Context

Two fundamental issues were starkly revealed by Edward Snowden's disclosures, in 2013, concerning the UK government's interception and surveillance activities.

1. The government's agencies were doing more in these areas than had been evident from the passage of the relevant enabling legislation, and therefore more than elected representatives were aware of. This indicated a democratic shortfall in the way those powers had been assumed and exercised by the agencies concerned. In some cases their activities relied, for legitimacy [sic], on legal interpretations
2. The principles of necessity and proportionality which are clear in (particularly) EU legislation concerning law enforcement/national security use of personal data had been systematically disregarded. As a consequence, for instance, UK laws on mass retention of communications data were ruled unlawful.

Those two points set a clear context in which the government's current Investigatory Powers Bill (IP Bill) should be evaluated.

A number of other data points should be added to the context.

In December 2014 the Investigatory Powers Tribunal ruled against the government, finding that the interception regime operated by GCHQ was unlawful from 2004-2007. The regime failed to meet the European Convention on Human Rights' criterion that legal powers should be "foreseeable". It failed because the measures to ensure that the regime was not operated in an indiscriminate or arbitrary way were never made public - until, that is, they were forced into the public domain as a matter of court record. Even then, the measures were first disclosed only in closed session, and only then "transferred" to an open session of the IPT.

In July 2015 two MPs (one Conservative, one Labour) won a challenge in the UK High Court against the Data Retention and Investigatory Powers Act (DRIPA) - a victory made possible, in part, by the haste with which DRIPA was pushed through parliament. DRIPA, in turn, was enacted because its predecessor had been ruled unlawful: the EU Data Retention Directive 2006 was found, by the European Court of Justice, to fail the "necessity" criterion in its interference with the right to privacy. The government watched as, over a period of months, the UN, the European Parliament, and finally the ECJ stated that what it was doing violated the necessity and proportionality principles; it then claimed there was an "emergency", and enacted DRIPA in 8 days.

In the immediate aftermath of the Charlie Hebdo attacks in Paris, in January 2015, David Cameron expressed his determination to ensure that there should be no means of communication which the intelligence services are unable to read. This public position has resurfaced in the immediate aftermath of the November attacks in Paris, and again,

the government response has been to drastically cut the time allowed for parliamentary scrutiny of the draft IP Bill: in late November, despite a previous commitment *not* to 'fast track' this legislation, the Home Secretary set out a timetable requiring the joint committee on the IP Bill to submit its report by February 11th 2016. Taking into account the parliamentary recess over Christmas and the New Year, this means that the committee will have only three working weeks in which to do its work.

In both cases - the over-ruling of DRIPA and the November Paris attacks - the government has reacted by short-circuiting the consultation process, and rushing legislation through with minimal opportunity for scrutiny or debate.

The over-all picture is as follows:

- This government, like its (pre-Coalition) Labour predecessor, has repeatedly pressed for more extensive and more intrusive powers of interception;
- It has repeatedly indicated it would prefer no-one to be able to communicate confidentially, whatever the wider social or technical consequences;
- Its existing interception practices have repeatedly been ruled unlawful;
- Faced with legal challenges (which it loses) to what it does, the government has repeatedly brought forward legislation to legalise what it wants to do (and was doing already), rather than changing its behaviour to make it lawful.

This approach raises both systemic and specific issues which - on any analysis - cannot be adequately addressed through a three-week review of the draft. That is the first systemic issue: this legislation is being processed in a way which guarantees that it cannot be properly inspected. For a bill which affects the electronic communications and online lives of every UK citizen, that is a travesty.

Issues concerning civil and personal liberties.

The government's approach, over all, indicates an inexorable "direction of travel" in which civil and personal liberties are increasingly constrained, never enhanced or restored. That is a second systemic, societal harm which is never mentioned in the soundbites about "no place for criminals/terrorists to hide", "going dark", or "nothing to hide, nothing to fear". No serious contributor to the debate (and there are many on the side opposed to mass interception) questions the fact that serious crimes are planned and committed, or that serious countermeasures are appropriate. But the pro-surveillance argument (that one must sacrifice some civil and personal liberties in the name of security) deserves to be robustly challenged. Where does it lead? The implication is that one can achieve 100% security by sacrificing 100% of one's liberty. Not only is that untrue, it would also represent somewhere no-one in their right mind would want to live. A society in which individuals are unable to protect their personal

safety or privacy is one that lays them open to any malicious actor - including not just criminals, but also those in a position to abuse the exercise of surveillance powers.

See also a comment below, concerning the proposed accountability regime and the Bill's declaration of compliance with the European Convention on Human Rights.

Issues concerning transparency and accountability

In most areas of civil administration, western democracies are guided by principles of transparency and accountability. The third systemic issue with the IP Bill is that, in areas such as intelligence and national security (and, to some degree, in 'normal' law enforcement), the same degree of transparency and accountability is impossible to achieve. The argument, simply put, goes like this:

Govt.: "We need these powers in order to keep you safe from terrorists and criminals."
Citizen: "Are the powers proportionate and effective? Show us the evidence…"
Govt.: "We can't: it's confidential for operational reasons. If we showed you, the powers would cease to be effective."

In the absence of transparency, we therefore have to take on trust that the powers are necessary, proportionate, effective and being exercised with due accountability. In principle, that might suffice. There have been half a dozen commissioners responsible for oversight in various areas of interception and intelligence, each theoretically able to inspect and report on the exercise of the powers in question. Their annual reports are an exercise in the anodyne. On the basis of the reports alone, no-one would raise a ripple. The problem is that Snowden revealed a colossal gap between the little the oversight reports reveal, and what was actually being done. That gap is far wider than could be accounted for by the need for operational security. The IP Bill does nothing to close it - indeed, in reducing the oversight regime to a single body, it will predictably result in less focus on each specific variety of surveillance and interception, and less effective supervision (see the comment below about the divided role of Judicial Commissioners).

The government has made much of the introduction of what it theatrically refers to as the "double lock". This involves having a senior minister *and* a judge sign off on interception warrants, and is being portrayed as a comprehensive control mechanism. The opening page of the Guide to the Bill is explicit: "following Secretary of State authorisation, these – and other warrants – cannot come into force until they have been approved by a judge". The problem is that that is not what the Bill says. In fact, (Sections 20 and 25) a warrant can come into force without a judge's approval, and operate for five days before that approval must be given. So the "double lock" is a comprehensive and universal protection - except when it is not.

And what happens if, during that five day period, the targeted interception causes unwarranted harm to the individual in question, and the judge (within the five day period) refuses to approve the warrant? The Bill appears not to acknowledge this possibility. In fact, protections afforded to individuals under the Bill are very limited. For instance, Clause 169 (6) describes the Judicial Commissioner's responsibility for ensuring that the Investigatory Powers Commissioner does not jeopardise the success of or impede any civil servant, or "compromise the safety of those involved" in an intelligence, security or law enforcement operation. But it does not specify whether "those involved" include the subject of the operation. The implication is that only those conducting the operation benefit from this protection. Not only does this fail to represent the interests of citizens, it also unwisely divides the role of Judicial Commissioners between ensuring that the law is correctly put into practice, and constraining their own Commissioner in the exercise of his or her function.

Clause 171 of the Bill sets out as if it intends to protect individuals against erroneous or wrongful use of its powers, but almost immediately takes away with one hand what it has offered with the other (the italics are mine):

"The Investigatory Powers Commissioner *must* inform a person of any relevant error relating to that person of which the Commissioner is aware and which meets the conditions in subsection (2)."

Subsection 2 qualifies the Commissioner's duty as follows: the Commissioner must consider the error to be a serious one, and the Investigatory Powers Tribunal must then not only agree, but must also conclude that informing the person concerned is in the public interest. Note the way in which that equation is balanced: the IPT has to consider that informing the individual is in the *public* interest (not the interest of the individual about whom the serious error has been made). The IPT is not being asked to decide whether there is a public interest reason why the individual should *not* be informed. The default position is clearly expected to be that the individual will *not* be informed unless there is a general public interest in that happening.

This directly undermines the motivation of those responsible, to maintain transparency and accountability in the exercise of the powers provided by the Bill.

It gets worse. Clause 171 goes on to undermine citizens' rights under the Human Rights Act 1998, as follows:

"The fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error. "

Both the Commissioner and the Tribunal have to agree that the error has caused significant prejudice or harm to the person concerned. What constitutes significant prejudice or harm is not stated.

Let's not forget that the Bill as enacted *must* be preceded by the following declaration of compatibility (my underscore):

EUROPEAN CONVENTION ON HUMAN RIGHTS
"[Name to be replaced] has made the following statement under section 19(1)(a) of the Human Rights Act 1998:
In my view the provisions of the Investigatory Powers Bill are compatible with the Convention rights."

Issues concerning encryption

The IP Bill will doubtless, over time, be used to support the government's stated aim of ensuring that it has access to any communications, whether encrypted or not. This has been described as countering the risk that the intelligence and law enforcement services cannot function if the digital world "goes dark" (that is, if the contents - as opposed to the fact - of communication are pervasively encrypted). This gives a misleading impression, as the basis for the proposed powers, in two ways:

- First, it fails to acknowledge the role played by meta-data in support of intelligence and law enforcement analysis. Nicholas Weaver (International Computer Science Institute, Berkeley, California) has written a lucid analysis of why a focus on preventing encryption is misguided and unnecessary [1], and this piece [2] by the Electronic Frontier Foundation eloquently explains why the corresponding "don't worry, it's only metadata" argument is so dangerously bogus.
- Second, there is the simple fact that, through unencrypted traffic, open source intelligence and meta-data combined, the intelligence and law enforcement services now have access to a volume of data which dwarfs anything they had prior to the advent of the Internet. This is evident in the kinds of volume cited, for example, by the Guardian [3], according to whom GCHQ's Tempora program (interception of fibre optic links) was already collecting 21.6 petabytes of data per day, with an expected capacity of twice that. This figure does not include data from other sources, such as the Bulk Personal Datasets whose collection is permitted by the IP Bill, and which are described in this article [4] by investigative journalist Duncan Campbell.

What hampers the intelligence and security services, in these circumstances, is not paucity of data but surfeit of it: too much data makes it harder for agencies to identify, process and share the items that are critically important. The visible symptoms of this are the repeated instances in which we are told that "in retrospect it was found that intelligence and security services had been aware of x and his/her activities", but that for

some reason (unexplained under the current accountability/transparency regime) it had not been possible to act effectively on that information.

So, what does the Bill actually say on this subject? In fact, it only mentions "encryption" four times in 300 pages.

Three out of four of those mentions have little if any technical force:

- Clause 28 of the Guide to the Draft expresses the need for government agencies to interfere with communications devices, in cases where encryption prevents them from accessing the data they want;
- Part 8, Chapter 1, Section 169(3) requires the Investigatory Powers Commissioner to keep an eye on agencies' investigation of encrypted data;
- Page 285, Explanatory Note on Clause 187 explains that GCHQ may now "make use of" encrypted data and related information, and not just "monitor or interfere" with it.

The fourth mention is on page 29 of the Guide to the Draft, clauses 62 and 63. These explain that current legislation (RIPA, the Regulation of Investigatory Powers Act 2000) obliges Communications Service Providers (CSPs) to help give effect to interception warrants, including the capability *to remove any encryption applied by the CSP to whom the notice relates*. Clause 63 says that the draft Bill will not impose any additional requirements in this respect, over and above those in RIPA.

What does that mean in practice?

First, bear in mind something Bruce Schneier has said about encryption:

"Encryption works best if it's ubiquitous and automatic. The two forms of encryption you use most often -- https URLs on your browser, and the handset-to-tower link for your cell phone calls -- work so well because you don't even know they're there." [5]

Second, Doug Tyger's 1999 paper "Why Johnny Can't Encrypt" [6] gives a useful account of the technical and usability challenges people face in trying to use encryption technology to good effect.

The upshot of these two commentaries is that, the more you expect end users to involve themselves in encrypting their communications, the less likely they are to do it, and to do it successfully.

The draft IP Bill seems to rely on exactly that. If, in the interests of ease and convenience, you rely on your CSP to encrypt your emails, instant messages and VOIP sessions, then you have to expect that they will remove that encryption on demand. If, instead, you go to the trouble of installing an end-to-end email encryption plug-in (such

as GPGMail), then the encryption of your email is not "applied by the CSP", and the Bill doesn't oblige them to remove it.

However, in that case the Bill provides for what it calls "equipment interference": the ability for an agency to tamper with communications devices so as to make interception possible. The Bill, naturally, says nothing about how this might be done - but one way might be to arrange for a keystroke logger to be installed on a computer, so that the user's passwords (and therefore their keychains) can be accessed.

Another option might be for the CSP to make it possible for the agency to modify a router, firewall or cable modem - again, with the goal of compromising security measures applied by a user. As clause 63 of the draft puts it: the IP Bill "will provide an explicit obligation on CSPs to assist in giving effect to equipment interference warrants".

Then there are the grey areas.

- What, exactly, counts as a CSP? If you are staying in a hotel, and the hotel provides you with Internet access, are they acting as a CSP? If, like many hotels, they force you to access the Internet through their own "captive portal", are they in a position to stop you using a VPN or establishing an HTTPS session, and if so, would the IP Bill oblige them to do so on demand? The draft doesn't address these questions, and a prospective law would have to be much clearer on the difference between public versus private communications service providers, what "public access" means, and any relevant distinctions between a "communications service provider", an "online service provider", and the provider of a commercially-available application that enables communication.
- Part 1, Section 2 of the draft says it is not an offence to intercept your communications if the person doing so has the right to control the operation or use of the system. Again, this seems to legalise the interception of your communications by, for instance, whoever grants you access to a hotel's network.
- And what happens if a service provider such as Google provides you with the means to apply end-to-end encryption to your mail traffic? Does that count as "encryption applied by the CSP", and if so, how is the service provider supposed to remove it on demand? If it's genuinely end-to-end, the service provider *ought* to have no access to the keys you use… so is this a requirement for crypto back-doors, by the back-door, so to speak?
- I mention Google as an example, not just because it's offering end-to-end mail encryption, but also because it's a non-UK company. The draft Bill sets out the kind of mutual legal assistance agreements under which it expects to get the co-operation of non-UK authorities, but it also tries to explain the distinction between UK and overseas interception. This is a notoriously tricky area, and the draft is unclear on the details. In some cases, the legality of intercepting my communications could depend on whether or not I am in the UK at the time (Part 1, Section 10); I suspect it's asking a lot of an agency to turn interception on

> or off based on whether or not I'm on a business trip at the time… and yet, if they fail to do so they could be breaking the law.

The draft Bill certainly seems like a step back from Mr Cameron's well-publicised statements about leaving terrorists nowhere to hide their communications. That is a good thing; the goal of simply making it impossible for bad actors to communicate securely is unrealistic, and risks giving rise to policies that do far more harm than good.

The Bill does not appear to prohibit terrorists (or me, as a UK citizen) from using mail encryption, VPNs, Tor and other tools to try and keep my communications confidential. But if I'm lazy, and rely entirely on the encryption applied by others, I should assume that they will turn it off on demand. The quote I gave from Bruce Schneier is significant in that regard: in both the examples he gives, the encryption could be neutralised by a CSP acting under an interception warrant.

If I rely on my own use of encryption tools, I should expect the intelligence services to try to compromise my devices, or look for weaknesses in my use of the tools, if they want access to my data.

The draft does little, in my view, to clarify the kinds of grey area set out above, and in that respect it misses the opportunity to address problems which have been obvious for some years. The logical inference is that it was not intended to do so, and that some of those grey areas are actually helpful to the agencies in question - even though they also reduce clarity and transparency of the law. Rather than being drafted to clarify these issues, it's more likely that the primary purposes of the Bill relate to other topics discussed in these comments - such as the introduction of new requirements for mass data retention, and the limited new role of judges in approving interception warrants.

The government has clearly succumbed to the temptation to use November's terrorist attacks in Paris opportunistically, to shorten the consultation process for this Bill. That is regrettable. Laws made in haste are seldom wise, and often counter-productive. This is no time for a reflex reaction: it is a time to reflect deeply on what our core values are as a society, and on how our laws and practices can best represent those values.

The government may also take this opportunity to try to legislate against specific technologies. Any attempts in that direction should be strongly resisted. Legislation should be directed at behaviour, not technology.

The government should also bear in mind (and the attacks on Paris amply illustrate this point) that UK legislation in this regard needs to fit into a global context. The UK, of course, has specific national security interests - but these cannot be protected by UK-only actions or UK-only laws. The cross-border dimension is crucial: it needs to be factored into encryption policy through collaborative engagement with other stakeholders, and reflected in a recognition that the UK government damages its own,

and its citizens' interests by weakening the protections they are able to apply on their own behalf, or request from service providers.

Issues concerning Internet Connection Records

Perhaps the principal technical change proposed by the Bill concerns so-called "Internet Connection Records". Clause 71 (9) sets out what the Bill means by "relevant communications data" in this context, and Clause 193 attempts to draw the technical distinction between what may legally be retained and "content of a communication". This is intended to constrain ICRs so that they do not reveal what the communication is about.
ICRs are not meant to reveal "anything of what might reasonably be expected to be the meaning of the communication".

To remind you - the Guide says this:

"in the particular context of web browsing anything beyond data which identifies the telecommunication service (e.g. bbc.co.uk) is content". The stated aim, here, is that an ICR should only record the fact that the bbc.co.uk site was visited, but disregard any details that might follow that basic URL (the Uniform Resource Locator, or web address).

In that context, the text of Clause 193 simply does not make any sense. The URL of a website or online service is, in many cases, explicitly intended to convey information about the nature of the service provided, and that in turn supports inferences about the meaning of communication with that website.

Clause 193 (6) b says:

"any meaning arising from the fact of the communication or from any data relating to the transmission of the communication is to be disregarded"

However, a website whose URL indicates that it concerns sexual health, or insurance quote comparison, cannot avoid revealing something about the meaning of the communication with that site.
It is not clear who is supposed to disregard this information, or how they are supposed to do so while still satisfying the requirement to keep a record of which websites a device has connected to.
A communications service provider seeking to comply with this aspect of the Bill faces, in my view, a problem statement which is either meaningless or insoluble - or both.

The technical implications of the Bill are unrealistic in other respects, too, reflecting an apparent lack of understanding about the realities of the World Wide Web and its Internet infrastructure. Two examples may illustrate some of the problems:

1 - If I explicitly visit, say, the website of the New York Times, my browser also establishes connections to numerous third-party services, some of which embed visible content on the NYT home page, and others of which represent tracking services which are invisible to the end user. I, as the user, did not intend to visit any of those services, and in many cases I may be unaware that the connection has been made. But as far as the IP Bill's Clause 193 goes, each of those newly-established connections to an online service must be captured in an ICR.

Two hypothetical outcomes present themselves: one is that under the 'user-friendliest' interpretation of the goal as expressed by the Guide (as cited above), these connections will be considered as "content beyond data which identifies the telecommunication service" and not captured. In this case, this seems to be an obvious mechanism for malicious actors to exploit as a covert communications channel, thus entirely subverting the purpose of the Bill. The other is that the connections are all considered as ICRs within the intent of the Bill. In this case, the Bill increases by a factor of 10 or 20 the data CSPs are obliged to retain, with no prospect of a practical benefit (given that malicious exploitation as described above would be a vanishingly small proportion of such connections). In this respect, the Bill is likely to prove both disproportionate and ineffective at a stroke.

2 - The Guide's qualification of interception in this area ("in the particular context of web browsing…") leaves unanswered the question of ICRs for web applications that are not accessed via a browser. Mobile devices and, increasingly, connected or 'smart' objects use Internet and web protocols, but do not present the user with a browser interface. Increasingly, applications may keep a connection open for hours or days, meaning that many of the time-related examples the government presents in support of retaining such "connection" records make no sense. This has been well articulated by, among others, Adrian Kennard (Managing Director of a UK Internet Service Provicer) in his written submission [7] concerning the Bill.

Again, a CSP seeking to judge how to comply with the Bill will have nothing practical to work with. The Guide - not being part of the Bill - has no legal force, so if it expresses intentions or details that are not reflected in the Bill, what appears in the Guide is nothing more than an aspiration.

The overwhelming impression left by the sections of the Bill dealing with ICRs is that policymakers' idea of what ICRs are, and what they want to achieve through their retention, are vague, under-informed, and therefore not a safe basis on which to legislate.

References

[1] https://www.washingtonpost.com/news/in-theory/wp/2015/12/14/we-think-encryption-allows-terrorists-to-hide-it-doesnt/
[2] https://ssd.eff.org/en/module/why-metadata-matters
[3] http://www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work
[4] http://www.theregister.co.uk/2015/12/16/big_brother_born_ntac_gchq_mi5_mass_surveillance_data_slurping/
[5] https://www.schneier.com/blog/archives/2015/06/why_we_encrypt.html
[6] http://www.ischool.berkeley.edu/newsandevents/news/20150818whyjohnnycantencrypt
[7] https://www.techdirt.com/articles/20151128/00573032936/uk-isp-boss-highlights-technical-stupidity-snoopers-charter-proposal.shtml