GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

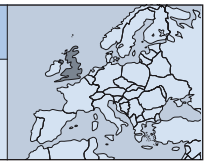
Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

UNITED KINGDOM

GCHQ: The NSA's Little Brother... not so little anymore



Open Rights Group
Javier Ruiz Diaz
www.openrightsgroup.org

Introduction

The documents leaked by the whistleblower Edward Snowden show that the United Kingdom (UK) is collecting information on millions of innocent citizens worldwide, in breach of human rights. British spies are also spreading malicious software, breaking internet security and carrying out attacks against protest groups, companies and other actors that are not terrorists or serious criminals.

So far the attention of most of the international media and public opinion has focused almost exclusively on the National Security Agency (NSA), the signals intelligence agency of the United States (US). But the NSA operates a global surveillance machine that relies on a network of key partners ranging from Israel to Sweden. First and foremost is its UK counterpart, the General Communications Headquarters (GCHQ).

It is important that civil society organisations throughout the world concerned about mass surveillance broaden the focus of their attention from the US and the NSA to include the UK and GCHQ.

Below we summarise some of the key activities of UK surveillance agencies exposed by Edward Snowden.

Beyond signals intelligence

Mastering the internet

> *But we are starting to "master" the Internet. And our current capability is quite impressive... We are in a Golden Age.* (GCHQ internal document)[1]

The activities of the UK's GCHQ are so inextricable from those of the NSA that from a certain perspective it makes little sense to treat them as separate entities. This cooperation started in earnest during the Second World War, and continued during the Cold War, with Britain providing forward listening stations in colonial outposts such as Hong Kong.

But the documents leaked by Snowden reveal many instances where the responsibilities of the UK can be clearly determined. For example, we know that GCHQ scoops the personal data of millions of innocent people around the world[2] by tapping into fibre optic cables that pass through Britain. This programme is called Tempora, and it is described in detail in the thematic report on the Five Eyes in this edition of GISWatch.

It is shocking that a private NSA contractor like Snowden had access to such an amount of information on British intelligence, and it is certainly not the full picture. Nevertheless, the leaks about GCHQ reveal an agency pursuing global domination of cyberspace by any means necessary.

Hacking private webcam conversations

> *Unfortunately ... it would appear that a surprising number of people use webcam conversations to show intimate parts of their body to the other person.* (GCHQ internal document)[3]

The programme Optic Nerve involved tapping into the private webcam communications of innocent Yahoo subscribers and collecting millions of still images, including substantial amounts of explicitly sexual materials.[4] The programme, apparently unknown to Yahoo, targeted 1.8 million unwitting users in a six-month period without any form of minimisation or filtering. The agency did this in order to improve their facial recognition capabilities, with the metadata and images being fed into the key NSA databases and its search engine, XKEYSCORE.

US senators have launched an investigation[5] into Optic Nerve, accusing GCHQ of a "breathtaking lack of respect for privacy and civil liberties." GCHQ

1 MacAskill, E., Borger, J., Hopkins, N., Davies, N., & Ball, J. (2013, June 21). Mastering the internet: how GCHQ set out to spy on the world wide web. *The Guardian*. www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet

2 MacAskill, E., Borger, J., Hopkins,N., Davies, N., & Ball, J. (2013, June 21). GCHQ taps fibre-optic cables for secret access to world's communications. *The Guardian*. www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

3 Clark, J. (2014, February 27). UK spies on MILLIONS of Yahoo! webcams, ogles sex vids - report. *The Register*. www.theregister.co.uk/2014/02/27/gchq_optic_nerve

4 Ackerman, S., & Ball, J. (2014, February 28). Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ. *The Guardian*. www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo

5 Ackerman, S. (2014, February 28). Senators to investigate NSA role in GCHQ 'Optic Nerve' webcam spying. *The Guardian*. www.theguardian.com/world/2014/feb/28/nsa-gchq-webcam-spy-program-senate-investigation

has simply provided a boilerplate response about compliance with UK laws.

Psychological operations against non-violent protest groups

> *[15:42] <·····speakeasy·····> we're being hit by a syn flood*[6]
> *[16:44] <·····speakeasy·····> I didn't know whether to quit last night, because of the ddos*[7] (Anonymous chat room log)[8]

GCHQ has moved from collecting "signals" and generating intelligence for other bodies, to proactive action,[9] now representing 5% of GCHQ's "business".[10] This action ranges[11] from psychological warfare, such as deleting a target's online presence and spreading false information, to hacking and disabling target systems through denial of service (DOS) attacks.

A leaked catalogue of GCHQ hacking tools[12] shows that they built specific software for manipulating online communications and behaviour, not just collecting information. Among many others, these include tools to modify online polls, the popularity of YouTube videos, and traffic to specific websites.

It is particularly worrying that GCHQ considers as legitimate targets groups not involved in terrorism or serious crime, such as the "hacktivists" of Anonymous.[13] Their chat rooms were shut down by GCHQ's own hacking operations in 2011, called Rolling Thunder, with the effect of pushing away some 80% of visitors. GCHQ has also targeted supporters of Wikileaks,[14] albeit in a less aggressive manner.

Industrial-scale hacking

GCHQ is a key partner in a joint system developed with the NSA capable of attacking millions of computers in a semi-automated process. Quantum[15] is a collection of tools that turn the global listening apparatus of these agencies – dozens of both owned and hacked computers and routers in the heart of the internet backbone – into an active cyber weapon.

These are tools for hacking on an industrial scale. They analyse their target computers and automatically deliver tailored malware that allows the agencies to control computers, including the microphone and camera. These malware tools are sometimes distributed by creating fake Facebook or LinkedIn pages.

GCHQ's own legal departments appear to have raised concerns about the legality of these techniques,[16] which are directed not just against dangerous criminals, but in many cases innocent administrators of computers networks and international mobile operators.[17] In a particularly scandalous case, GCHQ used these tools to hack into the systems of Belgian telecoms firm Belgacom.[18]

Weakening the internet

In order to make it possible for the NSA and GCHQ to break into thousands of computers, the agencies have been actively undermining fundamental security technologies, such as encryption systems. The UK has its own programme to weaken internet security called Edgehill.[19]

The revelations that UK and US security services have actively sought to lower the security of the internet as a whole for their own purposes have caused massive consternation[20] among the internet technical community. There are concerns that cyber

6 https://en.wikipedia.org/wiki/SYN_flood

7 https://en.wikipedia.org/wiki/Denial-of-service_attack

8 NBC News Investigations. (2014). *The Snowden files: British intelligence agency describes attack on Anonymous*. msnbcmedia.msn.com/i/msnbc/sections/news/snowden_anonymous_nbc_document.pdf

9 The Intercept. (2014, April 4). Full-spectrum cyber effects. *The Intercept*. https://firstlook.org/theintercept/document/2014/04/04/full-spectrum-cyber-effects/

10 NBC News Investigations. (2014). *The Snowden Files: British Spies Used Sex and 'Dirty Tricks'* . msnbcmedia.msn.com/i/msnbc/sections/news/snowden_cyber_offensive2_nbc_document.pdf

11 NBC News Investigations. (2014). *The Snowden files: British Spies Used Sex and 'Dirty Tricks'* . msnbcmedia.msn.com/i/msnbc/sections/news/snowden_cyber_offensive1_nbc_document.pdf

12 Greenwald, G. (2014, July 14). Hacking Online Polls and Other Ways British Spies Seek to Control the Internet. *The Intercept*. https://firstlook.org/theintercept/2014/07/14/manipulating-online-polls-ways-british-spies-seek-control-internet

13 NBC News Investigations. (2014). *The Snowden files: British intelligence agency describes attack on Anonymous*. msnbcmedia.msn.com/i/msnbc/sections/news/snowden_anonymous_nbc_document.pdf

14 Greenwald, G., & Gallagher, R. (2014, February 18). Snowden Documents Reveal Covert Surveillance and Pressure Tactics Aimed at WikiLeaks and Its Supporters. *The Intercept*. https://firstlook.org/theintercept/article/2014/02/18/snowden-docs-reveal-covert-surveillance-and-pressure-tactics-aimed-at-wikileaks-and-its-supporters

15 cryptome.org/2013/12/nsa-quantum-tasking.pdf

16 Gallagher, R. J. (2013, December 12). GCHQ's Dubious Role in The 'Quantum' Hacking Spy Tactic. *Ryan Gallagher*. notes.rjgallagher.co.uk/2013/12/gchq-quantum-hacking-surveillance-legality-nsa-sweden.html

17 Paterson, T. (2013, November 10). GCHQ used 'Quantum Insert' technique to set up fake LinkedIn pages and spy on mobile phone giants. *The Independent*. www.independent.co.uk/news/uk/home-news/gchq-used-quantum-insert-technique-to-set-up-fake-linkedin-pagesand-spy-on-mobile-phone-giants-8931528.html

18 Der Spiegel. (2013, September 20). Belgacom attack: Britain's GCHQ hacked Belgian telecoms firm. *Der Spiegel*. www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html

19 Larson, J., Perlroth, N., & Shane, S. (2013, September 5). Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security. *ProPublica*. www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption

20 Schneier, B. (2013, September 5). The US government has betrayed the internet. We need to take it back. *The Guardian*. www.theguardian.com/commentisfree/2013/sep/05/government-betrayed-internet-nsa-spying

criminals and other spying agencies will eventually use the same weaknesses.

Intercepting the internal communications of internet companies

> Unfortunately we live in a world where all too often laws are for the little people. Nobody at GCHQ or the NSA will ever stand before a judge and answer for this industrial-scale subversion of the judicial process. (Mike Hearn, Google security engineer)[21]

The NSA – in partnership with the FBI – has direct access to data held by several major US internet companies through the PRISM programme. But in addition, the NSA and GCHQ have been intercepting the private cables that connect the data centres of some of these companies, including Google and Yahoo. The joint programme – called Muscular[22] – is based in Britain and mainly run by GCHQ.

This type of bulk collection had been ruled illegal in the US[23] because operations in the homeland have to filter out the data of US persons (citizens and permanent residents). The NSA appears to bypass these restrictions by getting GCHQ to collect the data, which they are then free to search and process.

Failures in the regulation of GCHQ

> *All of GCHQ's work is carried out in accordance with a strict legal and policy framework which ensures that our activities are authorised, necessary and proportionate, and that there is rigorous oversight.* (GCHQ boilerplate response to inquiries)
>
> *We have a light oversight regime compared with the US.* (Leaked GCHQ internal memo)

The legislation governing GCHQ is very complex. The organisation operated in the shadows from its creation[24] until 1994, when its existence was officially recognised in the Intelligence Services Act,[25] which also created a parliamentary committee to provide some oversight. The Regulation of Investigatory Powers Act (RIPA 2000)[26] created a system of warrants and further oversight by independent commissioners.

The UK surveillance system has some peculiarities, for example:

- Ministers or staff, not judicial courts, sign surveillance warrants.
- A secret court, the Investigative Powers Tribunal, which is deemed by rights groups to be insufficient, hears complaints about surveillance or intelligence services.
- Intercept evidence is not admissible in court in order to protect the methods of the security services. This means that when police or GCHQ wiretap a phone call they will use this to obtain further evidence, but a jury will not hear the content of the call. Metadata in the form of call logs and mobile location is widely used.

It is important to note that there is a legal and practical distinction between surveillance for national security by spy agencies and the use of similar techniques by police forces.

Weak oversight of the surveillance regime

A recent report[27] by the Home Affairs Committee of the British Parliament was overtly critical of the current oversight mechanisms. They found the Intelligence and Security Committee (ISC) to be too cosy with the executive, despite recent changes to its statute. For example, the ISC had cleared GCHQ of any wrongdoing about PRISM in July 2013,[28] soon after the first publication of leaked documents. As the evidence of potential abuse piles up month after month, the ISC remains broadly supportive of GCHQ.

According to the report, the independent commissioners tasked with monitoring the security services simply do not have the capacity to deal with the hundreds of thousands of surveillance requests in place every year.

Jurisdiction hopping

There are concerns that the NSA and GCHQ use gaps in their regulatory frameworks to help each other bypass limitations on indiscriminate surveil-

21 https://plus.google.com/+MikeHearn/posts/LW1DXJ2BK8k

22 apps.washingtonpost.com/g/page/world/how-the-nsas-muscular-program-collects-too-much-data-from-yahoo-and-google/543

23 Gellman, B., & Soltani, A. (2013, October 30). NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. *The Washington Post*. www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

24 www2.warwick.ac.uk/fac/soc/pais/people/aldrich/vigilant/lectures/gchq/

25 www.gchq.gov.uk/how_we_work/running_the_business/oversight/Pages/the-law.aspx

26 www.legislation.gov.uk/ukpga/2000/23/contents

27 UK Parliament Home Affairs Committee. (2014). *Oversight of the security and intelligence agencies*. www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/23108.htm

28 UK Parliament Intelligence and Security Committee. (2013, July 17). Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme. *Statewatch*. www.statewatch.org/news/2013/jul/uk-isc-gchq-surveillance-statement.pdf

lance carried out within national soil or affecting their own nationals.

The US and UK are not meant to spy on each other's population, but a leaked memo[29] from 2007 shows that the US is now "incidentally collecting" data on UK citizens who were not the target of any investigation. Proposals to increase privacy protections in any of these countries, such as those recently proposed by the Obama administration in the US,[30] are hollow if other countries in the alliance can help bypass them.

Mass surveillance is a breach of human rights

Bulk collection of data is lawful in the UK.[31] The Secretary of State[32] can sign special "certificates" that allow for mass surveillance of any targets outside the British Isles under very broad themes, including "intelligence on the political intentions of foreign governments; military postures of foreign countries; terrorism, international drug trafficking and fraud."

These certificates have been labelled "a blank cheque to spy on the world" by campaigners[33] who doubt they comply with international human rights laws.

Unaccountable hacking is unlawful

In contrast to the justifications provided for some of the other programmes, no government official has replied to the widespread evidence of mass hacking in leaked documents. Privacy International has challenged[34] the compliance of these activities with human rights legislation.

Weak public and political reaction

The public reaction to the Snowden revelations has been quite muted in the UK. There are several inquiries and reviews in motion but no substantial changes. The Royal United Services Institute has been commissioned by the deputy prime minister to report after the next general election in May 2015.[35] The parliamentary committee in charge of overseeing GCHQ has predictably concluded that the agency did not break any laws.[36] The Labour Party, currently in opposition, has asked for a fundamental review of surveillance to deal with the lack of trust in the spy agencies but it has stopped short of criticising the activities of GCHQ.

These timid reactions are in stark contrast to the US, where there are competing legislative reforms.[37] Undoubtedly the lack of political reactions reflects the low level of public awareness and debate about mass surveillance among the UK population. There are several hypotheses for this apparent lack of public concern.

Media self-censorship

The coverage of the Snowden leaks in the UK has fallen disproportionately on *The Guardian* newspaper, with little coverage in other papers and TV. The paper had a natural lead as the original recipient of the leaked documents. But while media outlets in other countries have since obtained source documents and produced their own stories, this has not been the case in Britain.

The UK operates a system of voluntary censorship for national security issues, called the D-Notice,[38] issued by the Defence, Press and Broadcasting Advisory Committee (DPBAC). The DPBAC sent out a reminder to the media the day after *The Guardian* started publishing the leaked documents, and it seemed to work.

Trust in the spy agencies?

Popular wisdom is that the enduring mythology about British spies, from Lawrence of Arabia to James Bond,[39] makes it hard to challenge the UK "secret state". In addition, GCHQ is widely credited with a major contribution to the allied victory in World War Two by cracking the German encryption

29 Ball, J. (2013, November 20). US and UK struck secret deal to allow NSA to 'unmask' Britons' personal data. *The Guardian*. www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data

30 Cohn, C., & Higgins, P. (2014, January 17). Rating Obama's NSA Reform Plan: EFF Scorecard Explained. *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2014/01/rating-obamas-nsa-reform-plan-eff-scorecard-explained

31 MacAskill, E., Borger, J., Hopkins,N., Davies, N., & Ball, J. (2013, June 21). The legal loopholes that allow GCHQ to spy on the world. *The Guardian*. www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world

32 In the United Kingdom, a secretary of state is a cabinet minister in charge of a government department.

33 Bunyan, T. (2014). GCHQ is authorised to "spy on the world" but the UK Interception of Communications Commissioner says this is OK as it is "lawful". *Statewatch*. www.statewatch.org/analyses/no-244-gchq-intercept-commissioner.pdf

34 Wilson, C. (2014, May 13). Explaining the law behind Privacy International's challenge to GCHQ's hacking. *Privacy International*. https://www.privacyinternational.org/blog/explaining-the-law-behind-privacy-internationals-challenge-to-gchqs-hacking

35 https://www.rusi.org/news/ref:N5315B2C9B1941/

36 BBC. (2013, July 17). GCHQ use of Prism surveillance data was legal, says report. www.bbc.co.uk/news/uk-23341597

37 Glaser, A. (2014, April 23). Comparing NSA Reforms to International Law: A New Graphic by AccessNow. *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2014/04/comparing-nsa-reforms-international-law-new-graphic-accessnow

38 www.dnotice.org.uk

39 Frith, H. (2014, February 20). Ian Fleming romance points up ambiguous attitude to spying. *The Week*. www.theweek.co.uk/tv-radio/57398/ian-fleming-romance-points-ambiguous-attitude-spying

codes at Bletchley Park.[40] In contrast, the 1960s and 1970s saw several scandals that shook the polished image of the UK spy agencies,[41] but their effect on current popular perceptions is unclear.

Trust in public institutions has declined in much of Europe,[42] and the UK seems to follow a similar pattern to other countries. In most European countries, citizens trust the police more than politicians and other public bodies.[43] It is possible that this trust somehow extends to spy agencies.

Terrorist threat

The UK is a clear target of terrorist groups due to its close alignment with the US and military involvement in Iraq and Afghanistan. Citizens are acutely aware of the threat, with constant reminders in public spaces. This has a likely influence on perceptions of the balance of risk.

Action steps

Don' t Spy on Us

UK civil society groups have been running a joint advocacy campaign – DontSpyonUS.org.uk – demanding fundamental reforms of surveillance legislation and practices:

> Don't Spy On Us is calling for a new Parliamentary Bill to make the spooks accountable to our elected representatives, to put an end to mass surveillance and let judges, not the Home Secretary, decide when spying is justified.[44]

The campaign is asking for international supporters to sign up and endorse its proposals.

Legal challenges

There are several legal challenges being brought forward by UK civil society groups. Open Rights Group, Big Brother Watch and English PEN, together with German activist Constanze Kurtz, have taken the UK government to the European Court of Human Rights. They managed to crowd-fund over £20,000 for legal fees[45] in just 48 hours.

Other organisations – including Liberty (the National Council for Civil Liberties) and Privacy International – have placed a complaint at the Investigatory Powers Tribunal. The first hearings have led to unprecedented disclosures, as the security services have been forced to defend the legality of their practices[46] – but in all likelihood the case will end up in a European court.

Most major reforms of the British security services over the past 30 years have been driven by European legislation and court rulings. For example, the RIPA law mentioned above was created in order to comply with the European Convention on Human Rights, as it became UK law. So it would be important for more civil society organisations and concerned individuals to challenge the activities of the UK at European courts.

Advocacy for reform

The Don't Spy on Us Campaign has a set of principles for reform, based on the 13 International Principles on the Application of Human Rights to Communications Surveillance.[47] They are trying to get all major political parties to support a wholesale review of surveillance. But while all the three main parties are proposing some form of review or enquiry, these fall short of the demands of civil society.

International agreements

Even if UK campaigners won each of their demands, reforms at the national level would not be enough. The UK and the US have built a very complex surveillance machine that involves many other countries, and reforms will need to take place elsewhere to be effective. Third party allies such as Sweden, France and Germany will need to put their own house in order as well.

There is a need for some form of international agreement, as no state will unilaterally reduce its surveillance capability. Mass digital surveillance and the corresponding militarisation of cyberspace are complex problems, much like nuclear weapons or climate change. These involve systemic changes beyond tinkering with oversight mechanisms.

Technical and business measures

Stopping mass surveillance requires more than legal and political changes. As long as the business models of internet companies are based on surveillance, governments will find a way to tap into these data pools. There is a need for new models that

40 www.bletchleypark.org.uk

41 www2.warwick.ac.uk/fac/soc/pais/people/aldrich/vigilant/lectures/gchq/

42 Park, A., Bryson, C., Clery, E., Curtice, J., & Phillips, M. (Eds.) (2013). *British Social Attitudes: The 30th Report*. London: National Centre for Social Research bsa-30.natcen.ac.uk/read-the-report/key-findings/trust,-politics-and-institutions.aspx

43 Committee on Standards in Public Life. (2014). *Public Perceptions of Standards in Public Life in the UK and Europe*. www.public-standards.gov.uk/wp-content/uploads/2014/03/2901994_CSPL_PublicPerceptions_acc-WEB.pdf

44 https://www.dontspyonus.org.uk/pi

45 https://www.privacynotprism.org.uk

46 https://www.privacyinternational.org/what-to-know-gchq-on-trial

47 https://en.necessaryandproportionate.org/text

minimise corporate surveillance for commercial purposes.

Mass surveillance systems are a very good example of Larry Lessig's maxim, "Code is law."[48] Any proposals for change must also involve technology. For example, there are several campaigns to promote widespread encryption,[49] and the technical community that keeps the internet running have started to consider a fundamental architectural redesign to make the job of the spooks harder.[50]

The securocrats strike back

The Snowden leaks were not a complete surprise to British human rights campaigners, who had long complained about legal loopholes creating the potential for excessive surveillance. The leaks arrived just as these groups were winning a temporary reprieve against legislative proposals to strengthen the UK's surveillance capability. The draft Communications Data Bill (CDB)[51] – dubbed the Snoopers' Charter – had proposed to give the security services automated direct access to the inner systems of communications providers and internet companies through a form of search engine.

The draft bill was blocked by the minority partners of the coalition government – the Liberal Democrats – due to concerns over the human rights implications of such an intrusive system. With hindsight, the CDB appears eerily similar to some of the systems described in the leaks, such as PRISM and XKEYSCORE. Although the law was put in the freezer, several hundred million pounds have already been spent on these systems. It is not known what level of implementation and oversight is in place.

Any hopes that the current UK government would voluntarily commit to fundamental reforms on mass surveillance were dashed with the introduction of the Data Retention and Investigatory Powers (DRIP) Bill[52] in July 2014. This emergency legislation was ostensibly introduced to deal with the fallout of the ruling of the Court of Justice of the European Union in April 2014 that declared the EU Data Retention Directive invalid.[53] The directive forced communications providers to keep logs of all calls, websites, emails, etc. from all customers, in case the security services needed them. This was found to be too broad and disproportionate to be compatible with human rights law.

The new bill is meant to be just a replacement of the Data Retention Directive, but it adds a unique extraterritorial expansion[54] of British surveillance powers to cover any form of internet provider anywhere in the world.

Instead of carefully considering the content of the ruling and its implications for all forms of indiscriminate blanket data collection, the UK government has rammed through parliament groundbreaking surveillance legislation without any proper debate. This has been achieved in a deal among the three main parties, which have all supported the core aspects of the bill. In exchange the government has now committed to review surveillance laws by the next election, in May 2015, and to introduce a US-inspired privacy board.

The DRIP Bill has already been threatened with legal challenges by human rights groups. Two parliamentarians have asked for a judicial review on the grounds that it breaches human rights, with the support of Liberty.[55] Open Rights Group also has plans to take the Home Office to court over the DRIP Bill.[56.]

48 Lessig, L. (2000). Code Is Law. *Harvard Magazine*, January-February. harvardmagazine.com/2000/01/code-is-law-html

49 https://en.necessaryandproportionate.org/text

50 https://www.w3.org/2014/strint

51 https://www.openrightsgroup.org/issues/Snoopers'%20Charter

52 services.parliament.uk/bills/2014-15/dataretentionandinvestigatorypowers.html

53 European Data Protection Supervisor. (2014, April 8). Press statement: The CJEU rules that Data Retention Directive is invalid. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2014/14-04-08_Press_statement_DRD_EN.pdf

54 Open letter from UK Internet Law Academic Experts to All Members of Parliament, 15 July 2014. www.slideshare.net/EXCCELessex/open-letter-uk-legal-academics-drip

55 https://www.liberty-human-rights.org.uk/news/press-releases/liberty-represents-mps-david-davis-and-tom-watson-legal-challenge-government%E2%80%99s-

56 Killock, Jim. (2014, July 18). Dear Theresa, see you in court. *Open Rights Group*. https://www.openrightsgroup.org/blog/2014/dear-theresa-see-you-in-court