UNIVERSITY OF CAMBRIDGE

CSaP centre for science and policy

Centre for Science and Policy

Policy Workshop Report: The Business of Encryption and the Encryption of Business

8 June 2016
Pitt Building, Cambridge

Summary

The UK's Investigatory Powers Bill, which proposes regulation for investigations conducted via communications technology, is moving rapidly through Parliament. Though the legal framework for digital communications is being determined in the political arena, this communication in practice largely occurs in a commercial framework. This workshop therefore focused on the intersection between business and encryption, which is embedded in a high-stakes political landscape pertaining to matters of national security, the economy, and human rights.

Encryption is the mathematical manipulation of information to render it readable solely by the person intended to receive it. Encryption policies are part of the business models of digital communications companies. Encryption technologies represent a business opportunity, and their underutilisation by UK businesses provides opportunities for cybercriminals.

Furthermore, encryption underpins the digital economy; online banking, as well as all online transactions, would not be secure without it. As the implications of the Bill are debated, it is more important than ever to understand how governments, corporations, and civil society are thinking about the business of encryption.

The workshop was held under the Chatham House rule and brought together a diverse range of perspectives from the research, policy, and technology sectors. Beginning with an overview of the political landscape, discussion focused on encryption and the economy as well as on encryption and technology companies and concluded with the identification of significant research gaps in this space.

Key questions for discussion included:

- How are businesses using encryption, and how should they be? How is government regulating the use of encryption, and how should it be?
- What are the implications of weakened encryption for business?
- How do technology companies determine their encryption policies, and what avenues exist for non-governmental actors to engage with this? How do companies' actions affect citizens' rights?
- What are the economics of encryption? Is there a market demand from the public for encryption?
- What synergies exist between the value of encryption for the economy and the value of encryption for human rights, and how might advocates best utilise them – or should they utilise them at all?
- Where is research urgently needed with respect to the intersection between business and encryption?

Discussion

1. The Political Landscape

Since 2001, western democracies have been operating in what legal theorist C. Schmitt would call 'states of exception', where certain laws are temporarily transcended in the name of exceptional circumstances (e.g. issues of national security). However, since 9/11, these purportedly temporary changes are beginning to look permanent. These states of exception have created a 'strange kind of irrational spiral' in terms of policy making leading to consequences such as those below:

- In the face of increasing pressure to minimise the risk from terrorism, various security agencies institutionalised a particular genre of responses – rational, given their mandates and structures – such as the ratcheting up of state surveillance. Subsequently, we are now living in a world where pervasive surveillance is a norm. Reconciling pervasive surveillance with democratic oversight and human rights poses severe challenges, as can be exemplified in current grapples over the UK's Investigatory Power Bill.
- Technology should not be ignored as a factor in this equation – roughly speaking, it provides both opportunities and threats. For example, the Internet could be described as a 'surveillance machine made in heaven' given its ubiquitous and pervasive nature. Encryption technologies make surveillance more difficult but can then lead to politically salient discourses such as the 'going dark' narrative and government measures that pose threats to the viability of business models employed by powerful companies.
- Policy makers in this arena seem to be operating in an evidence-free zone e.g. there seems to be no substantial cost-benefit analysis examining the tradeoffs surrounding encryption.

Discussion Takeaways

- From an economic perspective, encryption is subject to similar forces as privacy; we see elements of privacy paradox behaviour in the public engagement with both (individuals claiming to value these goods but acting contrary to those claims). One cause may be that – as with smoking and sugar consumption – the benefits of digital communications are experienced now by users, while the risks and costs seem to be in a distant future. Legislating around such behaviours historically has been difficult, with the risks reined in too late.
- Encryption policy making is subject to the difficulties incumbent in an assessment of asymmetric risk; rationally, state actors will always be incentivised to pursue more powers if overriding priority is given to national security. Another difficulty, particularly for policy makers and politicians, is a lack of technical understanding of the main constraints or what is in the realm of possibility. Additionally, several misleading discourses influencing encryption policy making are circulating, e.g. the all-or-nothing fallacy where a society can either have privacy or security, but not both simultaneously.
- Several discussants made the point that the lack of clarity around assessing information security issues relates to a lack of clarity around the market value of information-based assets in modern capitalist economies. One discussant noted that there is a significant stream of research on this topic, exemplified by the recent report of Sir Charlie Bean on the Office for National Statistics. Better representing of information-based assets on balance sheets would require a substantial overhaul of out-dated accounting tools and practices.
- Several discussants brought up the difficulty of conducting cost-benefit analyses of encryption policies. Control cases were suggested in terms of before-and-after tests, and one participant noted

that this type of analysis has a precedent, as Germany conducted a control case when considering implementation of a DRIPA-esque bill.

- The global nature of these issues must be paid due attention. For example, the UK could be setting a global precedent, where other states could point to the Bill for justification of significant overreach in surveillance measures.

2. Encryption and the Economy

One of the main issues with the UK's much-discussed Investigatory Powers Bill is the degrees to and ways in which companies can be compelled to assist in the 'removal of electronic protection' and equipment interference.

Encryption can encompass the use of technology to maintain confidentiality, to protect anonymity, and to facilitate access control. All three of these elements are entangled in complex ways, and the Bill attempts to separate them without much heed to their connections or the consequences.

Companies that are impacted by encryption can be divided into two main categories:

- Those for whom encryption is not the core business (e.g. Facebook and Google): from a consumer relations perspective, this can lead to these companies being very vocal about their uses of encryption in certain contexts. They also have significant reasons to oppose the IP bill, as their business will likely suffer significantly if they are forced to assist in state surveillance.
- Those for whom security is a main product: these companies can face significant risks in terms of state pressures and measures to weaken or provide backdoors to their products. UK businesses are particularly susceptible to such risks, particularly in the context of the Investigatory Powers Bill.

Unrealistic aspects of the Investigatory Powers Bill are not the only security challenges facing businesses; the nature of digital threats in combination with the weaknesses of current computer security design leave much to be desired. Relatedly, current security debates need to be oriented to reflect reality: encryption is not optional in today's economy. As computer security expert Matt Blaze recently tweeted, 'Given the state of net security, debating whether crypto should be legal feels like debating whether fire hydrants are an unsightly blight.'

However, security could be significantly improved if companies took responsibility for more rigorous information management so they retained only that data essential for their business needs. In this regard, the forthcoming EU General Data Protection Regulation could be useful to galvanise companies to address issues in storage and processing of data, particularly the kind of sensitive data storage mandated in the Investigatory Powers Bill in relation to Internet Connection Records (ICRs).

More on this can be found here, in Steven Murdoch's recent Royal Society piece focusing on the Exceptional Access provisions of the Investigatory Powers Bill.

Discussion Takeaways

- Much of the Investigatory Powers Bill is codifying more visibly existing practices, but it also contains some fundamentally new and troubling developments. The most salient example is the requirement regarding the retention of Internet Connection Records. The Bill stipulates that every telecommunications operator should, for one year, store records of every web domain that each of us visits. Participants pointed out that the implications for privacy and security were troubling, particularly because there appeared to be little proper legislative review of the scope of the law or possible damages. Additionally, retention and retrieval of ICRs would represent a significant

expense – and it is not clear at the moment if this has been estimated correctly and how the costs would be distributed between companies and the government.

- Several comparisons were drawn between the US and the UK. A number of discussants made the point that the Snowden revelations had resulted in in the 'rolling back' of the surveillance activities of all branches of the US government. The UK, in contrast, has seen no such rolling back; the group discussed why this might be the case. It might be, for example, because the UK government is less subject to constitutional constraints and because the British public is less concerned with these issues. However, the socio-political and economic setting is not static; as levels of cybercrime grow, terrorists attack, and economies fluctuate, the surveillance debate will only become more salient.
- Several discussants brought up the ramifications of the Bill for consumer trust in British technology companies and for citizen and corporate trust in the state. The concept of transparency, and measures to increase it, was proposed as one way to retain and recover trust, as well as expose malfeasance and change behaviour. Concrete suggestions in this arena included sufficient notification systems, better security reporting measures, and short retention of data.
- It was argued that the IP Bill could have severe consequences for the economic competitiveness of British companies in a global market if they are subject to vaguely justified and systematic Equipment Interference. The Bill, in effect, would not only put British companies at a disadvantage in terms of their abilities to provide information security, but would also notify everyone in the global market that they are at this disadvantage.

3. Technology Companies and Encryption

Encryption (particularly in the context of companies and how they use it) needs to be scrutinised. All encryption is not created equal; how does it vary by company, and what are the implications for users? In general, we need to inject more nuance into how we understand encryption, particularly in the context of companies' roles.

- Terminological vagueness is an issue in other arenas of the encryption debate e.g. the much-discussed 'backdoors' that would – in theory, and only in theory – allow the government, and only the government, to read communications encrypted by that technology. Assessing a product based solely on whether or not it allows for the introduction of backdoors is not enough, given the existing security weaknesses of many systems. Furthermore, a better technical understanding of backdoors is needed; in the recent Apple vs. FBI showdown, for example, any tool that was just purportedly for unlocking one iPhone would in fact have turned into a backdoor. We also need more nuance injected into debates and policy in terms of what kinds of criminal evidence is needed in different contexts, e.g. police investigations vs. intelligence.
- Encryption debates have recently and uniquely had civil society and companies on the same side, but this situation (and the reasons behind it) should be scrutinised.
- Talk within policy circles of a 'new sharing norm' among members of the public, based on privacy behaviours, could point to ignorance and resignation of individuals rather than acceptance.
- Finally, when encryption debates are framed in well-trodden narratives (e.g. positioning the intrusive state against the privacy-defending technology company, or vice versa), the result is a stripping out of the nuance of each context. Nuance is essential to any discussion regarding privacy. This could be exemplified in the case of Apple vs. the FBI, where the debate was arguably politicised for the company's reputational benefit.

Discussion Takeaways

- It was suggested that those representing civil society needed to be careful not to gloss over the nuance when aligning with companies on these social issues; there is a need to scrutinise—product by product, context by context—the kinds of encryption being used and the terms under which

they are being used. Corporations' proclamation of opposition to encryption backdoors shouldn't so easily lead to a blanket approval of their entire repertoires.

- The global nature of these issues needs to be taken into account; we could be facing severe negative market externalities in terms of how information is valued e.g. where use of personal data costs to consumers is not factored into transactions. Relatedly, the lack of harmonisation and standardisation in how sensitive data is treated in a globalised economy will eventually lead to 'huge political and commercial consequences'. Along these lines, there is a need for new international conventions, especially on cyber evidence, that set out rules for all to abide by regarding jurisdiction and proper warrants.
- The meaning and practice of informed consent, in terms of both general societal consent to unprecedented levels of surveillance and individual's consent to the tracking of their activities on particular platforms, needs more scrutiny. For example, the terms and conditions of use for popular platforms need to be comprehensible and readable; we need to acknowledge the fallacy that a user's agreement to terms and conditions indicates consent to surveillance – corporate, state, or otherwise.
- Corporate incentives are not necessarily aligned with better security for users. Regulation can be used to force this alignment, such as the security breach notification laws in the US, which made security breaches very expensive for companies.

4. Moving Forward

Following on from the point made at the start of the workshop, that policy making around encryption and business is not sufficiently based on evidence, the workshop concluded with a discussion on priority areas for research. Areas suggested included the following:

- How does trust work in different encryption contexts and in relation to different actors and expectations? How and why is trust changing?
- How is the privacy paradox manifested in different contexts, and how can it be addressed?
- How can we further inject issues of consumer protection into encryption debates, as opposed to predominantly focusing on national security? Relatedly, what work can be done on security standardisation, particularly in the context of Internet of Things? As the number of connected and potentially intrusive devices grows, universal and interoperable protocols for secure communication between devices and controllers are essential.
- If the Investigatory Powers Bill was made understandable, and we polled the public on whether or not they agreed with it, what results would we get? What could we do with this data? (This was in reference to an analogous campaign in India.)
- There is a 'discursive battle' surrounding encryption, where certain discourses (e.g. the 'dark corners', 'all-or-nothing', and 'nothing to hide, nothing to fear'), are very persuasive. How can we identify and trace such misleading discourses as well as counteract them?
- To what extent does understanding issues surrounding encryption require sophisticated technical/legal knowledge, and to what extent is that a myth put out there to benefit particular actors?
- How big is the shortfall and what is the nature of the shortfall between the information the government wants to collect and the resources they have to process that information?
- What kind of literature review or secondary research can be done on the effects of surveillance on behaviour; relatedly, what kind of review can be done of legal approaches to surveillance?
- How much 'bad guy activity', proportionally, is there actually online? How can this be measured?

- How have safeguards against government abuses in this space changed? For example, the sheer labour involved traditionally restricted the extent to which government could carry out surveillance. Now that technology has lowered this friction, legal safeguards become more necessary.
- Could changes in governance produce better policy and practice and more trust? For example, should cyber surveillance and cyber security be in a single entity or separate government organisations?

List of Attendees

- **Sir Richard Mottram** (Chair), former Permanent Secretary, Intelligence, Security and Resilience, Cabinet Office
- **Professor Ross Anderson**, Professor of Security Engineering, Computer Laboratory, University of Cambridge
- **Andrew Brown**, Lead writer and Editorial Board member, The Guardian
- **Guy Cohen**, Strategic Relationships Manager, Privitar Ltd
- **Dr Rob Doubleday**, Executive Director, Centre for Science and Policy
- **Dr David Erdos**, Lecturer in Law , Faculty of Law, University of Cambridge
- **Oliver Ferrari**, Policy & Engagement Team, Foreign & Commonwealth Office
- **Dr Florent Frederix**, Principal Administrator, Trust and Security Unit, EC DG Connect
- **Dr Julian Huppert**, Lecturer, Department of Physics, University of Cambridge
- **Rebekah Larsen** (Note-taker), PhD student, Digital rights and theories of power, Department of Sociology
- **Dr Ella McPherson**, Lecturer in the Sociology of New Media and Digital Technology, Department of Sociology, University of Cambridge
- **Dr Steven Murdoch**, Principal Research Fellow, Information Security Research Group, Computer Science, UCL
- **Professor John Naughton**, Senior Research Fellow, Centre for Research in the Arts, Social Sciences and Humanities, University of Cambridge
- **Professor Jim Norton**, External Board Member, UK Parliamentary Office of Science & Technology
- **Dr Julia Powles**, Postdoctoral Researcher, Faculty of Law, University of Cambridge
- **John Taysom**, Honorary Visiting Professor, UCL Department of Computer Science
- **Alex van Someren**, General Partner, Amadeus Capital Partners Ltd
- **Andrew Watson,** Technical Director, Object Management Group
- **Joe Westby**, Campaigner, Business and Human Rights, Amnesty International