



7 February 2017

**The Dilemmas of Privacy and Surveillance**

Professor Martyn Thomas

**Introduction**  
  
Cyberspace is a fifth dimension of the world that we live in, orthogonal to the three dimensions of physical space and the dimension of time. Cyberspace and the physical world interact in many ways, and *cyber* is now used to refer to far more than the internet; it covers radio frequency and other electromagnetic communications and the processing of sensor data for example. Cyberspace is somewhere we work, shop, play, dream, talk, meet and relax. We do almost all the things in cyberspace that we do in the three dimensions of physical space and whilst we consciously do some of these things in public, some of them we expect to be private. Privacy is long established as a basic human right and it can be essential for some individuals at various times in their lives, to protect their physical and mental health, their families, and the integrity of their work. In my lecture on *Big Data: The Broken Promise of Anonymity* (14 June 2016) I explained why it is simple-minded and offensive to claim that “if you have nothing to hide, you have nothing to fear”.

## In the physical world, societies have evolved many behaviours and structures to give us control over what we allow others to see of our private lives. There are walls, doors with locks, clothes and screens, safes and secret places. Gradually, technology has eroded privacy. Telephoto lenses have given paparazzi the ability to spy on people who have a realistic expectation of privacy. CCTV and image analysis have taken away the anonymity that we used to have in a crowd, whilst automatic number-plate recognition (ANPR) has reduced the privacy of car journeys. Millimetre wave body scanners can see through clothes, and the sensors that are being developed using new quantum technologies will be able to sense through solid objects and round corners[[1]](#endnote-1).

## In the physical world there are undesirable as well as benign activities and societies have created laws, to draw a line between acceptable and unacceptable behaviour, and law enforcement agencies (LEAs) to deter, detect and punish violations. Detection of crime involves discovering things that criminals would like to keep secret (such as their identity, the details of their illegal activities and the location of their illegal assets) and criminals will use whatever means are available to protect their secrets. To be effective, policing must breach the privacy of criminals.

Cyberspace has its own structures that have been designed to give us control over what we reveal and what we keep to ourselves, such as firewalls, passwords and encryption, and these Privacy Enhancing Technologies (PETs) have been developed to try to keep pace with the increasing need for privacy online.

Crime will exist wherever there is motive and opportunity and, just as lawful activities have moved into cyberspace, so has crime. Some of this can be best seen as cyber-enabled crime, such as the use of radio-frequency “sniffers” to record and repeat the signals that lock and unlock car doors remotely and disable car alarms. Some crimes are pure cybercrimes, in that they are crimes wholly in cyberspace, such as stealing cybercurrencies such as bitcoins or intercepting and redirecting electronic money transfers. Cyberspace is already far too important for it to be left unregulated and unpoliced and, to be effective, policing in cyberspace must breach the privacy of cybercriminals.

In a democratic society, it is important that the state should exercise the powers that citizens have given their government honestly, fairly and proportionately. The dilemmas that are the subject of this lecture arise out of the inescapable conflict between the essential human right to privacy and the requirement that law enforcement agencies (LEAs) breach that privacy if they are to be fully effective in performing their democratically agreed duties to detect and disrupt crime.

## Content and Metadata

## A distinction is often made between content and metadata: metadata (‘data about data’) refers (for example) to who you have phoned, emailed, messaged, Skyped … and when you did it, and where; contentis the data that reveals what you said in your messages and phonecalls. When programmes of wide surveillance are being defended, the argument is often made that metadata is not personal data and that any concerns about privacy or human rights only apply to the content.

In the physical world there is usually an obvious distinction between the address on a parcel and what is inside it. You can see a car passing and record the number plate without knowing where they are going and why, or see two people talking without knowing what is being said. Yet inferences can be drawn just from where someone has been; if a celebrity is photographed coming out of a drug rehabilitation clinic, damage may be caused if the photograph is published.

In cyberspace making a clear distinction between content and metadata becomes complex and difficult. The record of your web browsing may be considered to be metadata, though if you are the chef in 10 Downing Street and you visit a website about untraceable poisons followed by an online supplier of chemicals and then Visa, MI5 might reasonably become suspicious without having inspected the content of your shopping basket.

This means that it is very hard to draw a clear line between content and metadata and probably impossible to find a defendable way to express the distinction that can be implemented as a software algorithm and used to determine what should be collected, stored, searched and made available without consent or a court order. Is it content or metadata that someone is searching for information about sexually transmitted diseases? Or browsing a website on the same subject? Is it content or metadata that someone has visited a website belonging to a company that provides abortion services? Does the classification between content and metadata change if the data shows that they spent 40 minutes on several different pages of the site, during which time they also visited Visa and updated their calendar?

Data analysis can draw rich conclusions from metadata and from analysing the networks of contacts and communications between different individuals, and this can be done through the metadata of emails and messaging apps, through location data, and by analysing the patterns of internet traffic from your various electronic devices and those of your contacts and *their* contacts. What seems to be pure metadata can still reveal very personal details. Your phone records and app locations show where you were, and when, so it is easy to see where someone spends the night, and who they spend it close to, what offices, shops, clubs and clinics they visit and how often, and many similar details that reveal intimate details of personal and business lives. In my opinion, metadata that reveals personal information should be considered to be personal data and subject to the same privacy laws as would apply to any other form of data.

**The RAEng Report**

Ten years ago, the Royal Academy of Engineering published a report with the same title as this lecture *Dilemmas of Privacy and Surveillance[[2]](#endnote-2)* following a call for evidence and a year-long study chaired by Professor Nigel Gilbert FREng AcSS.

*RAEng report.tiff*The RAEng Report’s introduction to the basic dilemmas is still relevant:

*Privacy comes in many forms, relating to what it is that one wishes to keep private:*

* *privacy as confidentiality: we might want to keep certain information about ourselves, or certain things that we do, secret from everyone else or selected others;*
* *privacy as anonymity: we might want some of our actions (even those done in public) not to be traceable to us as specific individuals;*
* *similarly, we might wish for privacy of identity: the right to keep one's identity unknown for any reason, including keeping one's individual identity separate from a public persona or official role;*
* *privacy as self-determination: we might consider some of our behaviour private in that it is 'up to us' and no business of others (where those 'others' may range from the state to our employers);*
* *similarly, we can understand privacy as freedom to be 'left alone', to go about our business without being checked on: this includes freedom of expression, as we might wish to express views that the government, our employers, or our neighbours might not like to hear;*
* *privacy as control of personal data: we might desire the right to control information about us - where it is recorded, who sees it, who ensures that it is correct, and so on.*

*These various forms of privacy can potentially clash with a number of values. Each has to be weighed against one or more of the following:*

* *accountability for personal or official actions;*
* *the need for crime prevention and detection and for security generally: our desire to be able to engage in our personal affairs without anyone knowing is always offset against our desire for criminals not to have the same opportunity;*
* *efficiency, convenience and speed in access to goods or services: this relates particularly to services accessed online, where access might depend on entering personal, identifying information;*
* *access to services that depend on fulfilling specific criteria such as being above an age limit or having a disability, or being the genuine owner of a particular credit card;*
* *the need to monitor health risks, such as outbreaks of infectious diseases;*
* *public and legal standards of behaviour which might weigh against some personal choices.*

*The varieties of privacy and the various values it can be in tension with mean that one cannot appeal to a straightforward, singular right to privacy. Privacy is inherently contingent and political, sensitive to changes in society and changes in technology. This means that there needs to be constant reappraisal of whether data are to be considered private and constant reappraisal of the way privacy dilemmas are handled.*

This lecture updates the RAEng Report because much has changed in ten years. The ability to capture and analyse personal data has advanced remarkably and surveillance and data analysis technologies have been adopted far more widely, which has brought benefits and harm, often benefiting some people whilst simultaneously disadvantaging others. As one example, the use of *no fly lists* for air passengers may have deterred some terrorist attacks and saved lives (though this is difficult to verify); at the same time it has undoubtedly caused difficulties for many harmless citizens. The *Washington Post* reported in June 2016 that there were 81,000 names on the FBI’s no fly list[[3]](#endnote-3) though other estimates are far higher and the list certainly contains errors: the Guardian has reported that *“in 2012, JetBlue airline removed an 18-month-old girl from a flight before takeoff after she was flagged as no-fly. JetBlue later apologised, blaming the incident on a computer glitch”*[[4]](#endnote-4).

Surveillance technology will continue to grow in power and to be exploited more widely by national and foreign governments, public bodies and businesses, as we saw in my earlier lecture on 18 October 2016 *Are You the Customer or the Product?[[5]](#endnote-5).* If we are to gain the great benefits from Big Data and from data analytics[[6]](#endnote-6) then democratic decisions have to be made on what collection and use of data is reasonable in our society – and these decisions have to be enforced transparently and with judicial oversight.

Surveillance is carried out by governments and by commercial companies, and it is apparent that many people are more willing to share their personal data with companies than they are to share the same data with governments. People buy devices such as Amazon Echo with the Alexa Voice Service, that *“has seven microphones and beam-forming technology so it can hear you from across the room—even in noisy environments”*[[7]](#endnote-7). This raises privacy concerns for some users:

*“The device, after all, was uploading personal data to Amazon’s servers. How much remains unclear. Alexa streams audio “a fraction of a second” before the “wake word” and continues until the request has been processed, according to Amazon. So fragments of intimate conversations may be captured. A few days after my wife and I discussed babies, my Kindle showed an advertisement for Seventh Generation diapers. We had not mooched for baby products on Amazon or Google. Maybe we had left digital tracks somewhere else? Even so, it felt creepy”[[8]](#endnote-8).* Others have raised concerns about the voice recognition that is increasingly built into children’s toys such as the *My Friend Cayla* doll[[9]](#endnote-9).

The customers who buy such products are presumably happy to have their own and their children’s private conversations recorded and sent to commercial companies for processing. Yet it seems likely that many of the same people would feel uneasy if their government (or a foreign government) had a listening device in their house. Edward Snowden, the National Security Agency contractor and whistleblower, was certainly very concerned about what he had discovered about government surveillance. The files that he copied and released shocked the world.

**Government Surveillance: What did Edward Snowden reveal, and why?**

**Snowden.tiff**  
How Edward Snowden progressed from being TheTrueHOOHA, an 18 year old, technically naive user of the Ars Technica website[[10]](#endnote-10) and became a contractor working inside the NSA has been described many times.[[11]](#endnote-11) His role in the NSA was as a system administrator (a “sysadmin”) which gave him (and around 1000 other sysadmins) the ability to access hundreds of computers and their contents without leaving any record that he had done so.

Snowden seems to have become highly competent and to have grown increasingly alarmed by the scale of the surveillance activities that he discovered the NSA was undertaking. The Guardian reported that although Snowden had “a salary of roughly $200,000, a girlfriend with whom he shared a home in Hawaii, a stable career, and a family he loves”, Snowden said:

*I'm willing to sacrifice all of that because I can't in good conscience allow the US government to destroy privacy, internet freedom and basic liberties for people around the world with this massive surveillance machine they're secretly building. … I really want the focus to be on these documents and the debate which I hope this will trigger among citizens around the globe about what kind of world we want to live in. … … My sole motive is to inform the public as to that which is done in their name and that which is done against them.*

Snowden copied many thousands of highly classified documents[[12]](#endnote-12) and passed them to journalists Glenn Greenwald and Laura Poitras. These documents have been released (after some redaction, to remove the names of individuals who might be put at risk, for example) through leading newspapers in the UK, the USA, Germany and elsewhere. All the example slides used in this lecture have been copied from publicly available websites.

The security services such as the NSA are well funded and have extraordinary technical resources. The top secret files that Snowden downloaded and leaked revealed that the NSA and its partner agencies (which include GCHQ in the UK) collect huge amounts of internet traffic and other data and store it for later processing. It seems incredible that it could be possible to intercept all the data that flows through major internet cables – thousands of Gigabytes every second – but that is what Snowden revealed.

The USA is connected to 63 countries by fibre optic cables and the UK is connected to 57[[13]](#endnote-13). The NSA and GCHQ are able to probe these cables and to collect the data (called **upstream** collection, which is then stored, filtered to remove duplicated and irrelevant data (such as Netflix and music downloads) and scanned. According to the Guardian newspaper,[[14]](#endnote-14) by 2012

*‘GCHQ was handling 600m "telephone events" each day, had tapped more than 200 fibre-optic cables and was able to process data from at least 46 of them at a time. Each of the cables carries data at a rate of 10 gigabits per second, so the tapped cables had the capacity, in theory, to deliver more than 21 petabytes a day – equivalent to sending all the information in all the books in the British Library 192 times every 24 hours’.*

500 analysts from GCHQ and the NSA were assigned to analyse the collected data. The GCHQ upstream project had the codename TEMPORA*,* and the similar upstream NSA projects were called BLARNEY, FAIRVIEW, STORMBREW and OAKSTAR.

The Snowden papers revealed that the NSA also had a major **downstream** collection project called PRISM, which according to an NSA slide presentation collected data directly from Google, Facebook, Apple, Yahoo and other large US internet companies. Many other secret collection capabilities were revealed, the details of which can easily be found by following the links in the references that I have provided or by searching on the internet. The ambition of national security services is to collect all the available data, all the time (GCHQ called it **Mastering the Internet**) and by 2012 GCHQ and the NSA were remarkably close to this goal.

Edward Snowden’s revelations about the degree of surveillance carried out by American, UK and other nations’ security services caused widespread shock and led to changes in US law, greater use of encryption by law-abiding citizens as well as criminals and terrorists, and great tensions in the relationships between some US internet companies and the US Government. The response in the UK was more muted and the UK parliament has subsequently passed legislation[[15]](#endnote-15) to establish clearly the lawfulness of some of the actions that Snowden revealed and where the legality had been questioned. The Investigatory Powers Act has been described as “one of the most extreme surveillance laws ever passed in a democracy”[[16]](#endnote-16) and, as we shall see later, a ruling[[17]](#endnote-17) in the European Court of Justice may mean that some of the new powers are unlawful while Britain remains in the EU, and may mean that EU countries cannot export personal data to the UK after the UK leaves.

Law enforcement agencies (LEAs) and security services are interested in discovering who is committing or planning serious crimes and with whom, but official surveillance can extend to include political dissidence, pressure groups or industrial action – and even to fly-tipping and more minor matters.

Companies, journalists, estranged partners, stalkers and nosy neighbours also carry out various forms of surveillance and many commercial and professional activities (such as medical and legal consultations, merger and acquisition negotiations, and innovative product development) are necessarily secret. There will therefore always be people who have personal or commercial reasons to conduct their affairs in private.

There will probably always be concerns about the surveillance that is undertaken by companies or in support of the State’s obligation to keep its citizens safe and opinions will differ about whether such surveillance is proportionate and the extent to which those who undertake surveillance are properly accountable. This creates a contest between those who seek to enhance individual privacy, for whatever reasons, and those who wish to track what individuals are planning and doing, and whom they are meeting and where. Much of this contest is fought around the technical aspects of surveillance and the use of privacy-enhancing technologies (PETs).

## Example PETs and Dilemmas: Encryption, Tor and the Egotistical Giraffe

## The basic PET is encryption: making data unreadable through an algorithm that scrambles the data so that it can only be unscrambled by someone who already has a secret key. Encryption is used routinely by almost everyone; it is automatically applied by e-commerce websites, banks, most mail and messaging services, and wherever else the website URL starts https:. Encryption, applied properly, makes the data unreadable.

## Encryption has been a major challenge for LEAs and security services and they have committed substantial resources to overcoming it. In the 1980s and 1990s, the export of encryption technologies was prohibited by many countries, including the UK and the USA, though this was circumvented, most famously by Philip Zimmermann, who developed and released Pretty Good Privacy (PGP)[[18]](#endnote-18). Governments attempted to introduce “key escrow”, laws that required encryption keys to be revealed to the Government, but this was seen to be impractical and dangerous[[19]](#endnote-19). The security and intelligence agencies have continued to seek ways to circumvent encryption; the Snowden papers revealed that they had made remarkable progress.

NSA decrypt.tiffThe Guardian reported in September 2013[[20]](#endnote-20) that “*US and British intelligence agencies have successfully cracked much of the online encryption relied upon by hundreds of millions of people to protect the privacy of their personal data, online transactions and emails, according to top-secret documents revealed by former contractor Edward Snowden”.*

According to the Guardian, the program to break encryption, codenamed BULLRUN, had an annual budget of £250 million and the methods used *“include covert measures to ensure NSA control over setting of international encryption standards, the use of supercomputers to break encryption with "brute force", and – the most closely guarded secret of all – collaboration with technology companies and internet service providers themselves. Through these covert partnerships, the agencies have inserted secret vulnerabilities – known as backdoors or trapdoors – into commercial encryption software”.*

Security experts were appalled that the security agencies had deliberately weakened widely used encryption standards and commercial products, arguing that it undermined the internet security on which so much of society depends. They reasoned that the weaknesses would become known to other states and to criminals, and so technologists have fought back by redoubling efforts to create strong encryption methods and products. The encryption battle between the spooks and the geeks started seriously in the 1990s and is still fully engaged.

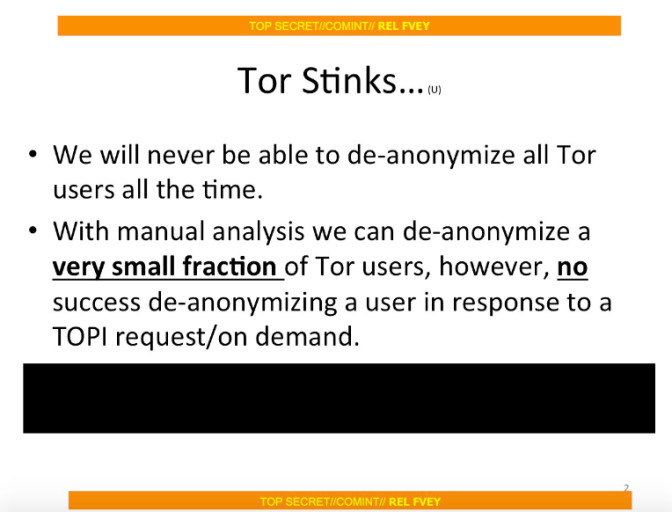
Encryption can protect the *contents* of messages but sometimes it can be important even to conceal internet browsing and who is communicating with whom. Tor, *The Onion Router,* was created for this purpose and the Tor project[[21]](#endnote-21) explains the need as follows

Using Tor protects you against a common form of Internet surveillance known as "traffic analysis." Traffic analysis can be used to infer who is talking to whom over a public network. Knowing the source and destination of your Internet traffic allows others to track your behavior and interests. This can impact your checkbook if, for example, an e-commerce site uses price discrimination based on your country or institution of origin. It can even threaten your job and physical safety by revealing who and where you are. For example, if you're travelling abroad and you connect to your employer's computers to check or send mail, you can inadvertently reveal your national origin and professional affiliation to anyone observing the network, even if the connection is encrypted.

Tor works by bouncing the Tor user’s browsing between a number of relay sites, over encrypted links, before it emerges into the internet and reaches the intended destination website.

How Tor works 2.tiffHow Tor works 1.tiff

Security agencies have found it difficult to identify Tor users, as some of the documents leaked by Edward Snowden revealed[[22]](#endnote-22).



The top secret papers leaked by Edward Snowden[[23]](#endnote-23) revealed that the Tailored operations Group in the US National Security Agency (NSA) had developed a way of identifying some Tor users and given it the codename EgotisticalGiraffe[[24]](#endnote-24) (the referenced top secret presentation gives more details). But the Guardian newspaper has reported[[25]](#endnote-25) that the US government recognises that Tor has many important and legitimate uses.

The Broadcasting Board of Governors, a federal agency whose mission is to "inform, engage, and connect people around the world in support of freedom and democracy" through networks such as Voice of America, also supported Tor's development until October 2012 to ensure that people in countries such as Iran and China could access BBG content. Tor continues to receive federal funds through Radio Free Asia, which is funded by a federal grant from BBG. The governments of both these countries have attempted to curtail Tor's use: China has tried on multiple occasions to block Tor entirely, while one of the motives behind Iranian efforts to create a "national internet" entirely under government control was to prevent circumvention of those controls. The NSA's own documents acknowledge the service's wide use in countries where the internet is routinely surveilled or censored. One presentation notes that among uses of Tor for "general privacy" and "non-attribution", it can be used for "circumvention of nation state internet policies" – and is used by "dissidents" in "Iran, China, etc".

It is inevitable that anything that allows people to communicate in secret will be used for illicit as well as for legitimate purposes. Government agencies that are responsible for detecting and preventing crime or for spying on foreign governments and foreign companies need to gain access to these secret communications, (including some that happened in the past, before the suspects were under surveillance). At the same time, the many legitimate users of secrecy, such as banks, e-commerce, lawyers (and almost every other organisation at one time or another) need to keep their systems secure against intrusion by criminals, competitors and hackers.

These are conflicting requirements; we cannot have systems that are completely secure whilst ensuring that criminals cannot use them to evade detection. When most of the world’s computing and communications uses commercial off-the-shelf software, we want security holes to be patched and bugs to be fixed, even if this closes some loophole that the NSA or GCHQ are using for their own purposes, such as the browser exploits in EgotisticalGiraffe. There is no easy answer to the question “how much security is enough but not too much?”

## The Investigatory Powers Act 2016

## The Investigatory Powers Act (IPA) became law on 29 November 2016. It is 227 pages of detailed legislation, plus 64 Schedules[[26]](#endnote-26). The Act, which has been called a *Snoopers’ Charter,* is extremely controversial: whereas Home Secretary Amber Rudd described it as *“world-leading legislation that provides unprecedented transparency and substantial privacy protection”*, Bella Sankey, policy director of Liberty, the Civil Liberties group, said that the Act *“opens every detail of every citizen’s online life up to state eyes, drowning the authorities in data and putting innocent people’s personal information at massive risk. This new law is world-leading – but only as a beacon for despots everywhere”*.

## The Independent newspaper explained[[27]](#endnote-27) that the Act *“adds new surveillance powers including rules that force internet providers to keep complete records of every website that all of their customers visit. Those will be available to a wide range of agencies, which includes the Department for Work and Pensions as well as the Food Standards Agency”,* adding *“As well as those internet connection records, surveillance agencies will also be given new powers to force companies to help hack into phones, and to collect more information than ever before on anyone in Britain”.*

Schedule 4 of the IPA[[28]](#endnote-28) defines the public authorities that can obtain data. It includes the police, MI5, MI6, GCHQ, MoD, Department of Health, Home Office, Ministry of Justice, Department for Transport, National Crime Agency, HMRC, Department of Work and Pensions, Ambulance Trusts, Criminal Cases Review Commission, Competition and Markets Authority, Financial Conduct Authority, A fire and rescue authority under the Fire and Rescue Services Act 2004, Food Standards Agency, Gambling Commission, Gangmasters and Labour Abuse Authority, Health and Safety Executive, Independent Police Complaints Commission, Information Commissioner, National Health Service Business Services Authority, Office of Communications, Serious Fraud Office and the equivalent authorities in Scotland, Northern Ireland and Wales.

The reasons why data may be obtained are defined in Section 61 (7) as

*(a) in the interests of national security,*

*(b) for the purpose of preventing or detecting crime or of preventing disorder,*

*(c) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security,*

*(d) in the interests of public safety,*

*(e) for the purpose of protecting public health,*

*(f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department,*

*(g) for the purpose of preventing death or injury or any damage to a person’s physical or mental health, or of mitigating any injury or damage to a person’s physical or mental health,*

*(h) to assist investigations into alleged miscarriages of justice,*

*(i) where a person (“P”) has died or is unable to identify themselves because of a physical or mental condition—*

*(i) to assist in identifying P, or*

*(ii) to obtain information about P’s next of kin or other persons connected with P or about the reason for P’s death or condition, or*

*(j) for the purpose of exercising functions relating to—*

*(i) the regulation of financial services and markets, or*

*(ii )financial stability.*

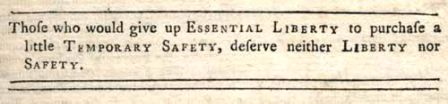
According to the Open Rights Group[[29]](#endnote-29), The Court of Justice of the European Union (CJEU) has issued a judgment that could force the Government to change the Investigatory Powers Act – just weeks after the law received royal assent. The judgment relates to a case that argued that the previous legislation (DRIPA[[30]](#endnote-30)) is inconsistent with EU law. The CJEU agreed, ruling that mass retention of personal data is not permissible, that access to personal data must be authorised by an independent body, that only data belonging to people who are suspected of serious crimes can be accessed, and that individuals need to be notified if their data is accessed. Although DRIPA expired at the end of 2016, the same principles are expected to apply to the powers in the new IPA; if this were upheld by the courts then the IPA would become unlawful whilst the UK remains a member of the EU and therefore subject to its laws. Once the UK leaves the EU, having UK data laws that would be illegal in the EU would be likely to become a barrier to the free movement of data between the UK and EU countries.

**Quis custodiet ipsos custodes?**

When such vast amounts of private data are collected and stored, the custody and security of that data are of great importance. The IPA provides considerable detail about the way in which the data should be held and who can authorise collection, retention and release. But it all comes down to trust. It was clear from the reactions to the Snowden papers that although it was obvious that the security and intelligence agencies (SIAs) were intercepting and collecting communications, almost no-one had realised that they could do it (and were doing it) on such a vast scale or that they had broken most encryption and put backdoors into many commercial products. It seems that even Cabinet Ministers were unaware of the scale and nature of these activities and of their possible illegality, so democratic oversight was certainly limited and many people considered it to have been inadequate.

## Governments do not have a flawless record of keeping secrets secret and the dilemmas will continue to grow, as more data is communicated, as data analysis techniques improve, and as the SIAs develop even better ways to carry out their surveillance. At the same time, privacy activists will challenge the SIAs in the courts and academic and commercial cryptographers will work to make their products and encryption ever more secure. The battle between the spooks and the geeks will continue and the answer to the question “who should win” can only be answered by careful and well-informed debate to determine what sort of society we want to live in, how much we trust current and future governments, agencies and companies, and where we want to place the balance between privacy and surveillance.

This is not a new debate. Benjamin Franklin expressed his views on the dilemmas in a letter to the Governor of Pennsylvania in 1755 and on the title page of his book *An Historical Review of the Constitution and Government of Pennsylvania*:



© Martyn Thomas CBE FREng, 2017

1. https://www.gov.uk/government/publications/quantum-technologies-blackett-review [↑](#endnote-ref-1)
2. <http://www.raeng.org.uk/publications/reports/dilemmas-of-privacy-and-surveillance-report> [↑](#endnote-ref-2)
3. <http://www.washingtontimes.com/news/2016/jun/20/fbi-no-fly-list-revealed-81k-names-fewer-1k-us/> [↑](#endnote-ref-3)
4. <https://www.theguardian.com/us-news/2015/dec/09/no-fly-list-errors-gun-control-obama> [↑](#endnote-ref-4)
5. <http://www.gresham.ac.uk/lectures-and-events/are-you-customer-or-the-product> [↑](#endnote-ref-5)
6. <http://www.gresham.ac.uk/lectures-and-events/big-data-the-broken-promise-of-anonymisation> [↑](#endnote-ref-6)
7. https://www.amazon.co.uk/dp/B01GAGVIE4 [↑](#endnote-ref-7)
8. https://www.theguardian.com/technology/2015/nov/21/amazon-echo-alexa-home-robot-privacy-cloud [↑](#endnote-ref-8)
9. http://fortune.com/2016/12/08/my-friend-cayla-doll/ [↑](#endnote-ref-9)
10. arstechnica.com. Snowden’s pseudonym in the arstechnica forums was TheTrueHOOHA. [↑](#endnote-ref-10)
11. <https://www.theguardian.com/world/2014/feb/01/edward-snowden-intelligence-leak-nsa-contractor-extract> [↑](#endnote-ref-11)
12. https://snowdenarchive.cjfe.org/greenstone/cgi-bin/library.cgi [↑](#endnote-ref-12)
13. <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1> [↑](#endnote-ref-13)
14. <https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa> [↑](#endnote-ref-14)
15. <http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted> [↑](#endnote-ref-15)
16. <https://www.openrightsgroup.org/press/releases/2016/investigatory-powers-act-most-extreme-surveillance-law> [↑](#endnote-ref-16)
17. <https://www.theguardian.com/law/2016/dec/21/eus-highest-court-delivers-blow-to-uk-snoopers-charter> [↑](#endnote-ref-17)
18. <http://www.pgpi.org/> [↑](#endnote-ref-18)
19. https://www.schneier.com/academic/archives/1997/04/the\_risks\_of\_key\_rec.html [↑](#endnote-ref-19)
20. https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security [↑](#endnote-ref-20)
21. <https://www.torproject.org/about/overview.html.en> [↑](#endnote-ref-21)
22. <https://edwardsnowden.com/docs/docs/tor-stinks-presentation.pdf> [↑](#endnote-ref-22)
23. The archive of papers leaked by Edward Snowden is many gigabytes in size and contains details of hundreds of top secret surveillance activities. It cab be accessed online, for example at https://snowdenarchive.cjfe.org/greenstone/cgi-bin/library.cgi [↑](#endnote-ref-23)
24. <https://cryptome.org/2013/10/nsa-egotistical-giraffe.pdf> [↑](#endnote-ref-24)
25. <https://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption> [↑](#endnote-ref-25)
26. http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted [↑](#endnote-ref-26)
27. http://www.independent.co.uk/life-style/gadgets-and-tech/news/investigatory-powers-bill-snoopers-charter-passed-royal-assent-spying-surveillance-a7445276.html [↑](#endnote-ref-27)
28. http://www.legislation.gov.uk/ukpga/2016/25/schedule/4/enacted [↑](#endnote-ref-28)
29. https://www.openrightsgroup.org/press/releases/2016/parliament-must-change-the-investigatory-powers-act-in-response-to-cjeu-ruling [↑](#endnote-ref-29)
30. http://www.legislation.gov.uk/ukpga/2014/27/pdfs/ukpga\_20140027\_en.pdf [↑](#endnote-ref-30)