seminar by Roger Clarke[1]

A public report thereof by Stine Bergersen (PRIO)[2]

A breakfast seminar by Professor Roger Clarke, with the title "The Contested Semantics of 'Security' and the Curious Case of PIA's applied to National Security Initiatives", took place on 29 August 2016 at PRIO premises in Oslo, Norway. The seminar was arranged within the framework of the LASIE project,[3] or 'LArge Scale Information Exploitation of Forensic Data' (2014-2017). LASIE is a research project co-funded by the European Union (EU) under the 7th Framework Programme for Research and Development (FP7), which aims to 'design and implement an open and expandable framework that will significantly increase the efficiency of current investigation practices, by providing an automated initial analysis of the vast amounts of heterogeneous forensic data that analysts have to cope with'.

The present report offers a succinct account of the presentation by Clarke, as well as some views, questions and comments expressed in the open session following the presentation. This short report, as well as being a summary of the event also of interest to the LASIE consortium partners not present, also holds the potential to stimulate further debates on the wider impacts of technology on the society, e.g. linked to both the practical and theoretical implementation of the LASIE-framework. The PowerPoint-presentation by Clarke is attached to this report.

The views expressed in the following are solely those of the speakers, and does not reflect the views of the LASIE consortium as a whole, its individual partners nor the European Commission.

Introduction

Dariusz Kloza, the LASIE project leader from PRIO and the chair of the session, opened the seminar by welcoming the participants, and by giving a brief introduction to PRIO, and the kind of research

1 Xamax Consultancy Pty Ltd, Canberra; Visiting Professor in Computer Science, Australian National University (ANU), Canberra; Visiting Professor in Cyberspace Law & Policy, University of New South Wales (UNSW), Sydney.

2 E-mail: stiber@prio.org.

3 Cf. www.lasie-project.eu.

conducted at the institute. In short, PRIO conducts research on the various conditions for peaceful relations between states, groups and people. As a backdrop for the theme of the seminar, within the department Dimensions of Security, where the research team[4] in LASIE is situated, the focus is on critical security studies, where several concepts of "security" are at play. "Security" is understood and explored at PRIO both as national security e.g. at borders, within cities, as societal and urban security, etc. That is to say that no predominant perspective on the concept is established. In general, and for a long time, the larger topics of semantics applied to security, and data protection and privacy, are considered interdisciplinary relevant. While there is no doubt that surveillance, privacy and data protection continue to be important topics for discussion in many and various disciplines, having this seminar was highlighted as especially relevant because of the current debates concerning the introduction of the EU General Data Protection Reform (GDPR); and the role that Data Protection Impact Assessments (DPIAs) play in the reform.

Kloza introduced the speaker, Professor Roger Clarke. Clarke was described as one of the fathers of (the modern understanding of) privacy and surveillance, the author of the concept of 'dataveillance' and a co-inventor and successful practitioner of Privacy Impact Assessments (PIAs) for more than 20 years. He is also a frequent commentator on these matters and a prolific author. Then the intervenants were introduced. Lee A. Bygrave is a Professor at the Norwegian Research Centre for Computers and Law at the University of Oslo, and has published particularly extensively within the field of privacy/data protection law. Finally, Rocco Bellanova, senior researcher at PRIO and a member of the PRIO's LASIE team was introduced as the second commentator.

Presentation by Professor Roger Clarke

The seminar was advertised internally at PRIO, on the public websites of PRIO, as well as internally within the LASIE consortium with the following description:

> *Conversations about security generally involve people talking at cross-purposes. The reason for this is that the meaning of the term 'security' is relative to the particular values that particular stakeholders perceive in particular assets, and the particular harm that those values might come to. Yet people seldom take the trouble to clarify which stakeholders, assets, values and harm they are talking about, even to themselves, let alone to other people. National security initiatives inherently involve clashes among alternative scope definitions. At the very heart of the matter is the conflict involved in constraining human rights in order to protect them. Appropriate decision-making about national security initiatives is therefore entirely dependent on the application of an effective evaluation process. Results are presented of a survey of Privacy Impact Assessments (PIAs) undertaken in respect of Australian Government national security initiatives. Despite the enormous intrusiveness of these initiatives into the rights of everyone in Australia, and the (to date) rare incidence of their use, the evaluation processes are shown to have been uniformly and seriously inadequate. Both the legislature and the executive have failed their obligations to Australian society. They continue to blindly accept a narrow and heavily biased conception of security, and fail to impose either pre or post controls on the club of national security agencies.*

4 Dariusz Kloza, Rocco Bellanova, Stine Bergersen and Ida Rødningen.

The presentation was structured roughly in two parts: the first part explored the semantics of security (underlining the importance of asking whether we understand the concepts in the same way), and the second part discussed a case study of a survey of Privacy Impact Assessments (PIAs) undertaken in respect of Australian Government national security initiatives. As the link between the two might not be obvious for everyone, Clarke highlighted indeed their existence.

The Semantics of Security

Clarke began the presentation by showing the audience with a selection of photographs, basically picturing mountain climbing and hiking in different scenic, but also rather extreme, contexts, with the aim to illustrate both how we feel different in these "dangerous" contexts, but also, how the carefully crafted steps, rails, signs etc. might work as an indicator that we maybe *should* be afraid, since they remind us that someone else has assessed this to be dangerous enough for these measures to be set up – but also that we are not, because we can see that warnings and protections have been provided. Against this backdrop, the notion of security was introduced as "a condition in which harm does not arise despite the occurrence of threatening events", and further, "a set of safeguards whose purpose is to achieve that condition".[5] Clarke underlines that there is indeed no one, reliable dictionary definition, but rather that the notion of security is broad, and in simple language has to do with *no harm*, *despite things*. In any case, we have to always regard security in a context.

Furthermore, Clarke presents what can be described as the conventional security model, which describes a generic threat, giving rise to a threatening event, which in turn impinges on or exploits vulnerability. Acknowledging this vulnerability, and faced with a threatening event, this can result in a security incident, which leads to harm to an asset. But there are several layers and expansions to this model. Expanding the conventional security model with the notion of *safeguards* means that a measure is introduced to counter a threat, and by introducing *countermeasures*, actions are taken to circumvent a safeguard. An introduction of safeguards implies an obvious interest in harms and assets, and would traditionally have impact in the sense of budgets and financial implications. The logic is then that *harm* means a deleterious impact on an *asset*. But, importantly, it is not a given which harm matters, and to which assets. This depends on the perspective that is adopted, and the values that are perceived in assets.

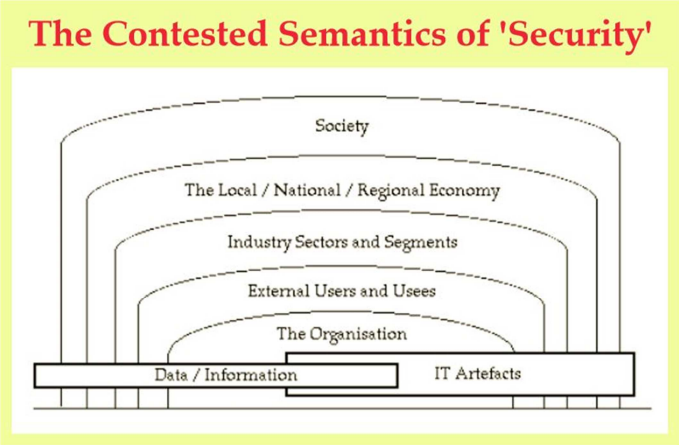
As a consequence, Clarke describes how it becomes necessary to define who the stakeholders are in the equation, and to ask: "whose security are we talking about?" Which tensions emerge, depends on the point of view of the different stakeholders, and which specific events and threats motivate which people. To discuss security via the overlaps and correlations between data/ information and IT artefacts, is one way, but does not provide a complete picture, and a wide range of different stakeholders should also be included in the discussion. By shifting the scope from a single organisation up to industry sectors and segments, different stakeholders emerge, and the picture immediately becomes more complex. Furthermore, by including the layers of local, national and regional economy (which would include e.g. competition among nations), the abstraction level increases further. Depending on the scope and focus, what is defined as "critical infrastructure" by e.g. governments, will also vary, to include various elements from industry sectors, such as transport,

[5] Cf. Attached PowerPoint presentation given by Clarke.

communications, energy and water. At the centre of such security discussions, are often *data* (abstract, empirical and synthetic) and *information* (defined as data applied in a context for a use). The question then becomes: *whose assets, which stakeholders and whose security?*

Clarke furthermore describes a "mostly forgotten scope for security" which highlights how some stakeholders, particularly external "users" and "usees", are often left out of the discussions. The concept of a usee can be explained in terms of the example of credit databases, where the stakeholder is not directly involved, but nonetheless affected.

As a result of the complexity of the different layers in the scope(s) of security, *tensions* arise. These tensions can arise among organisational objectives such as financial cost versus non-quantifiable costs, or among alternative scope definitions, exemplified by a case where a bot does not harm the host, and hence it can be seen as an externality for which no incentive exists to come up with a fix. The topmost layer of the model for the scope of security by Clarke, is the societal level. The full figure can be seen below, but Clarke also explained how the scope can be widened even further, by including also considerations such as the notion of humanity, of the biosphere, of the troposphere. It becomes a question of political economy, which should be looked at by measures of political science, e.g. questions of who are fighting for the different perspectives, what potential coalitions there are, and which of them have power.



Figur 1 Abstract from the PowerPoint presentation by Clarke, Slide 16

The question then arises: where and how can we place national security in this figure? Moving beyond the old-fashioned definitions encompassing mostly state protection from an attack, national security is maybe rather useful looking at via the concrete contexts in which it emerges. Some examples can be contexts of critical infrastructure security, public safety or prominent person safety. However, the use of the word is difficult, since labelling can have various implications, e.g. when mixed up with terrorism. A brief introduction is given of terrorism and national security (underlined as two very different things) in the Australian context, demonstrating how only very few incidents have occurred in the last decades. Even periodic big-scale raids have led to successful prosecutions of only 15 individuals, only 6 of them being instances of preparation to commit an act. The lack of constitutional protection for human rights is presented as a maybe unique factor in the Australian

context, and Clarke describes how various national security measures since 2001 have compromised many human rights, such as the freedom of movement.

PIA´s applied to National Security Initiatives

For the second part of the presentation, results are presented of a survey of Privacy Impact Assessments (PIAs) undertaken in respect of Australian Government national security initiatives. This part was based on a recent article, [6] where Clarke describes in more detail how democracy in Australia is gravely threatened by a flood of measures harmful to human rights that have been introduced since 2001, a large proportion of which are unjustified and not subject to effective controls. The passage of these measures through the Parliament has been achieved on the basis of their proponents' assertions and without appropriate scrutiny. Clarke describes how the parliament had several forms of impact assessment techniques available, but shows that they failed to require that such methods be applied. The focus is particularly on one specific form of evaluation – Privacy Impact Assessment (PIA). The study by Clarke found that the PIA process should have been performed for each proposal, but was in fact seldom applied, and where it was applied, the process and report were in almost all cases seriously deficient.

In sum, despite the enormous intrusiveness of these initiatives into the rights of everyone in Australia, and the (to date) rare incidence of their use, Clarke describes how the evaluation processes are shown to have been uniformly and seriously inadequate. The result being that both the legislature and the executive have failed their obligations to Australian society. They continue to blindly accept a narrow and heavily biased conception of security, and fail to impose either pre- or post-controls on the club of national security agencies. Ministers and Parliamentary Committees must demand prior evaluation of proposals that restrict civil freedoms, must ensure transparency in relation to the proposals and their justification, and must require effective controls over, and mitigation features within, those measures that survive the evaluation process. The overall goal with applying systematic PIA's to these processes is not only to document, but also to avoid implementing schemes that are unjustified, and, for those that are justified, to ensure that the design incorporates controls and mitigation measures. A description of the different elements in a PIA process is given, and Clarke gives examples of some of the benefits of doing a PIA (such as providing the organization with a vision of what it is you actually intend to achieve, and how), as well as some reasons for organizations not to do a PIA (such as costs and delays). The presentation of different case studies on Australian national security initiatives and PIAs concluded that PIAs do not operate as a control mechanism.

Interventions from discussants

After the presentation by Clarke, two invited discussants shared their comments and questions.

6 Roger Clarke, Privacy impact assessments as a control mechanism for Australian counter-terrorism initiatives, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.01.009

Lee Bygrave opened by complimenting the presentation for being informative, and for taking on a broad scope. Bygrave underlined that his intervention should not be seen as normative statements, but questions. He raised the issue of whether the concept of national security keeps being contested on purpose, by many players, since this gives them room for manoeuvring within their respective fields. In EU law, national security is a crucial concept, and a big part of regulations and constitutions. The concept, and the semantics of security, might be intentionally kept wide and flexible, as well as contested (and confused). Bygrave also asks the question of whether it is useful to distinguish between security and safety, and whether safety is seen as a subset of security. And further, if it is useful to distinguish between military and civil sector. The further discussion also touched upon how we can (acknowledging the findings from the Australian context) do PIAs as more than symbolic, e.g. by introducing legal mandates to back the PIAs up, as well as "evolution meta principles", the principle of proportionality and EU courts case law.

The intervention by Rocco Bellanova suggested that privacy often comes into play as an afterthought, something that comes after the introduction of a security measure, and which is to a large extent left to the individuals dealing with the law. National security is mentioned as rather a style of governing, with "external" being the key word, and it is a governing that facilitates the state to secure the state again. It also helps policy makers on what to do, and Bellanova also mentioned concepts such as the panopticon and biopolitics as traditional elements in a discussion of how a healthy population can be created and managed by the state. Furthermore, as many security measures are defined via the definition of a state of exception, society is in a sense defined via a long line of security measures.

It is also a question of rhetoric. Bellanova describes how after the Snowden-revelations, "everyone" discovered surveillance, which is now at the heart of security discussions. In terms of managing populations, Facebook is one good example of how this kind of surveillance becomes possible. Another one being PNR (Passenger Name Records), which are introduced to facilitate air travelling, but at the same time allows for the surveilling of the travellers. A question from Bellanova is how you can make the difference between security and these forms of more hybrid security (Facebook etc.)? Bellanova also asks the question of how PIAs can come into play when we are in a situation where basically everything is or can become a security tool, and how we can engage with the use/usees.

Following these two interventions was a session where Clarke responded to some of the comments and questions, and some questions from the audience were given. A very brief summary of this makes up the final section of this report.

Some of the issues commented on were a confirmation that there is indeed a confusion in terms between security and safety, and that Clarke includes safety in security, but also that there is a challenging ambiguity. He mentions, in the military context, that in some countries this line does not exist, but that in a western European state, we can usually talk about this kind of line. The increased use of drones was highlighted as an area where this ambiguity is currently making its presence felt. With regards to questions on PIAs, Clarke suggests to "get beyond window dressing", and that the onus should be put on organizations to do PIAs.

From the general audience, questions and comments were raised that highlighted the usefulness of the presentation by Clarke, the fundamental importance of semantics and of acknowledging the power of definitions. One question had to do with the difference between synthetic and empirical data, and another whether we can talk about different levels from "normal" to "state of emergency", or if this is a gradual shift. Another question had to do with how we can keep PIAs relevant in a time where you do not have personal data (i.e. Big Data), and what the distinctions and overlaps between PIAs and

Societal Impact Assessments (SIAs) are. For the latter, Clarke responded that SIAs have privacy as part of them, and that it depends on the country and context, and which assets and values you are looking to protect.

The concept of Data Protection Impact Assessments were also raised (in relevance to the current EU General Data Protection Regulation), but the conclusion among the participants pointed in the direction of DPIAs being too narrow, since it runs the risk of locking the discussion analytically to what the law defines in a certain context. For example, we know that the mere presence of CCTV can impact your behavioural privacy even though it does not record your data. The issue of PIAs versus risk assessments were also raised. Clarke describes how one tries to build PIAs into risk assessments guidelines and procedures, but that its success is dependent on organizations internalizing this. One solution can be to link PIAs into the already existing risk assessments that exist in the organizations.

Due to the interest in the discussion, the seminar went a little bit over the scheduled time, but was finally rounded off by Kloza, thanking everyone for their interest and participation.

The Contested Semantics of 'Security' and the Curious Case of PIAs applied to National Security Initiatives

Roger Clarke
Xamax Consultancy Pty Ltd, Canberra
Visiting Professor in Computer Science, ANU, Canberra
Visiting Professor in Cyberspace Law & Policy, UNSW, Sydney
http://www.rogerclarke.com/DV/PIANS {.html, .pdf}

Peace Research Institute Oslo (PRIO)
29 August 2016

The Notion of Security

A condition
in which harm does not arise
despite the occurrence of threatening events

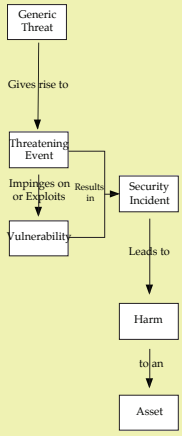
A set of safeguards
whose purpose is
to achieve that condition

The Conventional Security Model Key Concepts

- A **Threat** is a circumstance that could result in Harm
  A **Threatening Event** is an instance of a generic Threat
  A Threat may be natural, accidental or intentional
  An intentional Threatening Event is an **Attack**
  A party that creates an Intentional Threat is an **Attacker**
- A **Vulnerability** is a susceptibility to a Threat
- **Harm** is any kind of deleterious consequence to an **Asset**

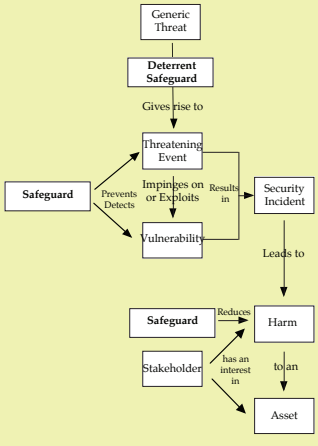
- A **Safeguard** is a measure to counter a Threat
- A **Countermeasure** is an action to circumvent a Safeguard

The Conventional Security Model



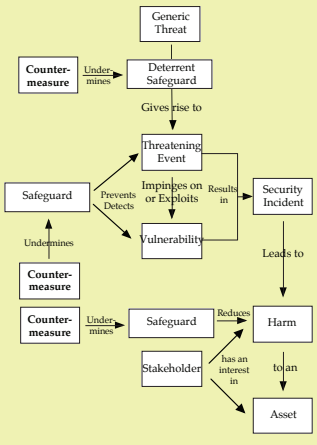
http://www.rogerclarke.com/EC/PBAR.html#App1

The Conventional Security Model + Safeguards



http://www.rogerclarke.com/EC/PBAR.html#App1

The Conventional Security Model + Countermeasures



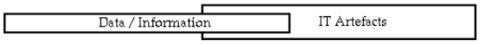
http://www.rogerclarke.com/EC/PBAR.html#App1

Asset, Harm, Value, Stakeholder

- **Harm** means deleterious impact on an **Asset**
- But which Harm matters, to which Assets?
- That depend on the perspective that's adopted and the **Values** that are perceived in Assets
- So it's necessary to define **Stakeholders**

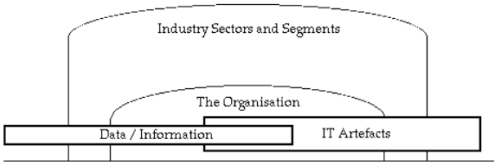
'Whose Security?'

The Scope of Security



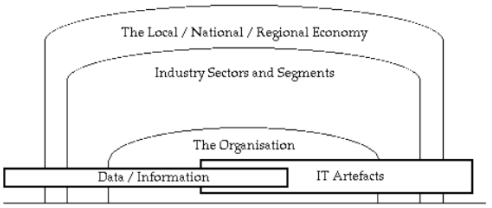
The Organisational Scope of Security

A Broader Scope for Security



Competition between Corporations
Collaboration, esp. re IT Infrastructure

A Yet Broader Scope for Security

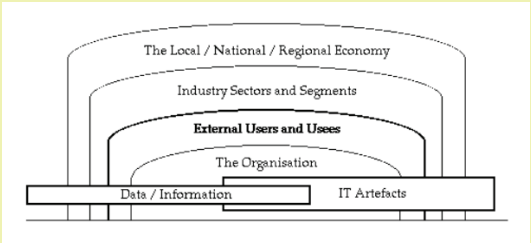


IT Infrastructure for Economic Development
Competition among Nations
'Critical IT Infrastructure'

Industry Sectors Designated by Governments as 'Critical Infrastructure'

- **Military-Industrial incl. Cryptography**
- **Transport**
- **Communications**
- **Energy**
- **Water**
- Public Health
- Emergency Services
- Law Enforcement
- Agriculture
- Financial Services

A Mostly-Forgotten Scope for Security



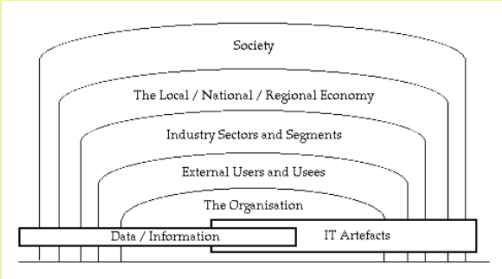
Tensions

- **Among Organisational Objectives**
  - Certain Costs vs. Contingent Costs
  - Financial Cost vs. Non-Quantifiables
  - Business-As-Usual vs. Invisibles

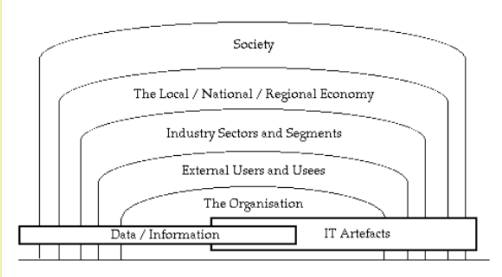
Tensions

- **Among Organisational Objectives**
  - Certain Costs vs. Contingent Costs
  - Financial Cost vs. Non-Quantifiables
  - Business-as-usual vs. Invisibles
- **Among Alternative Scope Definitions**
  - A bot doesn't harm the host, so there's no incentive to fix it (it's an 'externality')
  - Copyright material on P2P networks
  - Personal, Organisational, Sectoral, National, Supra-National Agency Interests

The Contested Semantics of 'Security'

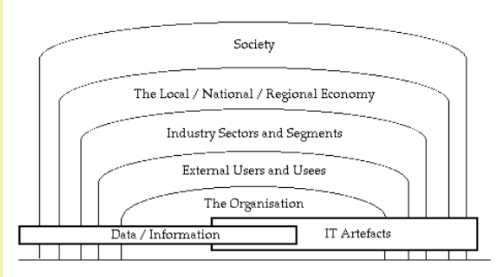


The Contested Semantics of 'Security'



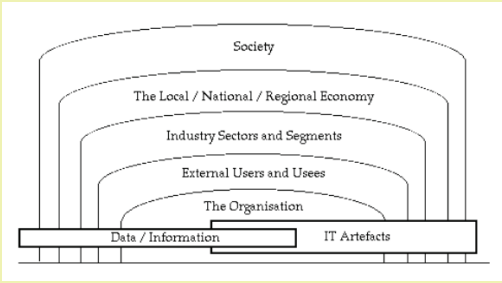
What about Humanity?
What about the Biosphere, the Troposphere?

Who are the Champions for Each Perspective?



Which have Power?
What Coalitions are feasible?

And where is 'National Security'?



Is this 'National Security'?

The protection of a nation from attack or other danger by holding adequate armed forces and guarding state secrets

Encompasses economic security, monetary security, energy security, environmental security, military security, political security and security of energy and natural resources

http://definitions.uslegal.com/n/national-security/

"specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy"

US Freedom of Information Act

Or is this 'National Security'?

- **Critical Infrastructure Security**
  Bombs in ports, ships, railways, energy, ...
  Anthrax in the water supply, ...
- **Public Safety**
  Bombs in aircraft, mayhem in marketplaces
  Major Events, e.g. 'The Euros', The Olympics
- **Prominent Person Safety**
  Bush and Blair; Rushdie and Kurt Westergaard
  Gx, APEC, CHOGM, ...

'Terrorism' conflated with 'National Security'

The use of violence or the threat of violence,
especially against civilians,
in order to alarm the public,
in the pursuit of political [or politico-religious] goals

'Terrorism' and National Security
The Australian Context

- Each decade pre 2000 saw some such event(s)
- 2002 – 88 Australian deaths in Bali,
  at a nightclub frequented by Australians
- **2015 – 1 domestic murder by a 15yo 'lone wolf'**
  That's the sole death in Australia since 2001
- Several credible claims of interdiction 2001-15
- But periodic large-scale raids have led to successful prosecutions of only 15 individuals re 6 instances of preparation to commit an act

https://www.crikey.com.au/2014/09/04/the-real-threat-of-terrorism-to-australians-by-the-numbers/
http://www.abc.net.au/news/2015-02-25/fact-file3b-five-facts-about-terrorism-in-australia/6226086

A (Maybe Uniquely?) Australian Factor
No Constitutional Protection for Human Rights

- Explicit decision at the end of the 19th century to not entrench human rights in the Constitution
  There are only 6 constitutional rights: trial by jury, just compensation, discrimination in one state against a resident of another state, freedom of religion, implied (and qualified) freedom of political communication, implied right to vote
- Australia acceded to ICCPR in 1980
- Successive Governments and Parliaments have refused to comply with ICCPR obligations
- There are no legislative provisions that can provide a basis for action for breach of the ICCPR

National Security Measures Since 2001 Have Compromised Many Human Rights

- Freedom from Arbitrary Detention (ICCPR Art. 9)
- Freedom of Movement (Art. 12) ======>>
- Right to a Fair Trial (Art. 14.1), Minimum Guarantees in Criminal Proceedings (Art.14.2-14-7)
- Privacy (Art.17)
- Freedom of Information, Opinion, Expression (Art. 19)
- Freedom of Association (Art. 22)
- Other Rights Potentially at Risk (Arts. 2.1, 7, 15, 21, 24, 26, 27)

http://www.rogerclarke.com/DV/IANS.html#App4
Extracted from AHRC (2008), Williams (2011), HRLC (2011, 2012) LCA (2012), Lynch et al. (2014)

e.g. Freedom of Movement (Art. 12)

- **Preventative Detention Orders for 48 hours, extensible**
  Renewable, self-issued not judicial, not subject to challenge or appeal, the person is held in secret, possible prohibition on contact with a lawyer, possible suppression of all facts re hearing – Criminal Code Division 105
- **Control Orders**
  Without conviction, or even charges, for criminal behaviour, based on mere civil standard of proof, secret evidence may be used, lack of transparency, due process and review, person's identity may be secret – Criminal Code Div 104, created in 2005
- **Powers to suspend, cancel and seize passports**
  – Australian Passports Act 2005 plus amendments 2014
- **(Some) Mercenary Behaviour Criminalised**
  Being in a 'declared area', reversed onus of proof, few reasons permitted – CTLA (Foreign Fighters) Act 2014

Whose Security? A Case Study
PIAs and National Security in Australia

Privacy Impact Assessment

- a systematic process, which ...
- identifies and evaluates ...
- from the perspectives of all stakeholders ...
- the potential effects on privacy of ...
- a project, initiative or proposed system or scheme
- and which includes a search for ways to avoid or mitigate negative privacy impacts

http://www.rogerclarke.com/DV/PIAsAust-11.html (2011)

Elements of the PIA Process

- **Surfacing and Examination** of the privacy impacts and implications of a proposal
- Development of a clear understanding of the Business Need that **justifies the proposal and its negative impacts**
- **Gauging of the Acceptability** of the proposal and its features by organisations and people that will be affected by it
- **[Assessment of Compliance** of the proposal with existing privacy-related laws, codes, best practices and guidelines]
- Constructive Search for, and Evaluation of, better **Alternatives**
- Constructive Search for ways to **Avoid** Negative Impacts, **and** ways to **Mitigate** Unavoidable Negative Impacts
- Documentation and Publication of the **Outcomes**

Clarke R. (2009) 'Privacy Impact Assessment: Its Origins and Development' Computer Law & Security Review 25, 2 (April 2009) 123-135
http://www.rogerclarke.com/DV/PIAHist-08.html

Australian Govt Policy re PIAs

- Data-Matching 'Program Protocol' since 1990, 1992
- PIA Guidance – versions of 2006, 2010, 2014
  "I strongly encourage government agencies to use the guide to assist them in playing a larger role in promoting privacy compliance" (Attorney-General, August 2006)
- Early signs of agency take-up c. 2008
- "It is expected that agencies will continue to voluntarily conduct privacy impact assessments as appropriate when developing policies which will impact on privacy" (Second Reading Speech Sep 2012)
- PC'er power to direct an agency to conduct a PIA since March 2014 – but yet to be exercised

http://www.rogerclarke.com/DV/PIAsAust-11.html
http://www.rogerclarke.com/DV/IANS.html#BGP

Efficacy of a PIA: A Five-Factor Test

1. Is there evidence of a PIA process being **performed**?
2. Were advocacy organisations **aware** of that process?
3. Did the project sponsor(s) **engage** with advocacy organisations?
4. Was the PIA **Report published** on completion?
5. Were advocacy organisations' views appropriately **reflected** in the PIA Report?

   However, it was known that there was a low incidence of published Reports. Hence:
6. Did the PIA **Report come to light** later, e.g. as a result of an FoI request by the media?

Results of the Five-Factor Test

AGD

- Passed the 5-factor test 2/36
- Engagement with advocacy organisations 3/36 (but their views were ignored)
- Secret (hence flawed) PIA processes 10/36

Other Agencies

- Passed the 5-factor test 1/36
- Engagement with advocacy organisations 5/36

Case Studies

1. Document Verification System (DVS) 2004-15
2. ANPR Mass Surveillance 2007-
3. Telecommunications Act s.313 2013-15
4. (Meta-)Data Retention 2003-15

Case Study 4 – (Meta-)Data Retention

- 2003-11 – AGD made multiple unsuccessful attempts
- 2012-13 – AGD enlisted Parltry 'friends of natsec' Ctee Ran a project, with no PIA or consultation
- 2014-15 – the Bill:
  - referred to the 'friends of natsec' Ctee
  - 30 public interest advocacy submissions: Incoherent proposal, Highly unlikely to even work let alone achieve its aims, Hugely privacy-invasive, Euro schemes have been disallowed, and failed anyway
  - No real changes, supported by Opposition
- 2015-16 – Requirements still incoherent, Implementation appears to be stalled

Reasons to do a PIA

- **Surfacing and Examination** of the privacy impacts and implications of a proposal
- **Development of a clear understanding of the Business Need that justifies the proposal and its negative impacts**
- **Gauging of the Acceptability** of the proposal and its features by organisations and people that will be affected by it
- **[Assessment of Compliance** of the proposal with existing privacy-related laws, codes, best practices and guidelines]
- Constructive Search for, and Evaluation of, better **Alternatives**
- **Constructive Search for ways to Avoid Negative Impacts, and ways to Mitigate Unavoidable Negative Impacts**
- Documentation and Publication of the **Outcomes**

Organisational Benefits of a PIA

- Risk Identification
- Risk Management
- Avoidance of:
  - Inadequate solutions
  - Feature retro-fitting
  - Unnecessary costs
  - Adoption impediments
  - Stakeholder uncertainty
- Informed media / communications strategy
- Competitive advantage
- Management of Trust / Reputation Aspects:
  - Regulatory Attention
  - Media Attention
  - Embarrassed Execs
  - Embarrassed Ministers
  - Brand Damage

Benefits of Consultation

- Information Gathering from all relevant perspectives
- Information Exchange among the participants
- Mutual Appreciation of one another's perspectives
- Issue Identification
- Solution Discovery
- Feedback about possible solutions from all participants
- Involvement of all parties
- Avoidance of Credible Complaints at a late stage of lack of disclosure of the project, particular features, and impacts

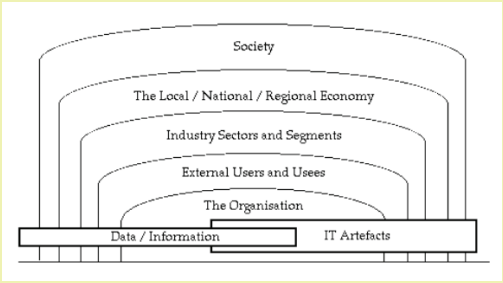
Why Not?
The Reasons for Organisations Not to Do a PIA

- Cost
- Delay
- Information Disclosure about the Organisation's Activities
- Opportunity for Opponents to achieve countervailing power

Conclusions about PIAs and NatSec

- 3 of the 72 projects (4%) passed every test
- 57 of the 72 projects **(79%) failed every test**
- AGD has continually breached expectations, public policy and arguably the law, but has avoided publicity and suffered no sanctions
- 7 advocacy organisations wrote jointly to the AG in September 2011. No reply was received
- The Parliamentary Joint Committee on Intelligence and Security (PJCIS) is a puppet
- The Privacy Commissioner is a captive
- **PIAs don't operate as a Control Mechanism over Australian National Security Initiatives**

The Contested Semantics of 'Security'



Where and What is 'National Security'?

Abuse of Social Control Architecture

- **By an Unelected Government**
  - That invades
  - That seizes power
- **By an Elected Government**
  - That acts outside the law
  - That arranges the law as it wishes
  - That reflects temporary public hysteria

National Security Cabal as Threat to Democracy

Evaluation Meta-Principles

Pre-Conditions
1. Evaluation
2. Consultation
3. Transparency
4. Justification

Design
5. Proportionality
6. Mitigation
7. Controls

Post-Condition
8. Audit

The Contested Semantics of 'Security' and the Curious Case of PIAs applied to National Security Initiatives

Roger Clarke
Xamax Consultancy Pty Ltd, Canberra
Visiting Professor in Computer Science, ANU, Canberra
Visiting Professor in Cyberspace Law & Policy, UNSW, Sydney
http://www.rogerclarke.com/DV/PIANS{.html, .pdf}

Peace Research Institute Oslo (PRIO)
29 August 2016

Agenda

- The Contested Semantics of 'Security'
- The Concept of 'National Security'
- The Australian Context
- PIAs on Australian 'National Security' Measures
- The Critical Role of Evaluation
- The (Ir)Responsibility of the Executive
- The (Ir)Responsibility of the Legislature