OPEN RIGHTS GROUP

DIGITAL SURVEILLANCE

Why the Snoopers' Charter is the wrong approach:

A call for targeted and accountable investigatory powers

About Open Rights Group

Open Rights Group (ORG) was formed in 2005 by a group of technology experts and activists to campaign for human rights and civil liberties in the digital age. ORG is funded by over 1,500 people, each contributing small regular amounts, and a number of grant giving organisations such as Joseph Rowntree Reform Trust, Sigrid Rausing Trust and Open Society Foundation.

Report Editors

Jim Killock
Executive Director

Since joining Open Rights Group in January 2009, Jim has led campaigns against three strikes and the Digital Economy Act, the company Phorm and its plans to snoop on UK Internet users, and against pervasive government Internet surveillance. He is working on data protection and privacy issues, as well as helping ORG to grow in size and breadth. He was named as one of the 50 most influential people on IP issues by Managing IP in 2012. In the same year ORG won Liberty's Human Rights Campaigner of Year award alongside 38 Degrees, for work on issues from copyright to the Snooper's Charter.

Peter Bradwell
Policy Director

Peter joined ORG in January 2011, initially working on copyright reform. Before this he worked at the think tank Demos for four years, where he focused primarily on technology policy and the relationship between technology and society. Peter has authored a number of reports, including our reports on mobile Internet censorship in the UK, the availability of digital film services and consultation responses on the Communications Data Bill and data protection legislation in Europe.

Ben Zevenbergen
Researcher

Ben joined the Open Rights Group on a part-time basis, to help with campaigns and research, alongside his PhD/DPhil on Internet science at the Oxford Internet Institute. He has worked on legal, political and policy aspects of the information society for several years. Most recently he was a policy advisor to an MEP in the European Parliament, working on Europe's Digital Agenda. Previously Ben worked as an ICT/IP lawyer and policy consultant in the Netherlands. Ben holds a degree in law, and a masters in information law.

Contents

Introduction:

Surveillance law is not a 'them and us' problem

"Anybody who is against this bill is putting politics before people's lives....

It's a question of whose side you're on."

Rt Hon Theresa May MP, December 2012[1]

This statement from the Home Secretary, made in December 2012, tells us a lot about the approach that her Department has taken to the development of surveillance policy. It also helps to explain why the draft Communications Data Bill (CDB) poses such a disproportionate risk to our privacy.

The Home Office have often framed the debate over the CDB in 'them and us' terms. But if this really does just come down to picking sides, it is odd that both of the Parliamentary committees tasked with examining the draft Bill – the Joint Committee on the draft Communications Data Bill and the Intelligence and Security Committee – reached such critical conclusions[2].

Both committees noticed that there are more questions to ask when considering surveillance law than whether you are on the side of criminals. They include what current capability gaps there are, what new information will be gathered and from whom, how intrusive the information is, how any technological solutions will work, and what authorisations for access to data should be required.

But at no time have the Government attempted to seriously address those questions openly. The Home Office instead wrote the Communications Data Bill in isolation.

In its report, the Joint Committee examining the CDB lamented that there was no consultation, no proper definition of the problem and no adequate explanation of, – or evidence for – the Home Office's proposed solution. The Bill appeared built to withstand public scrutiny, rather than be informed by it.

The result is, perhaps unsurprisingly, a draft Bill that the Committee concluded pays ***"insufficient attention to the duty to respect the right to privacy, and goes further than it need or should."*** The CDB would lead to the collection of far too much information, about far too many people – effectively everyone – and would allow far too many people access to it.

This report

This situation could have been avoided. This report demonstrates that surveillance policy makers have options, many of which are a lot less intrusive than the powers proposed by the CDB, and that civil society is open to meaningful engagement about surveillance laws in the digital age. It is written for a general audience by leading experts, academics and representatives of a number of civil society groups. The articles in this publication serve as an example of the sort of conversations that would be possible through a proper public debate about what information should be collected and who should have access to it.

The opening two chapters put the CDB in historical and legal context.

In chapter one, **Duncan Campbell** sets out the history of the tension between state surveillance and efforts to protect individuals' privacy. He explains why the draft Communications Data Bill is "the latest chapter in the history of British state surveillance." He also tells the parallel story of efforts to keep surveillance powers in check, including the 1972 Royal Commission on Privacy which "set out 10 principles of data protection that later underpinned data protection statutes in Europe and the UK."

In chapter two **Angela Patrick**, Director of Human Rights Policy at JUSTICE, gives an overview of the current settlement between the law, surveillance and the protection of privacy. She looks at how the draft Communications Data Bill could exacerbate problems with existing surveillance law, for example relating to oversight and complexity. She highlights that the overriding difference between the draft CDB and the existing law is the move "away from the presumption that for limited purposes, the State may access data already retained or reasonably obtainable by service providers...Instead, it creates a statutory basis for the generation, collection and retention of data about us all."

In chapter three, **Richard Clayton** outlines in detail key surveillance technologies, showing what information about us is available and how the technology to gather and access it works. He outlines how the 'filter' – a key part of the CDB proposals – will work. By correlating information from multiple sources, he explains how the filter can answer complex queries. For example, he suggests that "the source of an embarrassing leak could be identified by cross-correlating records to pick out exactly who in Whitehall sent out an email whose reception by a journalist triggered an immediate call to the relevant newspaper editor."

Peter Sommer, in chapter four, argues that while surveillance law "is about balancing competing objectives", a number factors inhibit "sensible and balanced discussion". They include the pace of technological change, the demands of the law enforcement community, the level of technical and legal expertise required to understand how best to respond, and the fear of getting it wrong.

Chapter five features contributions from a range of experts setting out how more privacy-friendly surveillance policy could work.

For example, **Caspar Bowden** suggests how 'data preservation' policies could work to limit whose data is collected. **Sam Smith** from Privacy International argues that more could be done to help law enforcement make better use of what information is already available. **Rachel Robinson** from Liberty recommends lifting the ban on the use of intercept evidence in court, and **Peter Sommer** calls for a Royal Commission into surveillance laws in the digital age.

In our conclusion we draw together these contributions and make some recommendations for future surveillance policy making.

Notes

1. http://www.thesun.co.uk/sol/homepage/news/politics/4678082/Track-crime-on-net-or-well-see-more-people-die.html#ixzz2NL7B6fcr

2. See the reports of the Joint Committee on the draft Communications Data Bill (December 2012) http://www.publications.parliament.uk/pa/jt201213/jtselect/jtdraftcomuni/79/7902.htm and the report of the Intelligence and Security Committee (February 2013) http://isc.independent.gov.uk/committee-reports/special-reports

Duncan Campbell is a British freelance investigative journalist, author and television producer. Since 1975 he has specialised in the subjects of intelligence and security services, defence, policing, civil liberties and, latterly, computer forensics.

Chapter 1

The history of state surveillance

Duncan Campbell

The range and reach of surveillance legislation proposed or in place in the United Kingdom is far from novel in its roots or in its impact on the balance of power and rights between the subject and the state. The proposals in the Communications Data Bill (CDB), and the manner in which the new Bill has been introduced and managed, fall full square within long British historical precedents that position privacy rights as an irritant to be managed by a combination of concealment, secrecy, information management, and misinformation.

A possible signal difference in 2013, if history now turns out not to go the way the Home Office and its allies desire, is that the proponents of effectively unrestrained surveillance have become sufficiently arrogant and indifferent toward necessary partnerships as to have brought a rain of criticism on their head, including the condemnation from the normally mild Intelligence and Security Committee that "more thought" and "coherent communications" are essentials before any Bill is reintroduced.

The government's pitch to Parliament in the summer of 2012 to support CDB began with the spectacularly ignorant claim from posted-in ex SIS officer Charles Farr that "Communications Service Providers (CSPs) no longer retain for their own business purposes communications data as we know it". They do, even if they don't log everything new that he and his team want harvested.

The manner in which the new Bill has been introduced and managed, fall full square within long British historical precedents that position privacy rights as an irritant to be managed

THE HISTORY OF STATE SURVEILLANCE

Farr later elaborated on his misunderstanding, saying "30 years ago, BT may have kept data because they needed it in order to bill people correctly". This claim was inaccurate and historically impossible, as the electromechanical exchanges of the early 1980s could not and did not generate call data records – "communications data". What is now called "itemised billing" did not generally get created in UK exchanges until the 1990s, and was only required to be available to police and intelligence agencies after the passage of RIPA in 2000.

But despite the rise of well-informed and technically knowledgeable civil society advocacy groups and NGOs, society's understanding of the importance of protecting privacy rights seems to have fallen as quickly in the past quarter century as Moore's Law has driven up the power and threat of digital processing to place society under unchecked surveillance.

Who now can see any place for or value in the 500 year old (if now politically inept) saying "An Englishman's home is his castle"? Or the corresponding dictum in the landmark US writings of Justice Brandeis, 1890, that privacy is the "the right to be let alone."

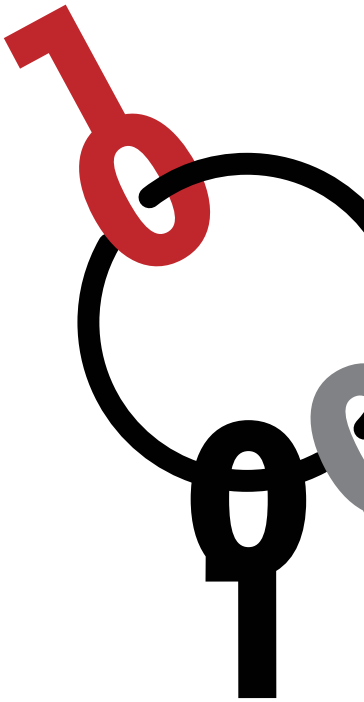
The presumption that the British state, acting clandestinely and using unwritten prerogative powers, was free to open mail, and in due course tap telephone calls and intercept and read e-mail, has been a constant from the time of the first Elizabethans up to the 1980s, when for the first time the conventions on human rights born from the defeat of Nazism started to impact UK state surveillance, through interventions by the European Court of Human Rights. It seems not entirely a historical accident that that Court is now under sustained attack.

Looking across Europe after more than 60 years, it seems apparent that the fundamental understanding of the importance of enforcing checks and balances, and of imposing regulation and supervision on state surveillance activity is better appreciated and respected in territories where Fascism was born or impacted the harshest than in the country which de facto brought the European Convention on Human Rights into being.

Thus, the German Grundrechte creates a stronger foundation now to enforce the values for which Britain and its allies fought, and which still drive some European resistance against ever increasing surveillance of the citizen, using digital technologies.

The same values are detectable in the language of the 1789 US Bill of Rights, and in particular the Fourth Amendment concerning unreasonable search and seizure. As recently as the 1970s, the Fourth Amendment seemed robust even as modern communications expanded, as when Congressional committees condemned US National Security Agency (NSA) surveillance of citizens' communications by the use of "watch list" mechanisms.

No such troubling debates affected the United Kingdom in 1975, the year the Church Committee reported to the US Congress. In the same year, in Britain, GCHQ and its costs and operations and surveillance power was entirely unknown to the public and parliament, even though then as now it was the largest and most intrusive of the intelligence agencies, attempting to intercept and sift all communications entering, leaving or passing through the UK, as well as from international sources.



The irony of secretly endorsing and creating structures akin to those used by historical and modern dictatorships seemed, then as now, to be undetectable in the vision of senior civil servants.

In the same year, in Britain unlike many other democratic states, telephone tapping and mail opening were outwith the law, conducted secretly (for tapping) by teams entering exchanges at dead of night and wiring up targets out of sight of normal staff.

In the same year, a national security ethos hardened by the cold war provided an easy tool for the state to discourage or suppress public information and discussion.

In the same year, unregulated police "local intelligence" collection on citizens, underpinned by secret recommendations to recruit an informer ("observer") on every street, outwith any direct needs for crime prevention and detection, were by then in form a century old.

The irony of secretly endorsing and creating structures akin to those used by historical and modern dictatorships seemed, then as now, to be undetectable in the vision of senior civil servants.

The first dawning perception in Britain that computer and digital technologies would impact and then determine relationships between the citizens and the state and other centres of power began in the late 1960s, but took no form until 1972, when the Royal Commission on Privacy set out 10 principles of data protection that later underpinned data protection statutes in Europe and the UK.

The Commission found that protecting individual privacy "was the social issue rated most important throughout the population." They also discovered that, among a wide range of potential threats to privacy outlined in surveys, none attracted more public concern, fear or hostility than the putative creation of a national databank.

The Commission found that protecting individual privacy "was the social issue rated most important throughout the population."

Intriguingly, 40 years later, the same important but dated phobia has informed the drafting of and debates on the CDB, and of debates on identity card legislation, largely because of the form in which Liberal Democrat policies and historical Conservative party opposition to New Labour's Identity Card proposals formed part of their 2009 election manifestos.

Because of this, absurd language has had to be used to explain that the output to the notorious "filter" at the centre of the CDB is anything but a national communications data database. Similar absurdities now compel the government to announce that each new attempt to introduce national ID numbers under another guise are not in fact, um, er, national ID numbers.

When in 1978 the Lindop Committee on Data Protection carried out an investigation of government computer databanks and surveillance systems then in place, they found, according to chair Sir Norman Lindop, that "the greatest threat, if threat there be, does not come from ... the entrepreneurial sector, it comes from the public sector."

They did not "fear that Orwell's 1984 was just around the comer ... But [they] did feel that some pretty frightening developments could come about quite quickly and without most people being aware of was happening".

His Committee's report highlighted a new computer system then recently installed by the former Special Branch of the Metropolitan Police, which was to deploy indexing and free text retrieval (FTR) of intelligence reports as raising "new dimensions of unease" because of FTR software's ability to associate people and any sort of information on them.

"The greatest threat, if threat there be, does not come from ... the entrepreneurial sector, it comes from the public sector."

THE HISTORY OF STATE SURVEILLANCE

The world has turned upside down. Whereas in the 1980s there was real public and political concern that the minor agency collecting TV licence fees had aggregated databases on households and addresses so as to target non-licence holders with implied accusations of evasion and criminality, by the noughties the claim to use central national databases as a threat was central to their advertising. The same tactic of encouraging fear of central national databases was then followed by HM Revenue and Customs.

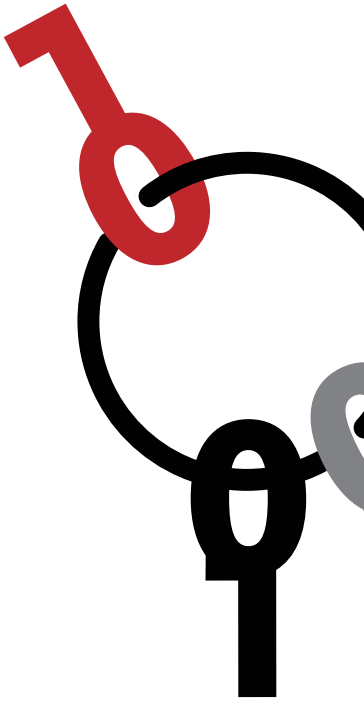
The national debate and understanding of surveillance now is undermined not only by the arrogance and disengagement from civil society concerns by surveillance advocates, but also by long term and mainly clandestine programs by interested parties to subvert public policy in advance of discussion and regulation, so as to prevent effective technical controls being introduced.

The most significant group doing this internationally is the so-called "Five Eyes" alliance of signals intelligence agencies of the main English speaking countries, including Britain's GCHQ and the US NSA. Their most important but not exclusive channels of intervention have been telecommunications standards bodies such as the ITU and the European Telecommunications Standards Institute (ETSI). ETSI, although nominally an independent, non-profit, standards organization for the telecommunications industry, has also been a vehicle for rewriting the technical specifications of new telecommunications systems as they come along, so as to make them "interception friendly".

In the darker and wholly secretive days of the 1970s and earlier, GCHQ and its allies built systems like the "ECHELON" Dictionary Network, intercepting and sifting all international satellite communication and using

free text search software years before Lindop sounded his warning. Using secrecy, they were ahead of the curve of public awareness and opinion – and still are – by intention and by design.

Thanks to the infiltration of surveillance agency interests into the ITU, ETSI and similar programmes, new mobile radio systems like GPRS, G3 and G4, and whatever may follow have come with surveillance systems built-in in advance, automatically available to be exploited by national governments and security agencies of every stripe. For parliamentarians and regulators here as elsewhere, the debate is often over before it begins. Caspar Bowden has highlighted how new US FISAAA legislation brought in 5 years ago requires cloud service providers to expose the private and commercial data they hold amounts to the latest and possibly most audacious step in this continuing campaign for access to private data.



In several senses, this is why the Communications Data Bill shows up an interesting new challenge in the UK, compared to the 1970s. No longer are telecommunications agencies single natural monopolies, either owned by or under the thumb of governments. While posing their own serious challenges to privacy, organisations like Skype, Google and Twitter, and the host of other enterprises using the power of the global common carrier that is the Internet, have no natural allegiance to the wide-ranging surveillance interests of the secret agencies.

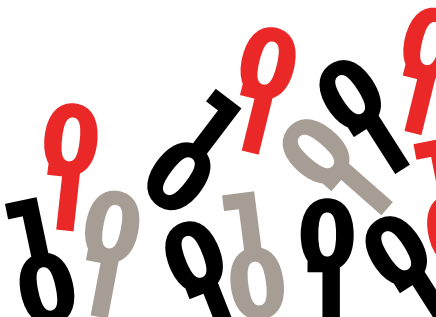
That is why the interchanges of the committees on the CDB in which these data multinationals set out their experiences with the Home Office have been so interesting. The companies say they will and do in general comply with due legal process, disclosing private data when asked for cause and with authority, compliant with applicable law, and perhaps checking

The Home Office response is the Communications Data Bill (CDB) – a long-laid plan to compel national Communications Service Providers to install Deep Packet Inspection extraction and aggregation centres

for proportionality and necessity. But they also told the committees that they refuse to open their customers up to all-purpose unchecked trawling, and that they require requests comply with their own local and international law.

The Home Office response is the CDB – a long-laid plan to compel national CSPs to install Deep Packet Inspection extraction and aggregation centres to defeat the adherence of the data corporation to due process, and to create a national communications data and interception database, in all but name.

Well-established legal restraints on unreasonable search and seizure, reframed as tests of proportionality and necessity, are historically rather new to the British state's attitude to surveillance. They are at the heart of the current debate on the CDB. The approach now taken will determine the form of the latest chapter in the history of British state surveillance.



For parliamentarians and regulators here as elsewhere, the debate is often over before it begins.

Angela Patrick is director of human rights policy at JUSTICE, an all-party law reform and human rights organisation. Angela is a qualified barrister, educated at Durham and Cambridge Universities. Before joining JUSTICE, from 2006 – 2011, she was assistant legal adviser to the UK Parliament's Joint Committee on Human Rights.

Chapter 2

Regulating surveillance, respecting private life[1]

Angela Patrick
Director of Human Rights Policy, JUSTICE

Surveillance is a necessary activity in the fight against serious crime. When targeted, it clearly plays a vital part in our national security. However, unnecessary and excessive surveillance destroys our privacy and blights our liberty. Technological changes have consistently created a tension between the law, surveillance and the protection of privacy. In 1970, JUSTICE first observed:

> *Privacy has been infringed as long as man has lived in society; in every community, there have always been eavesdroppers, gossips and peeping Toms. But until very recent times, the physical means of infringement available to those have been our natural senses, apparatus with which we are all familiar and against which we know instinctively how to protect ourselves. The arrival of advanced electronics, microcircuits, high-definition optics, infra-red film and the laser beam have changed all this.* [2]

The intervening decades and the advent of the Internet have changed our relationship with each other and with the technology we use to support our daily lives. This has also created a new impetus to harness this technology for the purposes of the prevention and detection of crime, creating new challenges to our expectations of privacy. [3] The legal framework in the UK has routinely struggled to keep pace.

Judicial scrutiny is the paramount means of protecting individual privacy in instances where the individual themselves may be unaware that their information is being handled

The common law famously stopped far short of an enforceable right to privacy. It has however long recognised the impact which living our lives observed may have upon our personal and social development.[4]

It is generally accepted that the greatest impetus for the structured regulation of surveillance within the United Kingdom has been the scrutiny of the European Court of Human Rights and the application of the right to respect for private and family life, home and correspondence, provided by Article 8 of the European Convention on Human Rights (ECHR), now transposed into domestic law by the Human Rights Act 1998 (HRA 1998). Article 8 (1) ECHR protects the right to respect of private and family life, home and correspondence. Article 8(2) provides that interferences with that right can only be justified when they serve a legitimate aim – such as protecting the rights of others or preventing and detecting crime – and the interference is necessary in a democratic society.

That each of the distinct acts of collection, retention and use of personal information is protected by our right to respect for private life, home and correspondence guaranteed by Article 8 ECHR is now a given.[5] However, the Convention also recognises that surveillance is a justifiable act of State in the interests of protecting the rights of the wider community. Balancing the competing public interest in personal privacy and the public interest served by acts of covert surveillance, in practice, involves answering a series of questions:

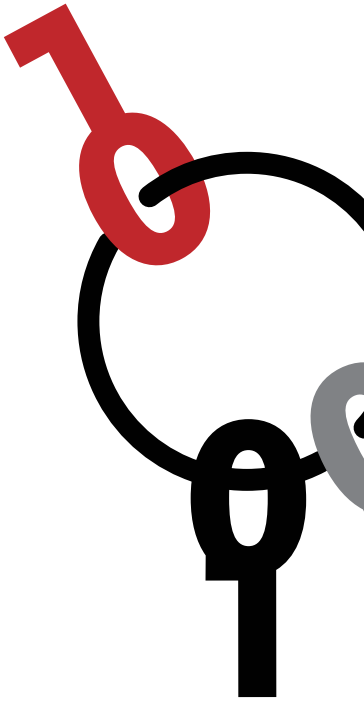
a. Is the law governing surveillance sufficiently clear and precise to allow individuals to understand when surveillance powers will be used? For example, when will personal data be retained, and in what circumstances may it be accessed by the State?

b. Do those statutory provisions – and their implementation – address a legitimate aim, addressing the prevention and detection of crime, or other significant public interest?

c. Has evidence been produced to show how surveillance benefits this aim, and to support the Government's case that the interference with individual privacy posed would be proportionate to those benefits?

d. Is surveillance the least restrictive means of achieving the aim and have alternatives been considered?

e. Are adequate and effective safeguards against abuse provided?



Surveillance generally occurs without the knowledge of the individual being watched. Only in the limited circumstances when the information is used in a trial or when an authority acknowledges the surveillance will an individual be able to challenge its propriety. In these circumstances, the European Convention on Human Rights places a significant obligation on the State to ensure that surveillance powers are closely drawn, safeguards appropriate and provision made for effective oversight:

> *[it is] unacceptable that the assurance of the enjoyment of a right … could be… removed by the simple fact that the person concerned is kept unaware of its violation.*[6]

The Court stressed that the justification of any surveillance measures places a significant burden on states to adopt the least intrusive measures possible:

> *[P]owers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions.*[7]

Interception of private communication (phone calls, emails, text messages, faxes, etc) or 'intercepts' are the most sensitive kind of surveillance.

Although the courts have stopped short of expressly requiring prior judicial authorisation of all surveillance operations, in many cases it has been considered essential. Judicial scrutiny is the paramount means of protecting individual privacy in instances where the individual themselves may be unaware that their information is being handled:

> *The rule of law implies, inter alia, that interference by the executive authorities with an individual's rights should be subject to effective supervision, which should normally be carried out by the judiciary, at least in the last resort, since judicial control affords the best guarantees of independence, impartiality and a proper procedure.*[8]

The primary focus of the European Court of Human Rights has been on the effectiveness of the law governing surveillance to avoid violations before they arise. Over the course of the 80s and 90s, the legislative framework in the UK was found seriously lacking, as we consistently failed to provide any adequate statutory basis for the use of covert powers of surveillance by our police and security agencies.[9]

Regulation of Investigatory Powers Act 2000 ("RIPA")

The Regulation of Investigatory Powers Act 2000, or 'RIPA' as it is commonly known, governs the use of covert surveillance by public bodies. This includes bugs, video surveillance and interceptions of private communications (e.g. phone calls and emails), and even undercover agents ('covert human intelligence sources'). It was introduced following a decision that the existing law on surveillance was insufficiently clear and incompatible with Article 8 ECHR.[10]

RIPA governs surveillance by the police and other law enforcement bodies (e.g. the Serious Fraud Office or the Serious Organised Crime Agency), the security and intelligence services (MI5, MI6 and GCHQ), as well as a large number of other public bodies, including local government.

In virtually every other common law country, interceptions and bugs by law enforcement require a judicial warrant.

As a general rule, RIPA governs active surveillance – actions interfering with individual privacy that would normally be illegal if carried out by a private individual, e.g. installing a listening device in someone's house, but that can be lawful when carried out for a legitimate governmental purpose, e.g. detecting crime. It does not extend to other privacy technologies such as databases or CCTV (except, for example, where the CCTV camera was installed in such a way as to monitor a private home). This kind of surveillance activity is governed by the Data Protection Act 1998, which affords individuals protection against the disproportionate and unnecessary use and processing of their personal data.[11]

RIPA distinguishes between interception of private communications and communications data (Part 1), and between directed surveillance and intrusive surveillance (Part 2).

'Directed' surveillance is surveillance that is conducted as part of a specific investigation and carried out 'in such a manner as is likely to result in the obtaining of private information about a person'.

'Intrusive' surveillance is directed surveillance that involves either residential premises, a private vehicle, or any kind of surveillance device. So, for example, following a suspect down a street as part of an operation would be directed surveillance. Planting a bug in someone's house, by contrast, would be intrusive surveillance.

Interception of private communication (phone calls, emails, text messages, faxes, etc) or 'intercepts' are the most sensitive kind of surveillance. With few exceptions, interceptions are authorised under warrant by the Home Secretary and anything obtained pursuant to a warrant – and the warrant itself – is completely inadmissible in any legal proceedings. This is because of the fears of MI5 and MI6 that using

Failing to address the criticism about complexity and ineffective administrative oversight, it would expand upon the pool of data available for the purposes of surveillance by creating a new statutory framework for the generation and retention of data.

intercept evidence would reveal too much about their interception capabilities. Interception without authorisation is a criminal offence.

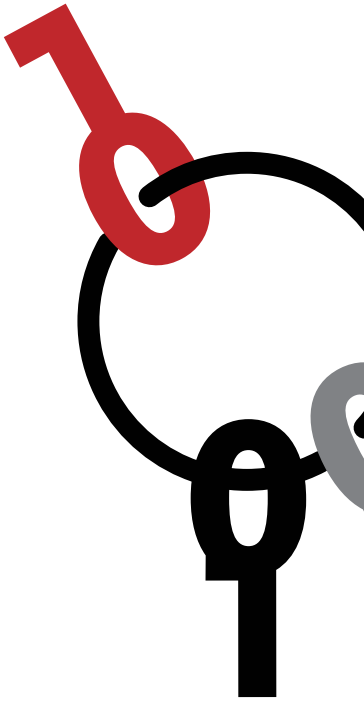
'Communications data' is different from intercepts in that it is information about a communication rather than its contents. For example, the record of your phone provider that you called a particular telephone number on a particular time and date is communications data. What was actually said as part of telephone call would normally be covered by an intercept.

RIPA is complex and the kind of authorisation required and level of oversight available depends very much on the kind of surveillance. Generally speaking, the least intrusive kinds of surveillance are largely self-authorised by a senior member of the public body concerned, with after-the-fact scrutiny by the relevant commissioner. More intrusive surveillance requires the involvement of the Surveillance Commissioner but there is no prior judicial authorisation required for intercepts – the most intrusive kind of surveillance. The application of the Act is not limited to police and security services, but extends to public authorities including local councils, HMRC and other statutory bodies serving public functions. However, the most intrusive types of surveillance are reserved for use by a more limited range of services who work on the prevention and detection of crime.

In virtually every other common law country, interceptions and bugs by law enforcement require a judicial warrant. This means that the police have to apply to a judge for permission before they can carry out surveillance. By contrast, an interception warrant under Part 1 of RIPA is granted by the Home Secretary.[12] The only requirement for judicial scrutiny under RIPA was introduced in 2012, when Parliament determined that local authorities exercising surveillance powers should first be authorised by a magistrate.[13]

In the digital age, it (communications data) may give a sophisticated picture of the type of device being used and may allow an individual's movements to be pinpointed across a series of mobile phone calls as they move across the country.

Part 4 of the Act provides for after-the-fact oversight by three different bodies: the Interception of Communications Commissioner, the Intelligence Services Commissioner and the Chief Surveillance Commissioners. Different activities are governed by different Commissioners. The Investigatory Powers Tribunal – a special Tribunal with extraordinary procedures which allow a complaint to be considered in secret and without confirming that an individual has been subject to surveillance – is established to hear complaints related to surveillance, including claims that an operation has violated individual rights under the HRA 1998.



RIPA was intended to provide a human rights compatible framework for the governance of surveillance in the modern age. Unfortunately, the Act has been subject to widespread criticism. One of our most senior judges has criticised the Act as "perplexing".[14] The Act has led to a decade of crises and public controversies. For example, at the heart of the phone-hacking scandal was a misunderstanding that intercepting a voicemail message was only a criminal offence if the recipient hadn't listened to it before the hacker did.[15]

Communications Data and the Draft Bill

The proposals in the Draft Communications Data Bill would adopt the existing RIPA oversight model and would build upon its framework for access to data. Failing to address the criticism about complexity and ineffective administrative oversight, it would expand upon the pool of data available for the purposes of surveillance by creating a new statutory framework for the generation and retention of data. The combination of this expanded model for retention and access may make the shortcomings in the RIPA model for oversight all the more glaring.

Communications data is defined by RIPA and includes subscriber data, traffic data and use data. Broadly, subscriber data is information held by a provider about a

It creates a statutory basis for the generation, collection and retention of data about us all, with a rolling picture of our communications to be retained by individual Communications Service Providers for one year.

user; traffic data outlines information such as the location of the communication and the people involved, and details of the equipment used; and use data relates to the use made of the relevant service (for example, what websites a user has visited etc).[16] For example, subscriber data as originally defined might capture account details and addresses or telephone numbers associated with an account. In the Internet age, it might extend to all of the information held by, for example, Facebook, on its users, including "likes", "dislikes", marital status, family relationships and employment history and photographs. Traffic data as defined might set out the location of two static telephones; in the digital age, it may give a sophisticated picture of the type of device being used and may allow an individual's movements to be pinpointed across a series of mobile phone calls as they move across the country. The definitions of communications data in RIPA would be adopted in the Draft Bill without amendment. The Parliamentary Joint Committee appointed to scrutinise the Draft Bill accepted that the definitions in RIPA are generally outdated.

Under RIPA "Requests" may be made for information that the provider already holds. Notices issued under RIPA may require a provider to acquire data it does not routinely keep on behalf of the requesting body. Notices and authorisations last one month unless renewed.[17] Service providers must comply with notices requiring access to communications data under RIPA, unless it is 'not reasonably practicable' to do so.[18] If necessary, the Secretary of State can seek an injunction for the enforcement of the notice.[19] Oversight is provided by the Interception of Communications Commissioner.[20] Since late 2005, public bodies able to make requests have been subject to an inspection regime carried out by an inspectorate under the direction of a Chief Inspector and the supervision of the Commissioner. Named public bodies can access different categories of data for different purposes, following internal administrative authorisation by a senior officer within their organisation. Local authorities may only access limited data following authorisation by a magistrate.

It is clear that the Government intends that this process will allow the process of obtaining data following authorisation to be significantly automated and controlled by a central system which is either digitally operated or operated by a staff team under contract to the Secretary of State

The Data Retention (EC Directive) Regulations 2009 (which implement the EU Data Retention Directive)[21] require certain public communications operators to retain information originally held for commercial purposes for up to 12 months.[22]

The overriding difference between the existing framework and the proposals in the Draft Bill is a shift away from the presumption that for limited purposes, the State may access data already retained or reasonably obtainable by service providers, when shown to be necessary and proportionate for the prevention or detection of crime and other reasons, which serve the public interest. Instead, it creates a statutory basis for the generation, collection and retention of data about us all, with a rolling picture of our communications to be retained by individual Communications Service Providers (CSPs) for one year.[23]

The Draft Bill envisages an entirely new regime for access to this expanded pool of data, albeit one which appears similar to the RIPA model of requests and notices served by public officials "authorised" to obtain data for specific purposes (Clause 10). However, the Bill also provides for the creation of a centralised "filter" mechanism (Clause 14). Even following pre-legislative scrutiny, it is extremely unclear how this filter will relate to the data which CSPs will be required to harvest and store. However, it is clear that the Government intends that this process will allow the process of obtaining data following authorisation to be significantly automated and controlled by a central system which is either digitally operated or operated by a staff team under contract to the Secretary of State (it has been suggested that the Metropolitan Police might tender for this role). Without further information about how the filter mechanism might operate – or indeed how it might relate to individual authorisations – it is incredibly difficult to consider whether it might be accompanied by adequate safeguards for the protection of privacy. However, the introduction of automation for the compilation of data across several different providers does suggest that the Government seeks to increase the

accessibility of data significantly. The Parliamentary Joint Committee appointed to scrutinise the Draft Bill described the process:

> *The Request Filter is a Government owned and operated data mining device which, to work efficiently, requires each CSP to maintain its own database of all its communications data in a common format. Each CSP database will be able to be accessed at any time by the Request Filter … The Request Filter can be equated to a federated database.*[24]

This combination of an expanded pool of data, in combination with easier access through automated processing raises a number of questions about the proportionality of these measures. The question is then whether each of these steps is justified and proportionate, and whether, taken together, they are necessary in a democratic society. Even if evidence can be produced to show that there is a legitimate need for change, without clear information on the operation of these measures, it is difficult to assess whether there will be adequate safeguards in place – including through effective oversight – to satisfy the requirements of Article 8 ECHR and to protect the right to respect for private life, home and correspondence.

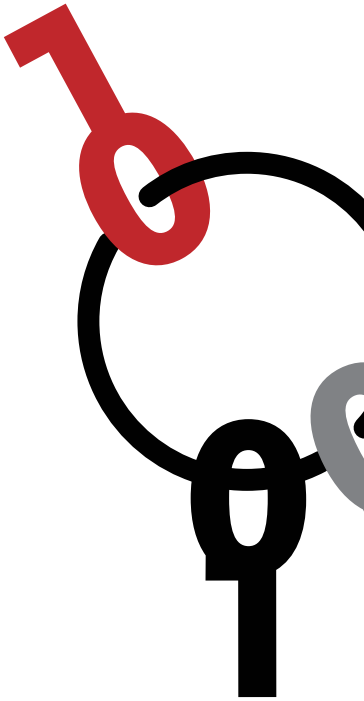
However, the compilation and the retention of data – as opposed to its use – has been subject to the increasing judicial scrutiny both at home and in Strasbourg.[25] For example, the routine retention of the DNA samples and profiles of innocent people – who had been arrested and released – as part of the National DNA Database has been ruled a disproportionate interference with the right to respect for private life. In that case, the European Court of Human Rights explained that measures which operate without regard to individual impact and characteristics must be accompanied by clear justification and appropriate safeguards.[26] More recently, the Court of Appeal ruled that the routine collection and retention by the

The arguments provided by the Government in support of the Bill have significantly underplayed the impact on individual privacy of data retention.

police of information about protesters not been suspected of any criminal offence could amount to a violation of the rights of those individuals to respect for private life in violation of Article 8 ECHR.[27]

The arguments provided by the Government in support of the Bill have significantly underplayed the impact on individual privacy of data retention. A failure to recognise the proper boundaries imposed by the Convention – and the HRA 1998 – will lead to a significant risk of litigation and subsequent legal challenge at home or abroad. Individuals will seek to have retained data deleted and may challenge a refusal to do so. The proper scope of the existing law on data retention – embodied in the EU Data Retention Directive – is currently being challenged in precisely this way across Europe. Digital Rights Ireland awaits a decision of European Court of Justice in Luxembourg on the legality of blanket retention under EU law.[28]

The UK is pushing the boundaries of international law on the retention of data for the purposes of the prevention and detection of crime. As learnt in the development of the DNA database; where arbitrary rules are imposed without proper justification, the law will push back.



Notes

1. This section provides a brief review of the history of the law on surveillance in the UK. For a fuller analysis of the development of the current law, see JUSTICE, Freedom from Suspicion: Surveillance Reform for a Digital Age, 2011.

2. JUSTICE, Privacy and the Law, 1970, para 110.

3. See for example, Malone v Commissioner of Police for the Metropolis [1979] 244 Ch 357 – 362.

4. See for example, the description in Blackstone's Commentaries on the Laws of England, Bk IV, Ch13: "Eaves-droppers, or such as listen under walls or windows, or the eaves of a house, to hearken after discourse…are indictable at the sessions".

5. In Malone v UK (1984) 7 EHRR 14, the Court considered the attachment of a 'meter check printer' to a telephone line for the purposes of recording the time calls were made, to whom and for how long. The Court considered that the collection of this information engaged the right to privacy, but in these circumstances could be justified by reference to the commercial need for a supplier of services to legitimately ensure a subscriber is charged correctly. This use was proportionate and justifiable. However, passing the information to the police without statutory authority and relevant safeguards against abuse was not. See, for example, paras 56 – 84. In Amann v Switzerland (2000) 30 EHRR 843, for example, the Court held that the storing of information about the applicant on a card in a file was found to be an interference with private life, even though it contained no sensitive information and had probably never been consulted. In Rotaru v Romania (2000) 8 BHRC 449, at para 43, the Court stresses that even 'public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities'.

6. (1978) 7 2 EHRR 214, paras 36, 41.

7. Ibid, para 42. See also Para 49: 'The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism adopt whatever means they deem appropriate'.

8. Rotaru v Romania (2000) 8 BHRC 43 at para 59.

9. Malone v UK (1984) 7 EHRR 14 prompted the introduction of the Interception of Communications Act 1985, the first statutory regulation of surveillance in the UK.

10. Halford v UK (1997) 24 EHRR 523

11. A fuller description of the law governing CCTV can be found in Freedom from Suspicion, from page 111. See also Protection of Freedoms Act 2012, Sections 29 – 36, which will introduce a new Code of Practice to govern the use of surveillance cameras and provide for the appointment of a new Surveillance Camera Commissioner. The scope of the Code and the proposed role of the new

Commissioner is outside the scope of this commentary.

12. RIPA, Section 5.

13. Protection of Freedoms Act 2012, Sections 37 – 38.

14. Attorney General's Reference No 5 of 2002 [2004] UKHL 40 at para 9 (Lord Bingham). See also para 29 (Lord Steyn).

15. Freedom from Suspicion, para 10.

16. Freedom from Suspicion, Chapter 4, provides fuller details on the existing rules governing interception of communications data. Sections 21 and 22 of RIPA govern the current framework.

17. RIPA, Section 23(4) and (7).

18. RIPA, Section 22(7).

19. RIPA, Section 22(8).

20. RIPA, Section 57(2)(b)). See further Freedom from Suspicion, Chapter 3 above.

21. Directive 2006/24 EC

22. SI 859/2009

23. Draft Communications Data Bill, Part 1.

24. Joint Committee on the Draft Communications Data Bill, First Report of Session 2012-13, Draft Communications Data Bill, HL Paper 79/HC 479, para 113.

25. Amann v Switzerland (2000) 30 EHRR 843

26. S & Marper v UK, (2009) 48 EHRR 50

27. John Catt v ACPO and the Commissioner of the Metropolitan Police [2013] EWCA Civ 192

28. Digital Rights Ireland v The Minister for Justice and Others, [2010] 2006/3785P. A fuller consideration of each of the challenges is provided by the European Commission in its report to the Council and the European Parliament on this issue: COM (2011) 225. http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf . There are additional questions raised over the compatibility of the operation of the Request Filter with EU law, in particular, whether the operation of the Filter will amount to "general monitoring" as prohibited by Article 15 of Directive 2000/31 EC (the E-Commerce Directive). These specific questions are outside the scope of this short introduction.

Dr Richard Clayton is a software developer by trade, but since 2000 he has been an academic at the University of Cambridge. He conducts research into email spam, fake bank "phishing" websites, and other Internet wickedness. He has assisted the APIG and APComms all-party groups of Parliamentarians in several inquiries into Internet issues, and has acted as a specialist adviser for Select Committees of both the Lords and Commons in various inquiries into Internet security topics. He is treasurer of FIPR (Foundation for Information Policy Research) and a member of the Open Rights Group (ORG) Advisory Council.

Chapter 3

Current and future surveillance technology

Richard Clayton

Surveillance technology is of two main types – equipment that keeps tabs on you in the physical world, and processes that track your activity "online" where computers keep a record of your communications and your financial activity.

The physical world is reasonably straightforward to understand. As is well known, very large numbers of CCTV cameras are installed in public and private spaces in the UK and a recording will be kept of what they see. The cameras may be fixed, or a remote operator may be able to choose where they point and how much they zoom in. The quality of the images captured varies very considerably – with older systems merely producing a blurry impression of what has occurred with little hope of identifying the people concerned. Newer systems can produce high quality material that will enable precise identification of individuals and may also capture audio to accompany the pictures.

Experimental systems process the recordings in real time, trying to match the images to mugshot galleries – with mixed results. The early trials, for example in Newham, were significantly overhyped – but face recognition technology continues to improve. Other systems attempt to identify individuals by their gait as they move from camera to camera, and others detect when people don't follow the usual routes through an underground station or a car park – perhaps because they are ill, or suicidal, or are contemplating a theft.

Many new phones are capable of learning their exact position using GPS and this information can be remotely accessed.

CURRENT AND FUTURE SURVEILLANCE TECHNOLOGY

The police ANPR (automatic number plate recognition) system records the index plates of vehicles passing an extensive system of cameras on major (and minor) roads. These systems permit immediate dispatch of interceptor vehicles when cars are stolen, or after-the-fact analysis to determine which vehicles were at a crime scene, where they came from and where they went to. More targeted deployments of cameras, linked to online databases, are used for random checks to determine if passing cars are insured and have a current vehicle excise license.

The examples so far have been mass surveillance systems – more directed surveillance traditionally involved police officers staking out a house and noting all the comings and goings. Nowadays, less labour-intensive surveillance may involve cameras and microphones being surreptitiously installed into light switches, or into a car, the location of which is continuously recorded by an attached GPS tracking device. The police are also getting interested in using drones for surveillance – mainly as a cheaper (and quieter) alternative to the police helicopter.

"Online" tracking can be equally revealing of people's actions and movements. The records created by an Oyster card user will show where they have travelled over the preceding couple of years; their bank and credit card records will show where they have been spending money and give an indication of what they have been buying. Companies like Tesco will, for those customers with loyalty cards, have complete records of their purchases and will be able to make educated guesses about their lifestyle, living arrangements, and some aspects of their medical history.

Mobile phones continuously interact with nearby cell towers so that incoming calls can be delivered. The phone companies are obliged to retain data about the location of a phone whenever a call is made or received, but if your phone is powered up then they have access to your location at all times and can provide this to law enforcement in real time if this is required. The location information can be

Proponents of this approach claim that by using Deep Packet Inspection equipment they can straightforwardly extract a summary listing of what is in someone's mailbox

extremely precise within cities, but in rural areas it may only give the most general of positions. However, many new phones are capable of learning their exact position using GPS and this information can be remotely accessed.

The records that telephone companies (both fixed line and mobile) keep can be rapidly interrogated to provide lists of calls made from any particular phone, or to any particular phone. These lists will also include the duration of the call and the physical location of the endpoints. Mobile handsets have a unique identifier called an IMEI; this is independent of the phone number which is set by the SIM card inserted into the phone. Call records can be identified either by the phone number or the IMEI device identifier – permitting the tracing of phone activity even when the SIM has been changed.

When interaction is by email instead of by phone then the authorities can still get lists of who is communicating with whom. The email provider is obliged (if they are within the European Union) to keep records of who email was sent to or from, along with timestamp information and exactly how large each email was. Once again, law enforcement regularly requests lists of this email metadata, which can be indexed by sender or receiver.

However, when the email provider is not within the jurisdiction then they may not be obliged to keep records of activity or they may not be prepared to hand over substantial amounts of detailed information to foreign law enforcement. One way of tackling this problem is for UK ISPs to wiretap all the Internet traffic going back and forth to the foreign website and then to reconstruct the email metadata for that site from the wiretap results.

Proponents of this approach claim that by using DPI (deep packet inspection) equipment they can straightforwardly extract a summary listing of what is in

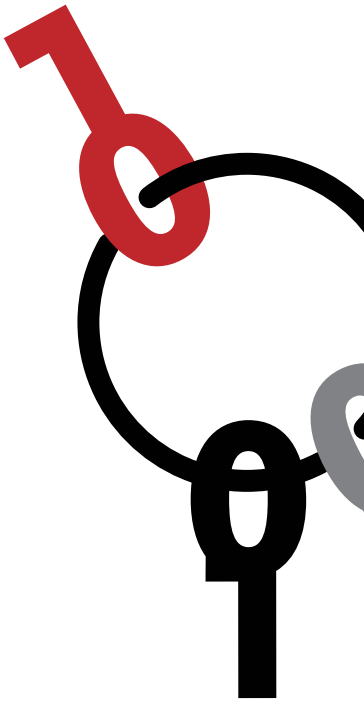
someone's mailbox – these are fixed format strings that are easy to locate on the page – whenever the user is looking at the relevant page. The content of the email would not be captured by this method – that would be "interception" and require special warrants – but the metadata created would be equivalent to what a UK-based provider is already required to keep.

It remains unclear how cost effective this DPI approach will be – as traffic levels increase, ever more DPI equipment would be needed. As a technique it is completely stymied by the use of web page encryption (which turns the traffic on the wire into incomprehensible blobs of data) and would doubtless be very fragile in that minor changes to the email website would require the data extraction code to be recast. The system could never be capable of handling more than a handful of foreign websites at any one time and operational security considerations make it unlikely that details about the currently targeted sites could be shared with the junior police officers who might to use the data for their investigations – i.e. it's hard to see how this sort of data could ever be used for anything outside the national security ambit.

There is, of course, all sorts of other surveillance-relevant information available on the Internet freely available that anyone can access. The police call this "open source" data and it includes Facebook pages, Twitter feeds, postings on public web forums and so forth. Should any of this information be of interest, then the police will generally wish to ascertain who has posted it. The owner of the relevant website will, upon receipt of a properly formed request, be able to supply the "IP address" of the poster. Police will also be told the IP addresses of computers used in hacking attacks and other bad events. The ability to determine which user's account was associated with a particular IP address at a particular time is called "traceability".

It is fundamentally inherent to this proposal that Filter data should be collected on everyone's activity and that this data should be made available en masse from the private companies, the Internet Services Providers and telephone companies that provide services, to government systems for the correlation processing.

Computers connected to the Internet are given a unique "IP address" and data packets are routed towards this IP address, so where there is direct two way communication it cannot be forged. The IP addresses are allocated to ISPs in contiguous blocks, so if it is necessary to determine "who did that?" then public records can be interrogated to determine which ISP was providing Internet service, and they can then consult their records to determine which customer was allocated the particular IP address at the relevant time. That information does not of course indicate whose fingers were on the keyboard, but it will clearly indicate where to look next, or whose door to break down.



This precise mapping of IP address to customer account is problematic for Internet access from smartphones – there are not enough spare IP addresses for every phone to get a unique allocation. Instead, phones share IP addresses in a very dynamic manner and although the mobile phone provider could record the detail of these allocations, at present they often fail to do so. Addressing this "traceability hole" is one of the key aims of current Home Office policies, although they've been rather coy about saying so, in the hope that criminals will not exploit the weakness.

So far, all of the surveillance and tracking systems have been considered in isolation, but this is about to change in a major way. One of the provisions of the draft Communications Data Bill is the creation of a data correlation system dubbed a "Filter". This system will combine enormous amounts of data from different systems, hoping to identify activity that would not have been apparent within a single system.

It is fundamentally inherent to this proposal that Filter data should be collected on everyone's activity and that this data should be made available en masse from the private companies, the ISPs and telephone companies that provide services, to government systems for the correlation processing. The data won't necessarily be physically combined on a single system (in fact it would be poor engineering to do

this) but it will be logically combined. The original collectors of the data will not have any knowledge of what it is being used for, or possibly even how much data is being processed, so there will be no opportunity for whistle-blowing should excesses occur.

The complexity and secrecy of the proposed "Filter" system will make it extremely challenging to ensure that misuse, or just simple "mission creep", does not occur.

This integrated processing promises to make it much harder for criminals to communicate over a diversity of systems and thereby avoid being tracked – records of phone calls, emails and tweets could be easily combined. But the system's capabilities go much further than that and the type of "big data" system envisaged will be capable of complex data mining tasks. To take a fictional example from Charlie Brooker's "National Anthem", the source of a YouTube upload could be identified by the uniqueness of its size and timing; or, closer to real life, the source of an embarrassing leak could be identified by cross-correlating records to pick out exactly who in Whitehall sent out an email whose reception by a journalist triggered an immediate call to the relevant newspaper editor.

The trade-off for these new insights into criminal activity is that more information must be automatically collected about everyone ("just in case"), it must be stored for long periods, measured in years, and it must be handed over to the government operated filter for processing with the inherent assumption that the processing will be necessary, proportionate and authorised. There is tremendous scope for misusing such a system; a police state would relish the opportunity of correlating data on everyone out on the streets for a demonstration, everyone gathering in groups behind closed doors – or just collating a list of everyone who passed on an email containing a subversive joke. The complexity and secrecy of the proposed "Filter" system will make it extremely challenging to ensure that misuse, or just simple "mission creep", does not occur.

The source of an embarrassing leak could be identified by cross-correlating records to pick out exactly who in Whitehall sent out an email whose reception by a journalist triggered an immediate call to the relevant newspaper editor.

Peter Sommer is currently a Visiting Professor at De Montfort University and a Visiting Reader at the Open University. Before that he was at the London School of Economics for 17 years, ending up as a Visiting Professor. His research interests and publications include cyber security, cyberwarfare and the reliability of digital evidence. His main income comes from acting as an expert witness, for both prosecution and defence interests in criminal cases and in civil proceedings.

Chapter 4

Why digital technology poses a problem for surveillance law

Peter Sommer

It is easy enough to get agreement on the general aims of surveillance law: intrusion should pass tests of necessity and proportionality and there must be a robust framework of oversight.

But laws require words of precise meaning and easy interpretation. Precision is needed by those who wish to undertake surveillance and those who authorise their requests. Third parties such as communications services providers, public authorities and financial services companies who are asked to co-operate, those who turn out to be innocent but have been subject to excess and seek redress, and the courts who may have to arbitrate, all have to be clear about what is permitted and what records should exist of decisions made. The legal words need to reflect the reality of how the technology works.

A number of factors conspire to inhibit sensible and balanced discussion of surveillance laws, some practical in terms of the knowledge needed, some from politics. And there are a few elements that present real challenges about the efficacy of laws passed to regulate surveillance.

One excuse for political inaction, some MPs say, is that surveillance is not a doorstep or constituency surgery issue like jobs, the economy or the closure of a local hospital. But even if the public are not interested in the twists and turns of surveillance legislation, they can have strong feelings in the face of abuse, as shown by concern about the use of Regulation of Investigatory Powers Act (RIPA) powers against fly-tipping and dog fouling, the deployment of undercover police officers

The legal words need to reflect the reality of how the technology works.

who had long-term sexual relationships with environmental activists, and the use of "dead children" identities.

Surveillance Policy in General

Surveillance is part of more general security policy. Some politicians will have you believe that there is only one aim: to keep people, institutions and the community safe. But there are two others: to protect the essential values of society (freedom of speech, open and fair judicial processes, right to dissent, privacy such that the state only intrudes when provably necessary), and to deliver value for money.

Surveillance law is about balancing competing objectives, not absolutes. But for lazy politicians it seems simpler to use the scare language of paedophilia, terrorism and "lives lost" than to make the nuanced arguments of managing risks. Easier, too, for opposition politicians to say an incumbent is weak and not doing "enough".

Changes in the Landscape

But there are particular problems in getting to grips with how far surveillance capabilities and technologies have changed – and the implications.

First we need to look at the changes, some of them a function of our increasing personal use of digital devices but others the result of the deployment of official and commercial information-gathering and storage facilities.

Over 80% of the UK population has access to the Internet from home and each UK household on average owns three Internet-enabled devices. RIPA currently allows the collection of a user's activities in terms of the "top level" of a website and data is retained for a year.

Surveillance law is about balancing competing objectives, not absolutes.

Costs of hard disk storage fall by 50% every 18 months – a 1000GB (1 TB) hard disk now costs about £55 – so that in a typical warrant execution on domestic premises the police can expect to find several PCs of various vintages, plus external data storage devices such as disks and USB memory sticks.

There are 130 mobile phone contracts per 100 of the population and 52% of mobile phone users have a smartphone which is in effect a powerful ultra-portable computers. Nearly all these devices contain substantive files, copies of emails sent and received and histories of such Internet activity as websites visited or research carried out by the owner. Police can obtain this information under PACE powers.

All mobile phones will contain some records of calls made and received and copies of SMSs made and received – Ofcom says 200 SMSs are sent per person per month. While the phone is switched on, it constantly re-registers its presence with the nearest mast; this archive of an individual's detailed movements is retained for 12 months. Cell site analysis is now one of the most powerful and widely used of investigative techniques and is available under RIPA and the EU Data Retention Directive.

At the same time the availability of Closed Circuit Television (CCTV), both publicly and privately owned, has expanded greatly, in terms of the quantity of cameras and their locations, as has the quality of images. The UK's National Policing Improvement Agency (NPIA) operates a national DNA database, which is one of the world's largest, with profiles on an estimated 5,570,284 individuals as of 31 March 2012. The NPIA also operates a national automatic number plate recognition system (ANPR), which by March 2011 was receiving 15 million sightings daily, with over 11 billion vehicle sightings stored. A national fingerprint database contained 8.3m individuals' prints in April 2010. Another newer method for tracking the movements, at least of people in London, is via the Oyster card.

What characterises many of these changes is "rapid incrementalism" – change that occurs bit-by-bit, just too slowly to easily register in the public imagination but nevertheless has profound impact

At the same time, commercial companies have built up their databanks – through customer relationship software and credit data. Some companies – Google, Facebook, twitter – base almost their entire business on acquiring and then monetising personal data.

What characterises many of these changes is "rapid incrementalism" – change that occurs bit-by-bit, just too slowly to easily register in the public imagination but which nevertheless has profound impact – rather as personal computing power and mobile telephony have become wholly embedded in many people's lives.

There have also been significant improvements in specific surveillance technologies, covered elsewhere in this publication.

Data Amalgamation or Link Analysis

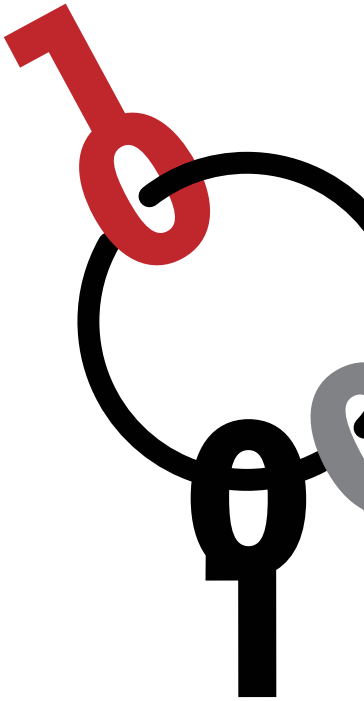
Some technologies are introduced on one agenda and then deployed against others: ANPR finds stolen, unlicensed and un-insured cars but also tracks all vehicular movements on major roads. Data is collected for one purpose and retained forever on a "you never know it may be useful" basis – DNA, finger prints and, once legally obtained from Communications Service Providers (CSPs), cell site and web log data. (The 12 month period is the time the CSP holds data pending a request from law enforcement). "Convenient" and "efficient" means by which CSPs pass information to law enforcement – the semi-automated provision of mobile phone call data records, for example, can have the effect of by-passing the impact of the application of the "necessity" and "proportionality" tests.

Yet other aspects only become obvious on very close scrutiny. Data amalgamation, sometimes called "link analysis", consists of linking different streams of evidence into chronologies of events, and assessing who knew who, and is a fundamental feature of investigations. But once all data is digital, software can combine and

There are particular problems in getting to grips with how far surveillance capabilities and technologies have changed – and the implications.

produce visualisations; the more data there is, the greater the granularity of the resulting analysis – and the greater the intrusion, far more than was ever envisaged when necessity and proportionality tests were applied to the original streams of evidence.

Many of the technological changes have had a drastic effect on the economics of surveillance. Traditional physical surveillance of a single important target may involve the cost of at least six operatives, more if the coverage is 24-hour. Live mobile phone movement coverage, aided perhaps by ANPR data and CCTV, can be handled by one operative sitting in an office. Seldom argued is the possible conclusion that the agencies may need less in the way of manpower.



Internationalism

Perhaps the greatest challenge both to policy makers and legislators is that globalisation and technology are taking matters far out of their control. The Internet is global and attempted restrictions on it inhibit innovation, trade and the exchange of ideas. Global information facilities companies like Google, Amazon and Microsoft offer search, communications, storage and processing services of immense social and economic value. Such companies are multi-jurisdictional as are the technical resources they offer, which are located in many different places; at any one time it may be unclear where a specific item of data is being held. Many of these companies have collected vast amounts of personal data about their customers, much of it of great potential value to police and spook investigators.

Most of the services are encrypted – mainly to protect customers from criminals but with the effect of denying surveillance agencies easy access. Ultimately there are often legal routes to access, but these are far slower than the speed at which criminals and terrorists move. It is a highly awkward realisation for nation states

and their legislatures to understand that their powers and capabilities have weakened, and that they need to form new types of co-operative relationship with these global Internet entities.

Legislators need knowledge of the technical capabilities of surveillance technologies.

Practical Problems

The practical problems are, alas, extensive.

- It is much easier to make incremental legal patches than fundamental changes: bigger bills require scarce larger legislative "slots" for time on the floor of Parliament and in committee. It is also easier for promoters to claim that a proposed change is almost negligible – "maintaining capability".

- Legislators need knowledge of existing law. But surveillance law is spread over many statutes and often depends on frequently changing codes of practice. Authorisers of intrusion are variously judges, senior law enforcement officers and a Secretary of State. There is a least one substantial oddity: interception of data in transmission is currently inadmissible, though all other forms of data acquisition are not.

Police and the security services follow the same course as all lobbyists: exaggerate and demand more than they need.

- Legislators need knowledge of how investigations take place, the techniques and resources used and where the costs occur. Most will probably not know unless they worked in law enforcement or as criminal lawyers.

- Legislators need knowledge of the technical capabilities of surveillance technologies. That has to include technologies currently deployed under existing law, as well as what the near future is likely to deliver. Law enforcers will say they are reluctant to provide detail in public for fear of alerting their targets.

- A similar need for secrecy is invoked when there are public demands for detailed breakdowns of costs, including claiming commercial confidentiality for vendors. When looking at estimates it is useful to consider other areas of related government expenditure: the annual cost of running the Serious Organised Crime Agency is £460m, and for the new Tier One UK Threat, CyberSecurity, the real new money being spent

is £650m over 4 years, of which £65m covers Home Office activities, with £28m allocated specifically to law enforcement. Apparently the Government has already spent £405m on the Communications Capability Development Programme even before its related enabling Bill has passed through Parliament.

- Legislators need to understand the nature and extent of the threats surveillance laws are meant to mitigate. In the last 12 months there has been an overall drop of 8% in recorded crime in England and Wales; only personal and retail thefts show an increase. ONS says there has been a 41% drop in recorded crime between 2002 and 2011, and a 26% drop using the British Crime Survey methodology. If we take the last time anyone died from terrorism, 2005, when "7/7" occurred with 52 victims, in that particular year you were over 61 times more likely to die in a road crash and 72 times more likely to incur a fatality in the home than to be killed in a terrorist atrocity. There has been approximately one serious terrorist attempt per year since then, all so far caught in time because once a plan moves towards action, the processes of sourcing material, establishing a bomb factory and recruiting personnel all create risks of detection for the actors.

Police and Security Service Pressures

Finally, there's the position of the major actors. Law enforcement and security agencies are expected to deliver public safety and successful prosecutions against budgets for resources and powers, which they will regard as inadequate. If politicians use the language of absolutes as opposed to managing risk, police and the security services do likewise. In any event, it is only reasonable that they should argue for "operational convenience" and lower levels of "bureaucracy". Police and the security services follow the same course as all lobbyists: exaggerate and demand more than they need. And there is a particular advantage in doing so. In the wake of a large disaster that they have been unable to prevent, they are able to point to an audit trail of requests for powers and resources denied.
And politicians know this.

Chapter 5

Alternatives to the current approach

Data preservation instead of data retention

Caspar Bowden

Caspar Bowden is an independent advocate for information privacy rights. He was an expert adviser to Opposition parties in the House of Lords for five bills, and author of the first paper on communications data retention and the most comprehensive online resource on RIPA. From 2002-2011 he was Chief Privacy Adviser to Microsoft in 40 countries, and from 1998-2002 was Director of the Foundation for Information Policy Research (www.fipr.org).

Ubiquitous personal communication technologies are here to stay. Because of exponentially falling data storage costs, two contrasting states of society can be envisaged. The default will be either that individuals determine whether and when their history is recorded, subject to exceptions, or data will exist about everyone all the time. This is the policy choice between data retention and preservation, and it is a sharp dichotomy.

Over two decades the UK has been in the vanguard of a core group of five European countries seeking systematic Internet surveillance. A blanket retention regime gives law-enforcement an "Internet Tardis" to go back in time and find out retrospectively what anyone was thinking about, whom they were talking to, and where they were. The dichotomy between retention and preservation is really about whether we want to give government such a "time machine" to scrutinize everyone's past behaviour without prior reason.

In contrast, targeted data preservation would likely mean that data is recorded only about 1% of individuals for whom there is some prior lawful justification. William Binney, who used to design such systems for the US National Security Agency (and has now become a whistleblower) and other independent technical experts agree this is sufficient to fight crime and terrorism effectively, when used intelligently.

The dichotomy between retention and preservation is really about whether we want to give government such a "time machine" to scrutinize everyone's past behaviour without prior reason.

However, security bureaucracies oppose preservation because they would be obliged to select targets, and they fear having to account for those decisions retrospectively.

The UK passed the first Internet retention laws with ATCSA 2001, and used its EU Presidency to enact the Data Retention Directive. The Communications Data Bill will set in stone the doctrine that all metadata in current and future services may be retained. Location data has special privacy risks. It can easily be correlated with other data. For example, Internet and mobile usage patterns reveal sensitive data, such as one's political and intimate life.

The Home Office has the Olympic chutzpah to call the apparatus for data-mining all this information a "Filter", and to justify it in the name of human rights. It says that by connecting up a virtual database (to hunt for arbitrary patterns of suspicion in all the data), they won't have to build a new central database. But the point is the untrammelled power to hunt through every private life with the tools of military intelligence.

This is a fork in the road, and these are the reasons why this Bill is the most dangerous long-term threat to a free society ever proposed by a democratic government, and should be rejected in its entirety. It ought to be obvious that continuously recording the pattern of interactions of every online social relationship, and analyzing them with the "Filter", is simply tyrannical.

The following elements are a basis for discussion for an alternative policy for preservation which respects human rights and provide proportionate and effective means for law-enforcement:

- Quick-response preservation on persons who have been identified as facing a real and immediate serious threat, and designated vulnerable groups.

- Convicts of specified crimes released on license must register their means of electronic communication for data preservation during a prescribed period.
- Case-by-case judicial authorization for preservation, targeted at those reasonably believed to be engaged in criminal activities (with emergency procedures). Similar reforms should be made for prior judicial approval of interception warrants. Targets should be notified afterwards of preservation and/or interception where suspicions prove unfounded (unless there are compelling reasons not to do so).
- A centre for analysis of preserved data, intended to investigate links between criminal groups, and generate new targets for preservation (subject to judicial authorization)
- Replace the current three Commissioners with a unified Surveillance Commission, reporting to Parliament, with multi-skilled investigators including human rights and computer experts, credibly able to detect and deter abuse, corruption, and insider attacks.
- A fixed ceiling on the number of interception warrants, and a larger ceiling for targets of communications data preservation, which could only be altered by Parliament.

It ought to be obvious that continuously recording the pattern of interactions of every online social relationship, and analyzing them with the "Filter", is simply tyrannical.

State surveillance: user notification and transparency

Simone Halink

Simone Halink is a legal expert at Bits of Freedom, the Dutch digital rights organization, focusing on privacy and communications freedom in the digital age. She studied law in Amsterdam and New York and worked as an attorney for a commercial Dutch law firm.

Introduction

States are regularly failing to ensure that laws and regulations related to communications surveillance adhere to international human rights and thus to adequately protect communications privacy. International experts, including the Dutch digital rights organisation Bits of Freedom, have therefore drafted international principles that provide a framework to evaluate whether current or proposed communications surveillance laws and practices are consistent with human rights.[1]

When applied to the Draft Communications Data Bill (CDB), the principles show that the bill is inconsistent with different aspects of human rights law as explained in chapter 2 of this publication. This contribution will focus on whether the CDB sufficiently enables individuals to fully understand the scope and application of communications surveillance laws, as embodied in the principles on 'user notification' and 'transparency'.

Transparency

The principle on 'transparency' requires States to be transparent about the use and scope of communications surveillance powers. This means that States must provide individuals with sufficient information to enable them to fully comprehend the scope, nature and application of the laws permitting communications surveillance. This principle also requires States to publish, at a minimum, aggregate information on the number of surveillance requests approved and rejected, and a disaggregation of the requests by service provider and by investigation and purpose.

The CDB falls short on both counts.

First, the use and scope of the CDB is unclear. The bill contains a very comprehensive power allowing the Secretary of State to make an Order requiring the communications operators to generate and retain communications data. The detail on what data is covered will be contained in notices beneath the legislation. This detail is currently kept secret to the general public. The fact that the government has given a very broad indication of the categories that will be covered by the CDB[2], does not solve this problem; it is insufficient to grasp the full meaning of the law.

When applied to the Draft Communications Data Bill, the principles show that the bill is inconsistent with different aspects of human rights law.

Additionally, the UK government does not provide sufficient information on surveillance requests by law enforcement in general. Although the report of the UK Interception of Communications Commissioner contains some aggregate data, it does not provide sufficient data to evaluate the types of requests, the extent of each access request, the purpose of the requests, and the scrutiny applied to them.[3] These flaws also extend to requests for communications data under the CDB.

User notification

The principle on 'user notification' requires individuals to be notified by default of a decision authorising the request for their communications data by law enforcement. Such notification must leave enough time and information to enable them to appeal the decision. A delay in notification should only be justified in exceptional circumstances.

The CDB is not consistent with this principle as a provision on user notification is absent.

The UK helped draft and sought to comply with different human rights instruments for over half a century.

The UK helped draft and sought to comply with different human rights instruments for over half a century. It can thus not afford to adopt legislation that is inconsistent with these laws. The UK government must therefore, amongst others, correct the above mentioned flaws.

Notes

1. The principles are currently being finalised and will be published shortly. An earlier draft of the principles is available at http://www.necessaryandproportionate.net/

2. IP address subscriber details, data identifying which Internet services or websites are being accessed, and data from overseas communications operators.

3. See: http://www.intelligencecommissioners.com/sections.asp?sectionID=2&type=top

Technology fuels surveillance harms

Dr. Joss Wright

Dr. Joss Wright is a Research Fellow at the Oxford Internet Institute, University of Oxford, where his research focuses on the themes of privacy enhancing technologies and online censorship, both in the design and analysis of techniques and in their broader societal implications. He obtained his PhD in Computer Science from the University of York in 2008, where his work focused on the design and analysis of anonymous communication systems.

Where laws intersect with technology, as is strikingly the case with surveillance, the discrepancy between the pace of technological change and the pace of legal change requires lawmakers to consider carefully the risks that arise from the future development and application of technologies. Crucially, and challengingly, it is necessary to differentiate between the limitations that exist in current technologies, and will disappear as technology develops; and those limitations that are fixed and inherent.

Information technologies, and in particular the Internet, have expanded the potential for surveillance to a degree that would have seemed fantastical in previous decades. Unprecedented levels of data can now be collected, stored, and analysed, and can be combined and controlled with an amazing degree of centrality.

The technical capabilities of the Internet not only allow this surveillance, they encourage us, through convenience, to place more and more of our lives into the spotlight. We now read news, search for information, talk to friends, organize social and business life, bank, and meet potential partners via the Internet. There is no precedent that can even approximate a model for the pervasiveness of the Internet in our lives -- not the phone network, not post or telegraph, not CCTV surveillance. Equating the Internet with historical technologies when making policy is not simply wrong, it is dangerously misleading.

From the state's perspective, the desire for surveillance is easy to understand. Such a wealth of data seems to promise an oracle allowing security services not only to investigate, but also to detect, predict and prevent crimes -- and ubiquitous surveillance can, certainly, achieve some of these goals.

The sheer wealth of data that surveillance reveals, however, tips the balance decisively from its power to help towards its power to

harm. Vast amounts of information can be handled by faster and faster computers, but the power and accuracy of the predictive algorithms are not so scalable -- when applied blindly to entire populations the ability to identify suspicious patterns is lost in the flood and becomes either worthless or actively harmful.

Pervasive and detailed information on individuals is a powerful tool. When investigating a crime the details of a suspect's activities, communications, and habits can be highly valuable. This tool, however, can be used just as effectively against all those individuals who are not under suspicion -- blackmail, fraud, stalking, and simple invasion of privacy are all enabled by such collections of data just as effectively as the investigation of crime. Placing an entire population in handcuffs to ensure that the criminals have been caught is not an acceptable policy.

As such, any legal framework for enabling surveillance must, in the first instance, be based on the notion of targeted gathering of data on well-justified grounds. This precludes the a priori gathering and storage of data -- such gathering should only occur in response to justified suspicions. Data that is found not to be useful, particularly where it concerns third parties, must be deleted quickly and verifiably. Further, there should be no institutionalised technical mechanism to surveil communications; instead, surveillance requests should be made directly to service providers who must be free to manage and control their own platforms.

As has been observed with existing laws, such as the UK's own RIPA, surveillance powers are easily and widely abused. Strict and independent audit, therefore, both of surveillance requests and data handling should be a key feature of any proposed surveillance framework. This must, of course, be supported by stringent penalties for misuse of either powers or data. Transparency, imposed both at a legal level and by the need to interact with private organisations that control infrastructure, is the only hope to mitigate the abuses that inevitably accompany such approaches.

The technological landscape in which we find ourselves is one in which the potential for surveillance is vast and growing. Surveillance law must therefore focus on restraining risks and abuses, without being carried away by false promises of effectiveness. Minimisation, decentralisation, accountability and limitation of access are all necessary steps to ensure that the cure is not worse than the disease.

Equating the Internet with historical technologies when making policy is not simply wrong, it is dangerously misleading.

Placing an entire population in handcuffs to ensure that the criminals have been caught is not an acceptable policy.

Freedom offline, surveillance online
– an unsustainable conflict

Nick Pickles

Nick Pickles is the director of privacy campaign group Big Brother Watch, an organisation set up to challenge policies that threaten our privacy and civil liberties, and to expose the true scale of the surveillance state.

The Internet has undoubtedly changed life beyond recognition in a relatively tiny fraction of time. Few areas of our lives are untouched by cyberspace and the impact on law enforcement is clearly one area that cannot be ignored.

The danger is that this pace of change, coupled with massive increases in computing power, sees the scale of surveillance increase far beyond what we would recognise as a civil balance between privacy and security. Worse, it leads to a policy response driven by a desire to do something quickly, rather than to manage the long- term consequences of legislation.

For many governmental organisations, the approach to surveillance and investigation offline is being replaced by a belief that more data is implicitly a good thing. Once data has been captured, the temptation – indeed, pressure – going forward will be to maximise the use of the information through increasingly invasive data mining.

However, a more fundamental shift is also taking place – that of governments seeking to use private commercial operations to gather data solely for use by agents of the state.

These issues are at the heart of the Communications Data Bill and pose a fundamental challenge to the future of a digital society, departing from the values that have underpinned democracy for centuries.

While technology may be changing, it should not justify moving further away from the basic principles of a democratic society as a

result. We would not ask newsagents to record what newspapers and magazines people buy, nor landlords to record who spoke to who in their premises. Surveillance without suspicion was, and remains, an affront to our right to live our lives in private.

Given the importance of encryption and private networks to ensuring data protection and information security, the tension between legitimate and necessary measures to protect the privacy of communications and the desire of law enforcement could become a hugely damaging spiral.

If the only barrier is the amount of computing power at your disposal, clearly Governments have the potential to use these tools to profile and analyse their populations in ways never before possible. If the promised improvements in security and reduction in crime are not delivered, as has been the case with every law enforcement innovation since the establishment of the police, the likely response will not be a different approach, but an acceleration of intrusion and ever broader types of data being collected.

This is the challenge we face as we seek to build a digital society. If Big Brother Watch's research has demonstrated anything, it's that surveillance is a rising tide. Once capability is installed, it is almost unprecedented for it to be removed. This is a key concern in the current debate, namely that once data is collected, changing the purposes for which it can be accessed and the ways it can be used is legislative tinkering, unlikely to attract substantive scrutiny.

John Stuart Mill wrote in On Liberty that "The strongest of all arguments against the interference of the public with purely personal conduct, is that when it does interfere, the odds are that it interferes wrongly, and in the wrong place."

This lesson remains true today, along with those values that built the modern democracies we seek to offer to the world as a beacon of hope for the oppressed and the imprisoned. Future generations demand of us that if we are to grant the state new powers, we bear responsibility of how they are used by those regimes that have not yet assumed power.

While technology may be changing, it should not justify moving further away from the basic principles of a democratic society as a result.

John Stuart Mill wrote that 'The strongest of all arguments against the interference of the public with purely personal conduct, is that when it does interfere, the odds are that it interferes wrongly, and in the wrong place.' This lesson remains true today.

Citizens not suspects: surveillance in a digital age

Rachel Robinson

Rachel Robinson is a Policy Officer at Liberty (the National Council for Civil Liberties). As a member of the policy team she is responsible for the organisation's parliamentary lobbying and policy development. Prior to joining Liberty Rachel worked as a Legal Officer for the charity Refugee and Migrant Justice and practised at the employed bar in the field of asylum and human rights law.

The moment that human beings form relationships, families and other associations, let alone complex digital societies, new tests emerge for the protection of personal privacy.

The technological advances of recent decades have magnified the challenge. An online message or entry to a search engine may be no less private and sensitive than a hushed conversation or a private letter was to an earlier generation.

Whilst we can accept that, without some proportionate and lawful intrusion, other vital concerns such as public safety would be impossible to pursue, we must not forget that a society which does not pay sufficient regard to personal privacy – and its meaning in digital age – is one where dignity, intimacy and trust are fatally undermined.

The holding of mass information through large-scale databases is one of the most significant societal changes with privacy implications in recent decades. Liberty has never opposed targeted surveillance but proposals such as the now discredited ID card scheme and current plans to introduce blanket collection and retention of communications data amount to nothing less than monitoring of the population at large, turning a nation of citizens into a nation of suspects.

Technological innovation is a double edged sword. The Internet has brought huge gains for free speech and association and has been a democratising force in repressive societies. By the same token it has also brought with it new ways of committing crime. But, often overlooked, are the huge gains for law enforcement

yielded by greater online communication. Increased access to records of communications between individuals is, in itself, a recent boon for police. Not too long ago, before the wide availability of mobile phones and email, most communications between individuals, if not carried out through traditional telephony or letter writing, would have been conducted face to face. This would have presented different – potentially more challenging – obstacles for crime prevention and detection. The fact that, in recent times, the State has benefitted from access to communications data already recorded and retained by communications providers, should not lead inexorably to the conclusion that total access to data should be required.

For good reason other – supposedly more intrusive – surveillance techniques available under the Regulation of Investigatory Powers Act, such as bugging (whether in private or in public), the use of human covert surveillance or the interception of communications need prior authorisation on the basis of individual suspicion. Once authorised they can only be carried out in the future. The Government is not presently arguing that we should all be routinely or randomly subject to bugging, covert tracking or interception 'just in case' but, if the present proposals for the collection of communications data become law, proposals for other types of blanket or random surveillance irrespective of suspicion "just in case" are a logical next step.

A proportionate surveillance regime for the future must recognise that technical capability is not the same as ethical imperative. In this country, the State has been all too willing to apply intrusive surveillance measures to the population at large. There is clearly unexplored potential for better use of targeted surveillance and the evidence gleaned as part of suspicion-led criminal investigations. A recent report published by the Joint Committee on the Draft Communications Data Bill made clear that law enforcement agencies are not making full use of the data already available to them.[1] Furthermore, for many years Liberty has been calling for the ban on the use of intercept evidence in courts to be lifted – a move which would allow for the effective prosecution of many more serious offences. Whilst blanket surveillance will inevitably bring some law enforcement gains, monitoring of an entire population smacks of authoritarianism, and will undermine the proud reputation for liberty we have developed as the oldest unbroken democracy in the world.

We must not forget that a society which does not pay sufficient regard to personal privacy – and its meaning in digital age – is one where dignity, intimacy and trust are fatally undermined.

If the present proposals for the collection of communications data become law, proposals for other types of blanket or random surveillance irrespective of suspicion "just in case" are a logical next step.

1. Joint Committee on the Draft Communications Data Bill, Report Session 2012-13, para 45. Available at: http://www.publications.parliament.uk/pa/jt201213/jtselect/jtdraftcomuni/79/79.pdf.

Peter Sommer is currently a Visiting Professor at De Montfort University and a Visiting Reader at the Open University. Before that he was for 17 years at the London School of Economics, ending up as a Visiting Professor. His research interests and publications include cyber security, cyberwarfare and the reliability of digital evidence. His main income comes from acting as an expert witness, for both prosecution and defence interests in criminal cases and in civil proceedings.

The future of surveillance laws

Peter Sommer

Surveillance laws are not about absolutes, but finding a balance between protecting individuals, organisations, the community and the state; limiting intrusions into people's lives to what is necessary and proportionate to the circumstances; cost; and an understanding of the range of threats.

In the end the only proper place for determining where that balance should be struck is Parliament, as the vehicle for democracy. Policing, and for that matter the activities of the security and intelligence agencies, in a country like the United Kingdom operate on the basis of consent. Without that consent law enforcement becomes much more difficult, expensive and potentially oppressive.

Elsewhere this publication shows just how far the landscape of surveillance technology has changed, and with it that balance. But there has been no recent rounded public discussion; the Communications Data Bill was presented as a minor technical amendment to existing law to "maintain capability". One has to go back to the early 1980s and the reviews leading to the Police and Criminal Evidence Act, 1984, designed to overcome obvious defects in the previous "judges rules" and to 2000 for the Regulation of Investigatory Powers Act which deals with electronic and human surveillance.

Commissions, Royal or otherwise, can sometimes seem a convenient political delay tool but, given the vast changes in surveillance technology and types of threat, surely some form of considered review would greatly enhance public debate – and lead to a complete overhaul of surveillance legislation written in language which reflects current technological realities?

As well as fact and evidence gathering, here are some obvious items for its agenda:

- Should we base electronic surveillance law on whether something is "communications data" or "content", always supposing we think that a distinction can be made? Would it be better to use levels of intrusion measured against suspected activity? This is the approach taken elsewhere in RIPA with "directed" and "intrusive" surveillance for physical watching of individuals. Can we also include laws about direct computer intrusion and undercover work?

- Material acquired by interception of data in transmission continues to be inadmissible and can only be used for intelligence purposes. It is a bizarre English law anomaly, is there any basis for its continuance?

- Is it right that surveillance authorisations are variously made by senior law enforcement officers and politicians as opposed to judges? What impact does this have when seeking assistance from overseas entities, as is becoming increasingly significant? Can we convert the assessment features of the current SPOC regime so that it directly assists a judge rather than being a law enforcement function?

- Do we really need to retain data about the electronic activities of the whole population against the possibility that a small fraction may be of future use in an investigation? Can we devise an order against targeted individuals whose data would be retained but only subsequently released when there was a proven need? But we would need to identify criteria for targeting these people in the first place.

- Strong plausible oversight is essential to giving public confidence to any surveillance regime. How do we move from the current sample auditing of requests for access to single streams of evidence to a position where a Commissioner tests for necessity and proportionality the entire process, including the linking and combining into databases of multiple streams of evidence? And should not the Commissioner have the power and resources to carry out no-notice inspections?

And the Commission, needs some permanence, as the surveillance landscape will continue to shift.

The only proper place for determining where that balance should be struck is Parliament, as the vehicle for democracy.

Do we really need to retain data about the electronic activities of the whole population against the possibility that a small fraction may be of future use in an investigation?

Communications data: getting there from here

Sam Smith

Sam Smith's work focuses on using the Internet for civic good, and he has been advising Privacy International since January 2012. He has worked on a range of human rights technology projects, building search engines about violence in Chechnya, wrangling data about political violence in Zimbabwe, and making research about modern slavery more accessible. He previously spent a decade working on research infrastructure in academia, and worked/volunteers with mySociety and the Nominet Trust, among others, around various policy interventions.

Photo: PaulClarke.com CC-BY Paul Clarke

In October 2012 a group of international civil society organisations and others spent several days devising principles to guide communications data surveillance and law enforcement access to communications data. This discussion about matching human rights protections with communications surveillance demands has involved experts from across the world. The current draft principles can be found at http://www.NecessaryAndProportionate.net.

Those principles set out that "activities that infringe on the right to privacy, including the surveillance of personal communications by public authorities, can only be justified where they are necessary for a legitimate aim, strictly proportionate, and prescribed by law"[1].

Throughout the Communications Data Bill process, the Home Office has appeared incapable of engaging with this sort of outside expertise or debate. As the Joint Committee stated, "industry, technical experts, lawyers and civil liberties groups could all provide valuable input…but they were not given the chance to do so".

The Home Office's blinkers exclude perspectives that may help create a better, more technologically astute and

proportionate approach to defining and fixing the problem of digital surveillance, and ignore the fact that law enforcement has access to far more detail on individuals than ever before. A suspect arrested today will likely be carrying significant detail on their movements and activities – evidence law enforcement would be able to use if they had the training to know that it was there.

The Filter

The 'filtering' provisions in the draft Communications Data Bill allow law enforcement authorities to search data held by multiple telecommunications companies from a single interface. This allows matching and the chaining of queries, which may go as far as allowing authorities to be able to ask multiple questions to correlate devices from several persons.

Development of the filter for data mining and complex queries will be designed and implemented without public consultation.

A very specific query may return detailed information about countless individuals, even if they had no direct connection to a topic of inquiry. This may occur, for example, when an image embedded from a different website is loaded.

The Home Office claim that only the data matched will be shown to the law enforcement officer doing their search. However, this is little protection in practice. While the filter may make existing queries slightly safer, the expansion of future queries, those as yet unconceived, is unlikely to be considered openly. We welcome the Home Office's embrace of agile development methods, however, the impact on civil liberties is ill-considered.

Evidenced by their attempts to include encrypted content in the retention policy, it is clear that the Home Office has difficulty understanding technical challenges. Instead, a claim of "National Security" trumps all and inhibits a proper conversation of what will work and be proportionate.

Development of the filter for data mining and complex queries will be designed and implemented without public consultation. The ISC report states that "evidence we have taken suggests that the filter will have to be constructed on an incremental basis, with rigorous testing and validation at each stage."

The hyperbole of urgency

The available evidence does not support the Home Office's hyperbole of urgency. Even if passed now, the bill would not be fully operational until 2018, and it is an attempt to solve a problem from 1998.

The Intelligence and Security Committee's report into the draft Bill states that for "the largest operation of its kind ever mounted by the Security Service" (prior to 7/7), less than 40 individuals were listed as having their full communications data histories analysed.

The proposed filter will be constructed and reconstructed to operate under and around a legal regime which is fundamentally unsuited to modern technology.

Of the "more than 4,000 telephone contacts" these persons had, the "vast majority of these calls or texts were wholly unconnected with attack planning or the wider facilitation network (and may have been as mundane as calling a takeaway restaurant)".

Conclusion

Obscured in a fog of secrecy and urgency, the lack of understanding of technology and Internet processes shown should be of deep concern to all. The proposed filter will be constructed and reconstructed to operate under and around a legal regime which is fundamentally unsuited to modern technology, let alone the challenges of agile development methods.

In summary, the draft Bill facilitates secret fishing expeditions, requiring surveillance of everyone. Police already have access to vast amounts of material from the mobile phones and computers of those arrested. As the ISC has previously stated in the context of their 7/7 inquiry report, "The focus then, rather than on gathering more intelligence, will be on the need to make better use of the intelligence they have gathered."[2]

Notes

1. http://necessaryandproportionate.net

2. Review of the Intelligence on the London Terrorist Attacks on 7 July 2005. UK Parliament, 2009. http://isc.independent.gov.uk/committee-reports/special-reports

A longer version of this note is available at www.PrivacyInternational.org

Conclusion and recommendations

Conclusion

Another surveillance law is possible

From the itemised records of the 90s through to the detailed records of our online behaviour, it is getting easier to track what we do. There is vastly more information now about our every movement than there ever has been.

Such information can be very useful to law enforcement agencies and other public bodies. There were 494,078 requests for 'communications data' under the Regulation of Investigatory Powers Act in 2011[1].

Some of the information about our connected lives is not legally available to law enforcement. Much of it, for example information from social media or our web histories, can be incredibly intrusive. It can reveal intimate details, including where we have been, what we have done, what we believe and who we know.

Through mistakes or abuse, the use of such information can lead to anything from wrongful suspicion through to the settling of scores. Merely the knowledge that what we are doing or saying is being tracked can have a chilling effect.

Just because information is useful to law enforcement does not mean that the state, or law enforcement agencies, or public bodies should be able to order its collection or have access to it. Our privacy rights are essential to ensure that we do not give away the power to collect and use information too cheaply.

The Government's current proposals, in the form of the Communications Data Bill, is a manifestation of the temptation to grab data where it exists, and of a failure to consider alternatives to blanket collection and retention of data.

Communications surveillance is a useful exercise. But we ask only that it be placed under the rule of law to ensure the effective and accountable use of what are significant powers.

Combined, the articles in this report add up to a call for more targeted, more transparent and more accountable surveillance laws. The authors offer a number of useful recommendations for how to achieve this.

Angela Patrick examines the case for judicial oversight in Chapter 2. She notes that oversight is extremely important where surveillance or data access is kept secret from the person investigated.

Caspar Bowden recommends a policy of 'data preservation' rather than blanket data retention. He suggests this could include quick response and emergency processes, and means to intelligently and accountably identify targets. He recommends a unified Surveillance Commissioner capable of carrying out a strong, independent audit with "multi-skilled investigators including human rights and computer experts."

Joss Wright recommends such audits be supported by stringent penalties for misuse of either powers or data, and for greater transparency. Simone Halink recommends building user notification into surveillance law, which would

require “individuals to be notified by default of a decision authorising the request for their communications data by law enforcement.“ Delays would be appropriate in exceptional circumstances.

Rachel Robinson of Liberty recommends lifting the ban on the use of intercept evidence in court. Sam Smith of Privacy International recommends investing in law enforcement’s capacity to use and analyse the data already available to them.

Peter Sommer recommends a more overarching review, potentially through a Royal Commission, to properly study surveillance in the digital age.

There is no shortage of ideas that could help inform policy makers’ thinking on surveillance in the digital age. There are other useful resources too. In particular the Draft International Principles on Communications Surveillance and Human Rights, which was put together by a number of civil society groups, provides a “framework against which we can evaluate whether current or proposed surveillance laws and practices are consistent with human rights”.[2]

This includes principles such as user notification, transparency and safeguards against illegitimate access. As Simone Halink points out in her contribution to chapter five, the government’s current proposals fall short when assessed against such principles.

In providing context and recommendations, the articles in this report offer a basis for a conversation about proportionate surveillance laws in the digital age. They are designed to help inform the ongoing policy debate sparked off by the Government’s draft Communications Data Bill and the subsequent inquiry by the Joint Committee.

In urging policy makers to consider these options, we are not picking sides or “putting politics before people’s lives”. We hope instead that the report makes policy makers aware of the many options available as they look to build privacy-friendly and effective surveillance law.

Notes

1. http://www.intelligencecommissioners.com/docs/0496.pdf

2. http://www.necessaryandproportionate.net/

Recommendations

1. Hold an overarching review, potentially through a Royal Commission, to properly study surveillance in the digital age.
2. Judicial oversight of requests for intrusive communications data, in particular for all traffic data requests.
3. Choose 'data preservation' rather than blanket data retention. Include quick response and emergency processes, and means to intelligently and accountably identify targets.
4. Create a unified Surveillance Commissioner capable of carrying out a strong, independent audit with "multi-skilled investigators including human rights and computer experts."
5. Reject vague proposals, such as those in the draft Communications Data Bill, for automated, pervasive analytics tools designed to trawl through and across datasets.
6. Provide stringent penalties for misuse of either powers or data.
7. Individuals should be notified by default of a decision authorising the request for their communications data.
8. Lift the ban on the use of intercept evidence in court.
9. Invest in law enforcement's capacity to use and analyse the data already available to them.
10. Use the International Principles on Communications Surveillance and Human Rights developed by Privacy International and other groups as a template for future laws.

Digital Surveillance

Why the Snoopers' Charter is the wrong approach:

A call for targeted and accountable investigatory powers

In the wake of the Government's proposed "Snoopers' Charter", ORG asks why intrusive new laws are being suggested, if they are needed at all and what the alternatives are. Some of the UK's most prominent surveillance experts examine the history of UK surveillance law and the challenges posed by the explosion of digital datasets.

Contributors include journalist Duncan Campbell, legal expert Angela Patrick from Justice, Richard Clayton of Cambridge University Computer Labs and Peter Sommer, Visiting Professor at De Montfort University.

This report is available at
www.openrightgroup.org/digitalsurveillancereport

About Open Rights Group

Open Rights Group (ORG) was formed in 2005 by a group of technology experts and activists to campaign for human rights and civil liberties in the digital age. ORG is funded by around 1,500 people, each contributing small regular amounts, and a number of grant giving organisations such as Joseph Rowntree Reform Trust, Sigrid Rausing Trust and Open Society Foundation.

Our Advisory Council includes Heather Brooke, Ben Goldacre, Cory Doctorow, Graham Linehan, David Allen Green, the MPs Tom Watson and Julian Huppert and a range of industry and legal experts and academics. We have a network of around 30,000 active supporters.

ORG led the campaign against the 'three strikes' provisions in the notorious (and UN Rapporteur-condemned) Digital Economy Act and successfully opposed BT and TalkTalk's involvement with the company Phorm, which planned to snoop on Internet traffic in order to profile users for advertising.

More recently ORG has also advocated for reforms to copyright, for example to permit personal copying and parodies using copyrighted work. Working with Privacy International and other campaign groups in Europe, ORG is also campaigning for stronger privacy rights in the new Data Protection Regulation. In 2012 ORG was jointly awarded the 'Human Rights Campaigners of the Year' award by Liberty.

OPEN RIGHTS GROUP