Two years after Snowden: protecting human rights in an age of mass surveillance

Executive summary

"The hard truth is that the use of mass surveillance technology effectively does away with the right to privacy of communications on the Internet altogether."
Ben Emmerson QC, **UN Special Rapporteur on counter-terrorism and human rights**

On 5 June 2013, a British newspaper, The Guardian, published the first in a series of revelations about indiscriminate mass surveillance by the USA's National Security Agency (NSA) and the UK's Government Communications Headquarters (GCHQ). Edward Snowden, a whistleblower who had worked with the NSA, provided concrete evidence of global communications surveillance programmes that monitor the internet and phone activity of hundreds of millions of people across the world.

Governments can have legitimate reasons for using communications surveillance, for example to combat crime or protect national security. However because surveillance interferes with the rights to privacy and freedom of expression, it must be done in accordance with strict criteria: surveillance must be targeted, based on reasonable suspicion, undertaken in accordance with the law, necessary to meet a legitimate aim and be conducted in a manner that is proportionate to that aim, and non-discriminatory. This means that mass surveillance that indiscriminately collects the communications of large numbers of people cannot be justified. Mass surveillance violates both the right to privacy and to freedom of expression.

This briefing presents an overview of the information that has come to light in the past two years about mass surveillance programmes run by the UK, US and other governments, as well as the key legal, policy and technological developments relating to mass surveillance and the right to privacy during this period. In this briefing, Amnesty International and Privacy International also present a 7-point plan of action to guarantee the protection of human rights in the digital age.

In the past two years, we have learned the extent of mass surveillance programmes operated chiefly by the NSA and GCHQ, with the close cooperation of their sister agencies in Australia, Canada and New Zealand - collectively known as the Five Eyes Alliance (or 'Five Eyes'). The revelations, which have been exposed by the media based on files leaked by Edward Snowden have included evidence that:

- Companies - including Facebook, Google and Microsoft - were forced to handover their customers' data under secret orders through the NSA's Prism programme;
- the NSA recorded, stored and analysed metadata related to every single telephone call and text message transmitted in Mexico, Kenya, and the Philippines;
- GCHQ and the NSA have co-opted some of the world's largest telecommunications companies to tap the transatlantic undersea cables and intercept the private communications they carry, under their respective TEMPORA and Upstream programmes;
- GCHQ and NSA hacked into the internal computer network of Gemalto, the largest manufacturer of SIM cards in the world, possibly stealing billions of encryption keys used to protect the privacy of mobile phone communications around the world.

Public opposition has grown globally. A poll commissioned by Amnesty International, which questioned 15,000 people from 13 countries across every continent, found that 71 per cent of people are strongly opposed to their governments spying on their internet and phone communications.

International and regional institutions and experts, including the UN High Commissioner for Human Rights and the Parliamentary Assembly of the Council of Europe, have expressed significant concerns about mass surveillance

programmes and warned about the danger they pose to human rights. In December 2014, the UN General Assembly adopted a second resolution on the right to privacy in the digital age, where it expressed deep concern "at the negative impact that surveillance and/or interception of communications...in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights."[7] In March 2015, the UN Human Rights Council established for the first time a permanent mandate for a Special Rapporteur on the right to privacy, a historic move that will ensure privacy issues are at the forefront of the UN's agenda for years to come.

Courts in a number of countries ruled against mass surveillance and intelligence-sharing practices. In the United Kingdom, the Investigatory Powers Tribunal ruled that, prior to the Tribunal's judgements handed down in December 2014 and February 2015, the regime governing the soliciting, receiving, storing and transmitting by UK authorities of private communications of individuals located in the UK, which have been obtained by US authorities pursuant to the Prism and Upstream programmes, contravened the European Convention on Human Rights. In the USA, a federal court of appeal ruled in May 2015 that the mass collection of US phone records was illegal.

Many of the world's largest technology companies have also spoken out against mass surveillance. In 2013, ten companies –including Apple, Facebook, Google, Microsoft, Twitter and Yahoo! – launched the Reform Global Government Surveillance Coalition, advocating for an end to bulk collection practices under the USA Patriot Act, among other legal reforms.

Several major companies took more tangible steps against surveillance, increasing the default security and encryption provided to users on their platforms and services, better protecting the privacy of internet users against indiscriminate mass surveillance.

There are also signs of limited legal reforms. For example, the USA Freedom Act, which was passed by the House of Representatives in May, attempts to end government bulk collection of US phone records.[1] However, the law would also require companies to hold, search, and analyse certain data at the request of the government, arguably expanding the statutory basis for large-scale data collection rather than ending it. Additionally, many other aspects of US surveillance remain under-regulated and unaccountable under the new law – including the mass surveillance of millions of people outside of the US. Pressure is needed to ensure that governments dismantle these extraordinarily invasive surveillance systems at home and abroad. A first step in this regard is to recognise that privacy rights are owed equally to persons abroad as to those present in one's own country.

Companies have a responsibility to respect the right to privacy online. To live up to this responsibility they should take far bolder steps to increase security on their platforms and services, so that private user data is not made freely available for harvesting by governments.

There is a rising tide of opinion against mass surveillance, but much remains at stake. Governments globally have enacted new laws granting mass surveillance powers of their own. This year has seen sweeping new surveillance powers introduced in Pakistan and France, while Denmark, Switzerland, the Netherlands and UK are set to present new intelligence bills in the near future.

Preserving privacy, and ultimately freedom of expression, will require concerted action by individuals, technologists, legal experts, civil society, international organizations, companies and governments. No single solution is sufficient; rather a combination of domestic legal reforms, strong international standards, robust privacy protecting technologies, corporate commitment to user privacy and individual action is needed.

[1] Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (USA FREEDOM Act of 2015), H.R.— 114th Congress (2015-2016).

Mass surveillance of internet and phone communications: what we learned about US and UK programmes

We now know, through the Snowden revelations, that the US and UK intelligence agencies have been operating indiscriminate mass surveillance programmes on a global scale, enabling the interception of a large proportion of the world's Internet traffic as well as the phone communications of hundreds of millions of people. These capabilities are coupled with vast intelligence-sharing practices between members of the Five Eyes Alliance, as well as with a web of intelligence agencies in dozens of countries around the world.[2] These are some of the programmes run by the NSA and GCHQ that have been revealed since 2013.

[text box starts]
Note on information about US and UK surveillance practices: The vast majority of information on mass surveillance practices by the USA and the UK in the public domain is based on documents leaked by whistleblower and former NSA analyst Edward Snowden. Documents leaked contain internal NSA and GCHQ documents. Some of the disclosures also include information about surveillance activities by other countries. Revelations about these mass surveillance practices have been published by various news organizations in several countries.

The US government has confirmed the existence of some of the programmes exposed by the revelations, such as the Prism programme, however the information in most of the revelations has not been confirmed – or denied by either the US or the UK governments. In the absence of rejection by the USA or the UK of information contained in these leaks, and the fact that the authenticity of the documents leaked by Edward Snowden has not been disputed by either of the countries, information about mass surveillance programmes from these leaks is assumed to be correct.
[text box ends]

1 - Tapping into global telecommunications networks

The NSA and GCHQ are directly intercepting transatlantic undersea internet cables in their respective Upstream and TEMPORA programmes.[3] These programmes intercept huge quantities of internet traffic, scanning and filtering every communication passing through the cables that make up the backbone of the internet. Undersea cable tapping provides UK and US intelligence agencies with unprecedented surveillance powers.

In one six-month period, GCHQ, under its OPTIC NERVE programme, intercepted 1.8 million Yahoo! video chats, capturing images, between 3 and 11 per cent of which contained "undesirable nudity", before processing them through facial recognition technology.[4]

In Canada, the Communications Security Establishment Canada (CSEC) intercepts cables and records up to 15 million downloads daily from file sharing websites like Rapidshare or Megaupload.[5] CSEC also monitors millions of emails, storing them for "days to months" as it applies analysis technology.[6]

---

[2] For further information, see Privacy International, *The Five Eyes*, online at: www.privacyinternational.org/?q=node/51 (accessed 28 May 2015)

[3] See Craig Timberg, *NSA slide shows surveillance of undersea cables*, The Washington Post, 10 July 2013, online at: www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html and Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, *GCHQ taps fibre-optic cables for secret access to world's communications*, The Guardian, 21 June 2013, online at: www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (both accessed 28 May 2015)

[4] Spencer Ackerman and James Ball, *Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ*, The Guardian, 28 February 2014, online at: www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo (accessed 28 May 2015)

[5] Ryan Gallagher and Glenn Greenwald, *Canada casts global surveillance dragnet over file downloads*, The Intercept, 18 January 2015, online at: https://firstlook.org/theintercept/2015/01/28/canada-cse-levitation-mass-surveillance/ (accessed 28 May 2015)

[6] Amber Hildebrandt, Dave Seglins, and Michael Pereir, *CSE monitors millions of Canadian emails to government*, CBC News, 25 February 2015, online at: www.cbc.ca/news/cse-monitors-millions-of-canadian-emails-to-government-1.2969687 (accessed 28 May 2015)

In New Zealand, the Government Communications Security Bureau (GCSB) uses satellite interception to capture internet and telephone data transmitted to and from the Asia Pacific region. In 2009 they upgraded their main base in Waihopai to be "full take", ensuring they had the capacity to capture all communications travelling on their networks, and sharing the raw data with the Five Eyes Alliance.[7]

2 – Accessing companies' data centres and internal systems

Nine companies including Apple, Facebook, Google, Microsoft and Yahoo! have been forced to hand over their customers' data under secret orders issued as part of the NSA's Prism programme,[8] while being gagged from publicly talking about it.[9]

The NSA and GCHQ then conspired to break into the main communications links that connect the data centres of some of these companies around the world. Under this programme, code-named MUSCULAR, millions of records are captured every day from internal Yahoo! and Google networks.[10]

Meanwhile, GCHQ targeted Belgacom, Belgium's largest telecommunications provider. The UK agency hacked internal employee computers in order to be able to grab private communications handled by the company. Belgacom has millions of customers including officials from the European Commission, the European Parliament, and the European Council.[11]

3 – Tracking the location of our mobile phones

The NSA collects nearly 5 billion records a day pertaining to the location of mobile phones around the world, under a set of programmes known collectively as CO-TRAVELLER. According to a 2012 NSA internal briefing, the organization is collecting so much locational information under the programme that the capabilities are "outpacing our ability to ingest, process and store" the data.[12]

4 – Listening into the telephone calls of an entire country

The NSA has obtained copies of every single telephone call made in entire countries. The voice interception programme, code-named MYSTIC and SOMALGET, is referred to as a "time machine" because it enables the NSA to replay recordings of any telephone call without requiring that an individual be targeted in advance for surveillance.[13] It has already been used to record all voice calls in the Bahamas and Afghanistan and to capture metadata of all voice calls in Mexico, Kenya, and the Philippines, affecting a combined population of more than 250 million people.

5 – Lobbying for surveillance laws abroad

---

[7]Ryan Gallagher And Nicky Hager, *New Zealand spies on neighbours in secret "Five Eyes global surveillance*, The Intercept, 3 April 2015, online at: https://firstlook.org/theintercept/2015/03/04/new-zealand-gcsb-surveillance-waihopai-xkeyscore/ (accessed 28 May 2015)

[8] The Guardian, *NSA Prism programme slides*, 1 November 2013, online at: www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document (accessed 28 May 2015)

[9] Leo Kelion, *Q&A: NSA's Prism internet surveillance scheme*, BBC, 1 July 2013, online at: www.bbc.co.uk/news/technology-23051248 (accessed 28 May 2015)

[10] Barton Gellman and Ashkan Soltani, *NSA infiltrates links to Yahoo, Google data centers worldwide*, *Snowden documents say*, Washington Post, 30 October 2013, online at: 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 (accessed 28 May 2015)

[11] Ryan Gallagher, *Operation Socialist: The Inside Story of How British Spies Hacked Belgium's Largest Telco*, The Intercept, 13 December 2014, online at: https://firstlook.org/theintercept/2014/12/13/belgacom-hack-gchq-inside-story/ (accessed 28 May 2015)

[12] Barton Gellman and Ashkan Soltani, *NSA tracking cellphone locations worldwide: Snowden documents show*, Washington Post, 4 December 2013, online at: www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html (accessed 28 May 2015)

[13] Barton Gellman and Ashkan Soltani, *NSA surveillance programme reaches 'into the past' to retrieve, replay phone calls*, Washington Post, 18 March 2014, online at: www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html (accessed 28 May 2015)

A team at the NSA known as the Foreign Affairs Division exists to pressure or incentivize other countries to change their laws to enable mass surveillance and co-operate with the NSA.[14] This team looks for loopholes in laws and constitutional protections that would enable foreign partner agencies to undertake mass surveillance operations that were never contemplated by the legislature.

According to Edward Snowden, Sweden, Germany and the Netherlands "received instruction from the NSA, sometimes under the guise of the US Department of Defence and other bodies, on how to degrade the legal protections of their countries' communications."[15]

GCHQ is also providing similar advice: one GCHQ document says that "[t]he Dutch have some legislative issues that they need to work through before their legal environment would allow them to operate in the way that GCHQ does. We are providing legal advice on how we have tackled some of these issues to Dutch lawyers."[16]

6 – Spreading mass surveillance

In order to acquire more information from their overseas partners, the Five Eyes provide equipment and expertise to assist partner agencies to tap undersea cables in their territories.[17] The technology enables partners to 'ingest' massive amounts of data in a manner that facilitates processing, and provides a copy of the intercepted communications to the Five Eyes. In 2011, the NSA spent a total of $91 million on these foreign cable access programmes with more than 13 overseas sites now in operation, two of which are in Germany and Denmark.[18] In Germany, the Bundesnachrichtendienst (BND) intercepts satellite and cable communications, and was reportedly sharing 220 million phone metadata records every day with the NSA.[19]

7 – Undermining encryption standards

The NSA and GCHQ have been sabotaging encryption standards, working to undermine the ability to securely communicate through their decryption programmes, Bullrun (NSA) and Edgehill (GCHQ).

A 2010 GCHQ document explained that "[f]or the past decade, NSA has lead [sic] an aggressive, multi-pronged effort to break widely used internet encryption technologies" and "insert vulnerabilities into commercial encryption systems."[20] Meanwhile, GCHQ was revealed to be exploring ways to break into the encrypted data of Facebook, Google, Microsoft's Hotmail and Yahoo!.[21] GCHQ also established a Humint [human intelligence] Operations Team, which

---

[14] Andrew Byrne, *Snowden: US spy agencies pressed EU states to ease privacy laws*, The Financial Times, 7 March 2014, online at: www.ft.com/cms/s/0/9f45bcb2-a616-11e3-8a2a-00144feab7de.html#axzz3a7iVHH6t (accessed 28 May 2015)

[15] Andrew Byrne, *Snowden: US spy agencies pressed EU states to ease privacy laws*, The Financial Times, 7 March 2014, online at: www.ft.com/cms/s/0/9f45bcb2-a616-11e3-8a2a-00144feab7de.html#axzz3a7iVHH6t (accessed 28 May 2015)

[16] Julian Borger, *GCHQ and European spy agencies worked together on mass surveillance*, The Guardian, 1 November 2013, online at: www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden (accessed 28 May 2015)

[17] Ryan Gallagher, *How secret partners expand NSA's surveillance dragnet,* The Intercept, 19 June 2014, online at: https://firstlook.org/theintercept/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/ (accessed 28 May 2015)

[18] Ryan Gallagher, *How secret partners expand NSA's surveillance dragnet,* The Intercept, 19 June 2014, online at: https://firstlook.org/theintercept/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/ (accessed 28 May 2015)

[19] Kai Biermann, *BND stores 220 million telephone data – every day*, Zeit Online, 2 February 2015, online at: www.zeit.de/digital/datenschutz/2015-02/bnd-nsa-mass-surveillance (accessed 28 May 2015)

[20] James Ball, Julian Borger and Glenn Greenwald, *Revealed: how US and UK spy agencies defeat internet privacy and security,* The Guardian, 6 September 2013, online at: www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security (accessed 28 May 2015)

[21] Nicole Perlroth, Jeff Larson and Scott Shane, *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, The New York Times, 5 September 2013, online at: www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?hp&_r=0 (accessed 28 May 2015)

according to an internal GCHQ document is "responsible for identifying, recruiting and running covert agents in the global telecommunications industry."[22]

8 – Hacking into phones and apps

The Five Eyes have built up their capabilities to infect individuals' devices with intrusive malware in order to be able to, in their words, "exploit any phone, anywhere, anytime."[23] UK and US spies have boasted that "if its [sic] on the phone, we can get it."[24] Far from deploying this tactic in exceptional circumstances only, the Five Eyes have aggressively developed these tools to infect potentially millions of computers and phones worldwide.[25] Canada's CSEC even spied on the computers and smartphones that connected Brazil's mining and energy ministry, in order to gather economic intelligence.[26] In a leaked NSA presentation, the agency commented on its own capabilities: "who knew in 1984 that [smart phones] would be Big Brother and the zombies would be paying customers?"[27]

9 – Controlling core communications infrastructure

Working in partnership with telecommunications companies, the NSA is "aggressively involved in shaping traffic" to artificially change the route of internet communications, redirecting them to flow past Five Eyes interception points.[28] When that fails, the Five Eyes secretly deploy malware into core telecommunications networks to enable them to copy traffic into the NSA's mass surveillance infrastructure. One of the ways the NSA does this is by "interdicting" shipments of computer hardware as they are delivered to customers, altering the hardware in order to ensure that they can gain access to networks "around the world."[29]

In essence, in addition to tapping the communications that cross their borders, the NSA and GCHQ are proactively trying to redirect communications traffic so that it travels past their probes and taps, allowing it to be intercepted, collected and analysed. In this way, the core infrastructure of the internet is being co-opted to feed data into the Five Eyes surveillance programmes.

10 – Stealing encryption keys

GCHQ and NSA hacked into the internal computer network of Gemalto, the largest manufacturer of SIM cards in the world, stealing billions of encryption keys used to protect the privacy of mobile phone communications around the world.[30] With these stolen encryption keys, intelligence agencies can unlock mobile communications without needing

---

[22] James Ball, Julian Borger and Glenn Greenwald, *Revealed: how US and UK spy agencies defeat internet privacy and security,* The Guardian, 6 September 2013, online at: www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security (accessed 28 May 2015)

[23] Nick Hopkins and Julian Borger, *Exclusive: NSA pays £100m in secret funding for GCHQ*, The Guardian, 1 August 2013, www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden (accessed 28 May 2015)

[24] Russell Brandom, *New NSA documents reveal massive data collection from mobile apps*, The Verge, 27 January 2014, online at: www.theverge.com/2014/1/27/5350714/new-nsa-documents-reveal-massive-data-collection-from-mobile-apps (accessed 28 May 2015)

[25] Ryan Gallagher And Glenn Greenwald*, How the NSA plan to infect millions of computers with malware*, The Intercept, 3 December 2014, https://firstlook.org/theintercept/2014/03/12/nsa-plans-infect-millions-computers-malware/ (accessed 28 May 2015)

[26] Amber Hildebrandt, Dave Seglins, and Michael Pereira, *Communication Security Establishment's cyberwarfare toolbox revealed*, CBC News, 2 April 2015, online at: www.cbc.ca/news/canada/communication-security-establishment-s-cyberwarfare-toolbox-revealed-1.3002978 (accessed 28 May 2015)

[27] Marcel Rosenbach, Laura Poitras and Holger Stark, *iSpy: How the NSA accesses smartphone data,* Der Spiegal, 9 September 2013, www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html (accessed 28 May 2015)

[28] Glenn Greenwald, *No Place to Hide: Edward Snowden, the Nsa, and the U.S. Surveillance State,* 2014, p.105.

[29] *Inside TAO: Documents Reveal Top NSA Hacking Unit*, Der Spiegel, 29 December 2013, online at: www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-3.html (accessed 28 May 2015)

[30] Jeremy Scahill and Josh Begley, *The great SIM heist: how spies stole the keys to the encryption castle*, The Intercept, 19 February 2015, https://firstlook.org/theintercept/2015/02/19/great-sim-heist/ (accessed 28 May 2015)

approval from telecom companies and sidestepping the need to get a warrant, while leaving no trace on the wireless provider's network that the communications were intercepted.

[frame/text box] International public opinion rejects mass surveillance

An international poll commissioned by Amnesty International, which questioned 15,000 people from 13 countries across every continent, found that 71 per cent of people are strongly opposed to their governments spying on their internet and phone communications. The poll was undertaken in February 2015.

Key findings of the poll include:

With regard to surveillance by own government:

- In all 13 countries covered by the poll, people did not want their own government to intercept, store and analyse their phone and internet use. On average, twice as many were against surveillance by their government (59 per cent) as those who approved (26 per cent).
- Most opposed to mass surveillance by their own government are people in Brazil (65 per cent) and Germany (69 per cent). Spain (67 per cent), where reports that the NSA tapped 60 million Spanish phone calls were met with outrage in 2013, also topped the opposition table.
- The majority of US citizens (63 per cent) are against their government's surveillance scheme compared to only 20 per cent in favour.

With regard to US mass surveillance of other countries:

- 71 per cent of respondents were strongly opposed to the United States of America monitoring their internet use.
- Strongest opposition to the USA intercepting, storing and analysing internet use came from Germany (81per cent against) and Brazil (80 per cent).
- Even in the country with least opposition, France, the majority of people still opposed US surveillance (56 per cent).
- In Australia, Canada, New Zealand and the United Kingdom – all countries with whom the USA shares the fruits of mass surveillance – more than three times as many people oppose US surveillance (70 per cent) as support it (17 per cent).

With regard to the role of companies

- 60 per cent of people think technology companies have a duty to help them secure their personal information from governments, as opposed to only 26 per cent who agree with firms providing authorities with access to data.

Experts and international bodies call mass surveillance a violation of human rights

Over the past two years, a number of prominent national, regional and international bodies and experts have pronounced mass surveillance a violation of human rights. Together, they form a substantial body of authoritative opinion on the legality of mass surveillance such as that practiced by the NSA and GCHQ.

First came a report in December 2013 by the **President's Review Board**, an expert board convened by US President Barack Obama to scrutinise the Snowden revelations. The Board condemned the NSA's mass surveillance programmes, stating that "the government should not be permitted to collect and store all mass, undigested, non-public personal information about individuals to enable future queries and data-mining for foreign intelligence purposes."[31]

The Board's view was echoed in a resolution the same month by the **UN General Assembly**, which expressed its deep concern at the negative impact that interception and collection of communications data, in particular when carried out on a mass scale, may have on the exercise of human rights.[32]

In January 2014, a report from the **Privacy and Civil Liberties Oversight Board**, an independent agency within the US government, found that the bulk collection of telephone metadata by the NSA to be unauthorized under Section 215 of the USA Patriot Act. The report also declared it to be a violation of the Electronic Communications Privacy Act and raises concerns under both the First and Fourth Amendments.[33]

The **European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee)** inquiry into the NSA surveillance programmes delivered its report in February 2014, finding that "the fight against terrorism can never be a justification for untargeted, secret, or even illegal mass surveillance programmes."[34] The LIBE Committee "takes the view that such programmes are incompatible with the principles of necessity and proportionality in a democratic society."

In July 2014, the **UN High Commissioner for Human Rights**, in a report entitled "The right to privacy in the digital age", pronounced, "The very existence of a mass surveillance programme... creates an interference with privacy."[35]

Her findings were reinforced in October 2014 by the **UN Special Rapporteur on counter-terrorism and human rights** who condemned mass surveillance by saying, "The hard truth is that the use of mass surveillance technology effectively does away with the right to privacy of communications on the Internet altogether."[36]

A second **UN General Assembly** resolution in December 2014 reiterated the sentiments of its 2013 resolution, expressing States' deep concern "at the negative impact that surveillance and/or interception of communications...in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights."[37]

The **Council of Europe's Commissioner for Human Rights** also weighed in, writing in an issue paper entitled *The rule of law on the Internet and in the wider digital world,* "it is becoming increasingly clear that secret, massive and

---

[31] *Liberty and security in a changing world: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, 12 December 2013, Recommendation 4, p.25, online at: www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (accessed 28 May 2015)

[32] UNGA Resolution 68/167: The right to privacy in the digital age, 18 December 2013, online at: www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167 (accessed 28 May 2015)

[33] Privacy and Civil Liberties Oversight Board, *Report on the telephone records programme conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*, Online at: www.documentcloud.org/documents/1008937-final-report-1-23-14.html (accessed 28 May 2015)

[34] *LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens*, online at: www.europarl.europa.eu/committees/en/libe/subject-files.html?id=20130923CDT71796 (accessed 28 May 2015)

[35] United Nations Human Rights Council, *The right to privacy in the digital age - report of the Office of the United Nations High Commissioner for Human Rights*, A/HRC/27/37, 30 June 2014, online at: www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (accessed 28 May 2015)

[36] United Nations, Promotion and protection of human rights and fundamental freedoms while countering terrorism – note by the Secretary-General, A/69/397, 23 September 2014, online at: https://firstlook.org/theintercept/document/2014/10/15/un-report-human-rights-terrorism/ (accessed 28 May 2015)

[37] United Nations, Resolution adopted by the General Assembly on 18 December 2014, 69/166. The right to privacy in the digital age, A/RES/69/166, 10 February 2015, online at: www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/69/166 (accessed 28 May 2015)

indiscriminate surveillance programmes are not in conformity with European human rights law and cannot be justified by the fight against terrorism or other important threats to national security."[38]

In April 2015, the **Parliamentary Assembly of the Council of Europe** adopted its own resolution, with perhaps the starkest condemnation of surveillance to date. The resolution stated "The surveillance practices disclosed so far endanger fundamental human rights, including the rights to privacy, freedom of information and expression, and the rights to a fair trial and freedom of religion: especially when privileged communications of lawyers and religious ministers are intercepted and when digital evidence is manipulated. These rights are cornerstones of democracy. Their infringement without adequate judicial control also jeopardizes the rule of law."[39]

Finally, and most significantly, the **UN Human Rights Council** took decisive action in adopting by consensus a March 2015 resolution that established a permanent independent expert on the right to privacy.[40] The Special Rapporteur on privacy will be appointed at the June 2015 session of the Council, and will have responsibilities which include reporting on alleged violations of the right to privacy, including those which arise "in connection with the challenges arising from new technologies."[41]

---

[38]Council of Europe Commissioner for Human Rights, *The rule of law on the Internet and in the wider digital world*, December 2014, online at: https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2734552&SecMode=1&DocId=2262340&Usage=2 (accessed 28 May 2015)

[39] Parliamentary Assembly, Resolution 2045 (2015) provisional version- mass surveillance, 21 April 2015, online at: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21692&lang=en (accessed 28 May 2015)

[40] United Nations Human Rights Council, *The right to privacy in the digital age*, A/HRC/28/L.27, 24 March 2015, online at: www.privacyinternational.org/sites/default/files/SR%20resolution.pdf (accessed 28 May 2015)

[41] United Nations Human Rights Council, *The right to privacy in the digital age*, A/HRC/28/L.27, 24 March 2015, online at: www.privacyinternational.org/sites/default/files/SR%20resolution.pdf (accessed 28 May 2015)

Judicial scrutiny of mass surveillance practices worldwide

Since June 2013, civil society organizations, companies and lawyers have launched a number of legal challenges against mass surveillance in all Five Eyes countries, as well as other countries believed to have extensive mass surveillance programmes. Notably, judgments in the UK and USA found some GCHQ and NSA practices to be unlawful. Several important cases are pending in domestic courts and the European Court of Human Rights.

The Five Eyes

[text box starts]
What is the Five Eyes Alliance?[42]
The Five Eyes Alliance is a secretive, global surveillance arrangement of States comprised of the United States National Security Agency (NSA), the United Kingdom's Government Communications Headquarters (GCHQ), Canada's Communications Security Establishment Canada (CSEC), the Australian Signals Directorate (ASD), and New Zealand's Government Communications Security Bureau (GCSB).

The alliance began in 1946; its purpose is sharing intelligence, primarily signals intelligence (SIGINT). Under the alliance's agreement, interception, collection, acquisition, analysis, and decryption is conducted by each of the State parties in their respective parts of the globe, and all intelligence information is shared by default. Their agreement is wide in scope and establishes jointly-run operations centres where operatives from multiple intelligence agencies of the Five Eyes States work alongside each other.
[text box ends]

In the **UK** in 2013, Privacy International, Amnesty International and eight other human rights organisations brought a legal challenge to UK communications surveillance practices. As a result, in February 2015, the Investigatory Powers Tribunal ruled that intelligence sharing between the USA and the UK was unlawful prior to its December 2014 and February 2015 judgments, because the rules governing the UK's access to the NSA's Prism and Upstream programmes were secret.[43]

During the legal proceedings the UK government was compelled to disclose information about the intelligence sharing relationship with the USA. While the Tribunal considered that following these disclosures the UK became compliant with Article 8 (right to privacy) of the European Convention, the claimant organisations disagree and have brought the case to the European Court of Human Rights (ECtHR). Two other cases challenging UK surveillance practices are currently pending at the ECtHR; claimants include Big Brother Watch, English PEN, the Open Rights Group and the Bureau of Investigative Journalism.[44]

Also at the **European Court of Human Rights**, in September 2014 Privacy International challenged the blanket exemption from freedom of information laws afforded to the British intelligence agency GCHQ. Privacy International was denied access to the Five Eyes Agreement, the document governing the secretive spying alliance. The application to the Court, which contends that a blanket exemption is a violation of the right to receive and impart information enshrined in Article 10 of the European Convention on Human Rights, has been adjourned pending the resolution of another case.[45]

In addition, in the **UK**, seven Internet and communications service providers from the UK, the USA, Germany, the Netherlands, South Korea and Zimbabwe, along with Privacy International, challenged the deployment by GCHQ of hacking capabilities and computer network exploitation techniques. In bringing the case, the claimants prompted the UK government to produce a Draft Code of Practice on "Equipment Interference", in itself a victory given that the use

[42] For more information, see www.privacyinternational.org/?q=node/51 (accessed 28 May 2015)

[43] The judgment can be found at www.ipt-uk.com/docs/Liberty_Ors_Judgment_6Feb15.pdf and the order at www.ipt-uk.com/docs/Liberty-Order6Feb15.pdf (both accessed 28 May 2015)

[44] See www.privacynotprism.org.uk/ and Bureau of Investigative Journalism, *A summary of the Bureau's application to the European Court of Human Rights*, 14 September 2014, online at: www.thebureauinvestigates.com/2014/09/14/a-summary-of-the-bureaus-application-to-the-european-court-of-human-rights/ (both accessed 28 May 2015)

[45] For more information, see www.privacyinternational.org/?q=node/459 (accessed 28 May 2015)

of hacking by British intelligence services was never previously formally confirmed. The case will be heard by the Investigatory Powers Tribunal in 2015.[46]

Most recently, in May 2015, the **US Court of Appeals for the Second Circuit** ruled in favour of the American Civil Liberties Union, finding that the mass collection of US phone records was not authorised by section 215 of the Patriot Act.[47] The Court noted that the "expansive development of government repositories of formerly private records would be an unprecedented contraction of the privacy expectations of all Americans," and heal that it was not authorised on the face of the legislation.[48] The Court added that such a momentous interference with privacy would have to be "preceded by substantial debate, and expressed in unmistakable language."[49]

In **Canada**, the British Columbia Council for Civil Liberties filed a lawsuit against Canada's signals intelligence agencies – the Communications Security Establishment Canada – claiming that its secret and unchecked surveillance of Canadians is unconstitutional.[50] The case is ongoing.

In **New Zealand**, the Green Party filed a complaint with the Inspector-General of Intelligence and Security (IGIS) over allegations that the surveillance agency Government Communications Security Bureau (GCSB) had been spying on New Zealanders in the Pacific. The IGIS announced in March 2015 that it would commence an inquiry, not only into the specific allegations, but into all of GCSB procedures and compliance systems.[51]

The **Australian** IGIS was also asked to investigate the actions of the Australian Signals Directorate (ASD) and its role in Five Eyes mass surveillance, but declined to proceed with an inquiry.

Challenges in other countries

A coalition of citizens and civil society organisations in the **Netherlands** challenged the intelligence sharing practices of the Dutch General Intelligence and Security Service and Dutch Military Intelligence and Security Services. In a case before the District Court of The Hague, the claimants argued that the receipt and use of foreign intelligence collected through US mass surveillance programmes should end.[52] The Court rejected the claim; this year the Dutch government will overhaul surveillance legislation.

In **Germany**, a legal challenge brought by lawyer Niko Härting against the Federal Intelligence Service (the Bundesnachrictendienst, or BND) argued that BND "strategic surveillance" of foreign email traffic was unconstitutional. The case was dismissed on procedural grounds – the Court found that Mr Härting lacked standing to bring the claim.

---

[46] for more information, see www.privacyinternational.org/?q=node/81 (accessed 28 May 2015)

[47] United States Court of Appeal for the Second Circuit, *ACLU v. Clapper*, Case 14-42, 7 May 2015, online at: http://pdfserver.amlaw.com/nlj/NSA_ca2_20150507.pdf (accessed 28 May 2015)

[48] United States Court of Appeal for the Second Circuit, *ACLU v. Clapper*, Case 14-42, 7 May 2015, online at: http://pdfserver.amlaw.com/nlj/NSA_ca2_20150507.pdf (accessed 28 May 2015), pp. 74-75.

[49] United States Court of Appeal for the Second Circuit, *ACLU v. Clapper*, Case 14-42, 7 May 2015, online at: http://pdfserver.amlaw.com/nlj/NSA_ca2_20150507.pdf (accessed 28 May 2015), pp. 74-75.

[50] British Columbia Civil Liberties Association, *CCLA Sues Canadian Government to Stop Illegal Spying*, online at: https://bccla.org/stop-illegal-spying/protect-our-privacy-case-details/ (accessed 28 May 2015)

[51] For more information, see Inspector-General of Intelligence and Security, *Inquiry into the Government Communications Security Bureau's process for determining its foreign intelligence activity*, 14 May 2015, online at: www.igis.govt.nz/announcements/ (accessed 28 May 2015)

[52] For more information, see Privacy First, *District court of The Hague wide off the mark in Citizens v. Plasterk cas*e, online at: www.privacyfirst.eu/actions/litigation/item/616-district-court-of-the-hague-wide-off-the-mark-in-citizens-v-plasterk-case.html (accessed 28 May 2015)

[spread starts]

Who has been spied on?

Governments almost always justify the need for mass surveillance on the basis of national security. However, Snowden has revealed that their capabilities and programmes end up being employed in contexts that go far beyond what is necessary to protect national security. As well as intercepting the communications of hundreds of millions of ordinary people, the NSA and GCHQ have put specific groups and individuals on their spying 'watchlists'. Amongst those who have been targeted are:

Medecins Du Monde (Doctors of the World)[53]
The organization is a well-known and highly regarded international organization that provides medical care to "those affected by war, natural disasters, disease, hunger, poverty or exclusion."[54]

"We were shocked by the allegations which amounted to a shameful waste of taxpayers' money; money that would be better spent vaccinating Syrian children against polio, rebuilding the Philippines' shattered health system or in any other place in the world where help was urgently needed at that time."
Leigh Daynes, Executive Director of Doctors of the World UK[55]

Joaquín Almunia, Vice-President of the European Commission
It was revealed the NSA and GCHQ spied on Joaquín Almunia, vice-president of the European Commission with a mandate overseeing competition policy. His mandate focuses on "fighting against cartels, preventing dominant companies from abusing their market power in any sector or any country in Europe, and maintaining a rigorous scrutiny of proposed mergers."[56]

"[The revelations] are unacceptable and deserve our strongest condemnation. This is not the type of behaviour that we expect from strategic partners, let alone from our own member states."
Pia Ahrenkilde Hansen, European Commission Spokesperson[57]

The United Nations Children's Fund (UNICEF)[58]
UNICEF is an agency of the United Nations that promotes the rights and well-being of children globally. The organization promotes girls' education, works on children's immunization and nutrition and to prevent the spread of HIV/AIDS among young people.[59]

---

[53] James Ball and Nick Hopkins, *GCHQ and NSA targeted charities, Germans, Israeli PM and EU chief*, The Guardian, 20 December 2013, online at: www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner (accessed 28 May 2015)

[54] Online at: http://doctorsoftheworld.org.uk/pages/what-we-do (accessed 28 May 2015)

[55] Leigh Daynes, *Doctors of the World: How we discovered GCHQ was spying on us*, 20 April 2015, online at: www.opendemocracy.net/digitaliberties/leigh-daynes/doctors-of-world-how-we-discovered-gchq-was-spying-on-our-operations (accessed 28 May 2015)

[56] Joaquin Almunia, Mandate, online at: http://ec.europa.eu/archives/commission_2010-2014/almunia/about/mandate/index_en.htm

57 European Commission, *Statement by Commission spokeswoman on the newspaper allegations of surveillance of Vice-President Almunia*, 20 December 2013, online at: http://europa.eu/rapid/press-release_MEMO-13-1189_en.htm?locale=en (accessed 28 May 2015)

[58] James Ball and Nick Hopkins, *GCHQ and NSA targeted charities, Germans, Israeli PM and EU chief*, 20 December 2013, online at: www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner (accessed 28 May 2015)

[59] See online at: www.unicef.org/about/who/index_introduction.html (accessed 28 May 2015)

Ahmad Muaffaq Zaidan, Al Jazeera's Pakistan bureau chief[60]

The NSA placed Ahmad Muaffiaq Zaidan, a respected investigative journalist and long-time Islamabad bureau chief for Al Jazeera, on a 'terror watchlist' based on metadata the agency collected.

"For us to be able to inform the world, we have to be able to freely contact relevant figures in the public discourse, speak with people on the ground, and gather critical information...To assert that myself, or any journalist, has any affiliation with any group on account of their contact book, phone call logs, or sources is an absurd distortion of the truth and a complete violation of the profession of journalism."
Ahmad Muaffaq Zaidan, Al Jazeera

Faisal Gill[61]

A member of the US Republican party who held a top-secret security clearance and who served in the Department of Homeland Security under President George W. Bush, he was one of several public Muslim figures in the USA who were revealed to be on a list of NSA and FBI surveillance targets.

"I don't know why…I've done everything in my life to be patriotic. I served in the Navy, served in the government, was active in my community – I've done everything that a good citizen, in my opinion, should do."
Faisal Gill

[60] Cora Currier, Glenn Greenwald, and Andrew Fishman, *US government designated prominent Al Jazeera journalist as member of Al Qaeda*, The Intercept, 8 May 2015, online at: https://firstlook.org/theintercept/2015/05/08/u-s-government-designated-prominent-al-jazeera-journalist-al-qaeda-member-put-watch-list/ (accessed 28 May 2015)

[61] Glenn Greenwald and Murtaza Hussain, *Meet the Muslim American Leader the FBI and NSA Have Been Spying On*, The Intercept, 9 July 2014, online at: https://firstlook.org/theintercept/2014/07/09/under-surveillance/ (accessed 28 May 2015)

Governments seek greater surveillance powers

Despite serious opposition, Five Eyes governments have taken limited or no steps to dismantle their mass surveillance programmes in the past two years. In the case of the UK, the government has sought to validate and extend existing unlawful practices. Elsewhere, governments have enacted new laws granting mass surveillance powers of their own. In some cases these new laws may even be an attempt to place on legal footing unlawful surveillance that governments were already conducting.

In July 2014, the **UK** government fast-tracked a new Data Retention and Investigatory Powers Act as 'emergency legislation' and rushed it through parliament in a single day. The Act was designed to revise UK data retention law in response to an April 2014 ruling by the European Court of Justice (ECJ) invalidating the 2009 Data Retention Directive. The law not only provides for ongoing blanket retention of communications data of UK residents, in direct contradiction with the ECJ ruling, it also extends the reach of UK interception powers by enabling the government to require companies based outside of the United Kingdom to comply with the UK's warrants.[62]

In addition, the Draft Communications Data Bill, or so-called "Snoopers' Charter", is likely to make a comeback in the UK after the election of a majority Conservative Government in May 2015. The controversial bill, which was defeated narrowly in 2014 and has been widely opposed by privacy and human rights groups, would further expand UK intelligence powers and provide access to bulk communications data by other agencies within the UK, such as the police.

In the United States, in contrast, there have been limited steps to reign in mass surveillance. President Obama responded to the Snowden revelations by issuing a presidential policy directive that purported to significantly limit retention and dissemination of collected data.[63] Moreover, Congress debated surveillance reform and, as of publication, the House of Representatives passed the USA Freedom Act, which attempts to end government bulk collection of US phone records.[64] However, the law would also require companies to hold, search, and analyse certain data at the request of the government, arguably expanding the statutory basis for large-scale data collection rather than ending it. Congress has also sought to significantly expand the NSA's access to personal information in the name of promoting cybersecurity. Furthermore, many other aspects of US surveillance remain under-regulated and unaccountable under the new law – including the mass surveillance of millions of people outside of the US. Additionally, the law does not sufficiently rein in the interception or collection of data other than phone records, nor does it ensure meaningful oversight by the Foreign Intelligence Surveillance Court.

The threat to privacy, and ultimately freedom of expression, has also increased as countries outside of the Five Eyes Alliance have sought to legalize stronger surveillance powers. This year has seen sweeping new surveillance powers proposed in legislation in Pakistan, France and Switzerland while in the Netherlands a new intelligence bill is expected in the near future.

In April 2015, **Pakistan**'s National Assembly approved a new cybercrime bill, drastically expanding the surveillance powers of the government. The Prevention of Electronic Crimes Bill – as it is called – now awaits vote in the Senate**.** If approved, the new law would mandate that service providers retain data about citizens' telephone and email communications for a minimum of one year.[65] Additionally, the bill would allow for the Federal Government to unilaterally share intelligence gathered from investigations with foreign intelligence agencies including the NSA, without the need for judicial authorization. The bill contains broad and insufficiently defined powers to "seize" data

---

[62] Liberty, Privacy International, Open Rights Group, Big Brother Watch, Article 19 and English PEN briefing on the fast-track Data Retention and Investigatory Powers Bill, online at: www.liberty-human-rights.org.uk/sites/default/files/Briefing%20on%20the%20Data%20Retention%20and%20Investigatory%20Powers%20Bill.pdf (accessed 28 May 2015)

[63] Presidential Policy Directive 28, Signals Intelligence Activities, 17 January 2014, online at: www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities (accessed 28 May 2015)

[64] Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (USA FREEDOM Act of 2015), H.R.— 114th Congress (2015-2016)

[65] Joint Statement from Article 19, Human Rights Watch, Privacy International, Digital Rights Foundation, and others on the Prevention of Electronic Crimes Bill 2015 Pakistan, online at: www.privacyinternational.org/sites/default/files/Prevention-of-Electronic-Crimes-Bill-International-Joint-Statement_2.pdf (accessed 28 May 2015)

(defined in the bill as making a copy of data), but does not specify the procedures to do this. By leaving this to the discretion of the Federal Government, the law fails to set out clear and accessible rules in line with international human rights standards.

In May 2015 in **France**, the lower chamber of the parliament enacted sweeping surveillance powers in a new intelligence law. The draft law, which the government says is a tool needed to prevent terrorism (without however defining this term in the legislation), allows the prime minister to authorise intrusive surveillance measures for several other broad and equally undefined goals such as "promot[ing] essential foreign policy interests", and preventing "any form of foreign interference." It is unclear what these vague terms encompass and the concern is that it could be used for reasons which often will have nothing to do with preventing wrongdoing. Most controversially, the draft law ignores the need for intelligence agencies to seek and receive a warrant authorized by a judge.

The law therefore fundamentally disregards the requirements of oversight and accountability of French intelligence agencies whilst simultaneously granting them broader and more intrusive powers. For example, for the purpose of preventing terrorism, the draft law requires internet and telecoms providers to place "black boxes" in their infrastructure to record metadata; it also allows security agents to hack into computers or mobile devices, track people's locations and spy on emails, texts and other communications from a person they think may be in contact with someone involved in suspicious activity, even if unintentionally, or because they are in the same geographic area for example, by using a device known as an IMSI Catcher which is physically deployed to intercept and decrypt SMS messages and phone calls from all mobile phones within a radius of several hundred metres.

Probably one of the most worrying aspects of this draft legislation is what it does not say. In particular, a major loophole contained in the draft law could pave the way for indiscriminate mass surveillance of all forms of internet use. Indeed, the draft law empowers the Prime Minister to authorise the interception of communications "sent or received abroad." Nothing is said about the surveillance techniques that could be used with regard to these communications, instead these techniques will be contained in a secret decree, hence bypassing Parliament. Furthermore, the bill does not say in any meaningful way what conditions will be required for such surveillance to be conducted and what procedures will need to be followed by the authorities. These are particularly critical flaws of the proposed legislation given that vast amounts of online communications transfer through servers located abroad. Such silence in the bill paves the way for arbitrary and indiscriminate surveillance against both French and non-French nationals.

In **Switzerland** two draft laws are currently under review that would provide the Swiss authorities with invasive new surveillance powers. The draft Intelligence Law will give the intelligence service powers to intercept communications running through internet cable traffic passing through Switzerland. The second law would introduce a requirement for telecommunications providers to retain metadata on all communications for 12 months.

Other European countries seem set to follow-suit. In the **Netherlands**, the government is proposing to update its law on Intelligence and Security Services to capitalize on the "explosive growth in international cable networks", as recommended by the Dessens Commission in December 2013.[66] In its formal response to the commission, the Dutch government proposed plans for the intelligence agents to have access to internet cable traffic passing through the Netherlands (much like the USA's Upstream and UK's TEMPORA programmes).[67] This would pave the way for indiscriminate interception, collection and storage of telecommunications material that is not targeted at an individual or an identifiable and distinguishable group or location, and is not based on reasonable suspicion. The Dutch government is set to present its new draft 'bulk interception' within the next few months.

Political pressure is also growing in **Finland** to establish its own mass surveillance system. In January 2015 a working group of the defence ministry proposed that new legislation should be initiated which would authorize wide powers for communications surveillance, including cross-border internet cable tapping, to the security, police and defence forces.

---

[66] Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een balans tussen bevoegdheden en waarborgen // Evaluation Intelligence and security services Act 2002. Towards a balance between powers and safeguards, 2 December 2013, from page 171 onwards (recommendation 8.5).

[67] Government Position on revising the interception system Intelligence and Security Services Act 2002, document 33820-4, 21 November 2014, online at: https://zoek.officielebekendmakingen.nl/kst-33820-4.html (accessed 28 May 2015)

US technology companies push back against mass surveillance

"People won't use technology they don't trust. Governments have put this trust at risk, and governments need to help restore it."
—Brad Smith, General Counsel and Executive Vice President, Legal and Corporate Affairs, Microsoft

Microsoft, Apple, Google, Facebook and Yahoo! were among a list of nine US technology companies to be implicated in the first wave of Snowden's disclosures.[68] The revelation that the NSA accessed their users' data, based on secret court orders through the Prism programme, sent shockwaves through the industry. In addition to cooperating with NSA data requests, further disclosures revealed the existence of secret programmes that provided the NSA with wholesale access to some companies' customer data. The Snowden revelations showed that the NSA was secretly intercepting data held by Google and Yahoo! as it passed between the companies' data centres – access that both companies claim they did not know about.[69] Further leaked documents suggested that the NSA had access to Microsoft encrypted emails and Skype video calls[70] and that the NSA had worked on programmes to be able to remotely access data on iPhone, Android and Blackberry smartphones.[71]

US companies faced a **consumer backlash as news of the leaks eroded trust and threatened revenues** – especially with customers outside of the USA. In a survey of 300 British and Canadian businesses released by PEER 1 in January 2014, 25 per cent of respondents indicated that they were moving data outside of the USA as a result of the revelations about the NSA with 81 per cent stating that they "want to know exactly where their data is being hosted."[72] A number of governments called for internet companies to keep their data on local servers rather than in the USA and encouraged the use of services that do not send data to the USA. For example, the German Interior Minister Hans-Peter Friedrich declared that, "whoever fears their communication is being intercepted in any way should use services that don't go through American servers."[73] France's Minister for the Digital Economy similarly insisted that it was now necessary to "locate data centers and servers in [French] national territory in order to better ensure data security." [74]

Looking to restore trust in their platforms and services, **major US technology firms have publicly spoken out against US mass surveillance programmes in the past two years**. A number of major companies have called on the US government to reform the laws underpinning bulk data collection and retention and disclose greater information about their mass surveillance practices.

---

[68] Barton Gellman and Laura Poitras, *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, The Washington Post, 7 June 2013, online at: www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (accessed 28 May 2015)

[69] Dominic Rushe, Spencer Ackerman and James Ball, *Reports that NSA taps into Google and Yahoo data hubs infuriate tech giants*, The Guardian, 31 October 2013, online at: www.theguardian.com/technology/2013/oct/30/google-reports-nsa-secretly-intercepts-data-links (accessed 28 May 2015)

[70] Glenn Greenwald, Ewen MacAskill, Laura Poitras, Spencer Ackerman and Dominic Rushe, *Microsoft handed the NSA access to encrypted messages*, The Guardian, 12 July 2013, online at: www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data, (accessed 28 May 2015)

[71] Marcel Rosenbach, Laura Poitras and Holger Stark, *iSpy: How the NSA accesses smartphone data,* Der Spiegal, 9 September 2013, online at: www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html (accessed 28 May 2015)

[72] Danielle Kehl, Kevin Bankston, Robyn Greene and Robert Morgus, *Surveillance Costs: the NSA's Impact on the Economy, Internet Freedom & Cybersecurity*, Open Technology Institute, July 2014, online at: www.newamerica.org/downloads/Surveilance_Costs_Final.pdf (accessed 28 May 2015), p.8.

[73] Jonah Force Hill, *The growth of data localization post-Snowden: Analysis and recommendations for U.S. policymakers and industry leaders,* 21 July 2014, online at: www.lawfareblog.com/wp-content/uploads/2014/07/Lawfare-Research-Paper-Series-Vol2No3.pdf (accessed 28 May 2015), p.6

[74] Jonah Force Hill, *The growth of data localization post-Snowden: Analysis and recommendations for U.S. policymakers and industry leaders,* 21 July 2014, online at: www.lawfareblog.com/wp-content/uploads/2014/07/Lawfare-Research-Paper-Series-Vol2No3.pdf (accessed 28 May 2015), p.6

"Revelations about government surveillance activities have shaken the trust of our users, and it is time for the United States government to act to restore the confidence of citizens around the world".

Marissa Mayer, CEO, Yahoo![75]

In the weeks following the disclosures, some companies **put pressure on the US government to increase transparency around requests made under** the **Foreign Intelligence Surveillance Act (FISA)**, the mechanism used by the NSA to gather data about foreign internet communications. By the end of June 2013, Microsoft and Google had filed a lawsuit in the USA asking to be able to reveal how many times both companies had been ordered to disclose data under FISA.[76] In February 2014, the US government allowed Microsoft, Facebook, Google and Yahoo! to disclose information for the first time about the volume of data they had been legally obliged to provide to the NSA.[77] The firms expressed that they could not disclose the precise numbers and types of requests they received.[78]

In December 2013, eight companies – Google, Microsoft, Facebook, Twitter, Yahoo!, AOL, LinkedIn, and Apple, launched **the Reform Global Government Surveillance Coalition** calling for "the world's governments to address the practices and laws regulating government surveillance of individuals and access to their information."[79] Expanding to 10 companies, with the addition of Dropbox and Evernote, the Coalition published an open letter addressed to the US Senate in November 2014 urging them to sign the USA Freedom Act into law. The coalition has also called for reforms including: "preventing government access to data without proper legal process; assuring that providers are not required to locate infrastructure within a country's border; promoting the free flow of data across borders; and avoiding conflicts among nations through robust, principled, and transparent frameworks that govern lawful requests for data across jurisdictions."[80]

In March 2015, the Coalition joined with other technology companies, privacy advocates and human rights groups in an open letter addressed to, among others, President Obama, Director of National Intelligence, James Clapper, and the Director of the NSA, Admiral Michael Rogers, calling for "a clear, strong, and effective end to bulk collection practices under the USA PATRIOT Act", the law which authorizes some of the bulk collection of metadata by the NSA.[81]

Other technology companies like Cisco, which makes core routing and switching equipment, have introduced more drastic measures to avoid NSA interception of their equipment. Instituting a new policy as a result of Snowden's

---

[75] Craig Timberg, *Major tech companies unite to call for new limits on surveillance*, The Washington Post, 9 December 2013, online at: www.washingtonpost.com/business/technology/major-tech-companies-unite-to-call-for-new-limits-on-surveillance/2013/12/08/530f0fd4-6051-11e3-bf45-61f69f54fc5f_story.html (accessed 28 May 2015)

[76] Charles Arthur. *Microsoft joins Google in demanding to disclose FISA requests*, The Guardian, 28 June 2013, online at: www.theguardian.com/technology/2013/jun/28/microsoft-google-fisa-united-states-government (accessed 28 May 2015)

[77] Spencer Ackerman and Dominic Rushe, *Microsoft, Facebook, Google and Yahoo release US surveillance requests*, The Guardian, 3 February 2014, online at: www.theguardian.com/world/2014/feb/03/microsoft-facebook-google-yahoo-fisa-surveillance-requests (accessed 28 May 2015) and Spencer Ackerman, *Tech giants reach White House deal on NSA surveillance of customer data*, The Guardian, 27 January 2014, online at: www.theguardian.com/world/2014/jan/27/tech-giants-white-house-deal-surveillance-customer-data (accessed 28 May 2015)

[78] Spencer Ackerman and Dominic Rushe, *Microsoft, Facebook, Google and Yahoo release US surveillance requests*, The Guardian, 3 February 2014, online at: www.theguardian.com/world/2014/feb/03/microsoft-facebook-google-yahoo-fisa-surveillance-requests (accessed 28 May 2015)

[79] Online at: www.reformgovernmentsurveillance.com/ (accessed 28 May 2015)

[80] Online at: http://reformgs.tumblr.com/post/102821955852/open-letter-to-the-us-senate (accessed 28 May 2015)

[81] Online at: https://static.newamerica.org/attachments/2579-nsa-coalition-letter/NSA_coalition_letter_032515_politico.pdf (accessed 28 May 2015)

disclosures, Cisco is offering sensitive customers the option to ship equipment to fake addresses in an attempt to foil the NSA.[82]

In addition to advocating for legal reform in the US, some companies have worked to increase the **default security and encryption provided to users on their platforms and services**. Apple was the first company to roll-out full-disk encryption on its mobile operating system when it launched iOS 8 in September 2014.[83] This now means all data on iPhones with iOS 8 – photos, emails, contacts, call history – is encrypted by default and inaccessible without entering the correct password. The company also uses end-to-end encryption to protect its text and video call services, iMessage and FaceTime; according to Apple, it "wouldn't be able to comply with a wiretap order even if we wanted to."[84] Google has followed suit by offering full-disk encryption for new devices loaded with its 5.0 Lollipop operating system, though few Android handset providers have yet adopted this.

Whatsapp also made the headlines by switching to provide end-to-end encryption in its instant messaging app, adopting the encryption protocol of an open-source app called TextSecure, developed to protect users' privacy. The steps by Apple, Google and Whatsapp to increase encryption since Snowden's disclosures is a sign that consumer pressure is pushing the industry towards greater privacy and security standards.

These developments provide greater protection to the privacy rights of users, however some governments have expressed concerns that stronger encryption will prevent law enforcement and intelligence agencies from accessing communications and threatened to force companies to install backdoors so that government agencies can access the data.

Law enforcement officials, including then US Attorney General Eric Holder and FBI Director James Comey, criticized Apple claiming its new encryption standard will prevent them from accessing data on iPhones for law enforcement purposes.[85] In January 2015, the British Prime Minister, David Cameron, said that if his party won the May 2015 election (which it did), the new government would introduce legislation to give the security services the power to read all messages sent over the internet.[86] He said:

"In extremis, it has been possible to read someone's letter, to listen to someone's call, to listen in on mobile communications…The question remains: are we going to allow a means of communications where it simply is not possible to do that? My answer to that question is: no, we must not."
David Cameron, UK Prime Minister, January 2015

---

[82] Darren Pauli, *Cisco posts kit to empty houses to dodge NSA chop shops*, The Register, 18 March 2015, online at: www.theregister.co.uk/2015/03/18/want_to_dodge_nsa_supply_chain_taps_ask_cisco_for_a_dead_drop/?mt=1426694168077 (accessed 28 May 2015)

[83] Cyrus Farivar, *Apple expands data encryption under IOS 8, making handover to cops moot*, ars technica, 18 September 2014, online at: http://arstechnica.com/apple/2014/09/apple-expands-data-encryption-under-ios-8-making-handover-to-cops-moot/ (accessed 28 May 2015)

[84] See www.apple.com/uk/privacy/privacy-built-in/ (accessed 28 May 2015)

[85] Julia Edwards, *U.S. attorney general criticizes Apple, Google data encryption*, Reuters, 30 September 2014, online at: www.reuters.com/article/2014/09/30/us-usa-smartphones-holder-idUSKCN0HP22P20140930 (accessed 28 May 2015)

[86] Christopher Hope, *Spies should be able to monitor all online messaging, says David Cameron*, The Telegraph, 12 January 2015, online at: www.telegraph.co.uk/technology/internet-security/11340621/Spies-should-be-able-to-monitor-all-online-messaging-says-David-Cameron.html (accessed 28 May 2015)

However, government attacks on encryption don't stand up to scrutiny. For years, the FBI recommended that people use encryption on their phones as protection against crime.[87] The overwhelming view among technology experts is that it is simply impossible to create backdoors only for "the good guys". In response to FBI criticisms of Apple, Bruce Schneier, one of the most eminent authorities on cryptography and computer security in the world wrote:

"You can't build a backdoor that only the good guys can walk through. Encryption protects against cybercriminals, industrial competitors, the Chinese secret police and the FBI. You're either vulnerable to eavesdropping by any of them, or you're secure from eavesdropping from all of them."
Bruce Schneier[88]

Reacting to David Cameron's announcement, technology writer Cory Doctorow said:

"If your Whatsapp or Google Hangouts has a deliberately introduced flaw in it, then foreign spies, criminals, crooked police…will eventually discover this vulnerability. They -- and not just the security services -- will be able to use it to intercept all of our communications. That includes things like the pictures of your kids in your bath that you send to your parents to the trade secrets you send to your co-workers."[89]

Technology companies have a very important role to play in the protection of the right to privacy. By adopting stronger encryption standards, they can ensure that the internet communications of billions of internet users are protected from intrusive surveillance and criminal attacks. Companies that fail to do so are not simply failing the trust of their users, but potentially also their responsibility to respect the right to privacy of their users. There are further steps that companies can and should undertake to ensure that their customers are better informed about the risks to their human rights; for example, they should transparently and clearly communicate the legal requirements for handing over user data to governments in every jurisdiction they operate in.

"If they are really honest, they [the security services] know that withholding encryption will penalise good people, not put a barrier up for bad people. There is no trade-off. It fundamentally doesn't work. There has to be other solutions."
Tim Cook, Apple CEO, 27 February 2014

---

[87] techdirt, *FBI Quietly Removes Recommendation To Encrypt Your Phone... As FBI Director Warns How Encryption Will Lead To Tears*, 26 March 2015, online at: www.techdirt.com/articles/20150325/17430330432/fbi-quietly-removes-recommendation-to-encrypt-your-phone-as-fbi-director-warns-how-encryption-will-lead-to-tears.shtml (accessed 28 May 2015)

[88] Bruce Schneier, *iPhone Encryption and the Return of the Crypto Wars*, 6 October 2014, online at: www.schneier.com/blog/archives/2014/10/iphone_encrypti_1.html (accessed 28 May 2015)

[89] Cory Doctorow, *What David Cameron just proposed would endanger every Briton and destroy the IT industry*, online at: http://boingboing.net/2015/01/13/what-david-cameron-just-propos.html (accessed 28 May 2015)

The Way Forward

Two years on from Edward Snowden's revelations, the vast mass surveillance apparatus operated by the US and UK intelligence agencies remains intact, and there are no indications on the horizon that they intend to halt the deployment – and indeed the expansion – of their capabilities.

Despite the information that has been revealed to the public, UK and US mass surveillance programmes remain shrouded in secrecy. Nothing illustrates this better than the UK government's policy of "neither confirm nor deny" (NCND). The NCND policy has left those who brought legal challenges against UK mass surveillance programmes with no choice but to make legal arguments about hypothetical scenarios – this has meant that actual programmes such as TEMPORA, the existence of which is clear based on the documents disclosed by Edward Snowden, are shielded from any kind of meaningful scrutiny.

Despite widespread condemnation of US and UK mass surveillance practices as violations of human rights, and courts ruling in both countries that some of these practices were illegal, it appears that no one has been held to account for authorising these intrusive programmes.

The message that the USA and UK – as well as their close partners Australia, Canada and New Zealand – are sending is clear: they will not give up their mass surveillance programmes easily. In addition, in the two years since Snowden's revelations, we have witnessed a growing number of countries, such as Egypt,[90] France[91] and Pakistan[92] seeking to increase their communications surveillance capabilities.

The threats to privacy online are increasing and with them the risks to freedom of expression. However, there has been a growing fight back with journalists exposing surveillance programmes, civil society challenging mass surveillance and companies that have strengthened privacy protections in their products. Most importantly, since the Snowden revelations, hundreds of millions of individual internet users have taken steps to protect their privacy online.[93]

This growing activism is what stands against the threat of pervasive surveillance where governments spy on everything and everyone, all the time. Technological advances will mean that surveillance technology becomes cheaper and more powerful; many of the capabilities available only to the NSA and GCHQ today will be commonplace for most countries in a matter of years. Protecting privacy and, ultimately, freedom of expression in this digital age requires action on several fronts: the widespread and unrestricted use of strong encryption and anonymity tools; domestic legal and policy reform; respect for international standards; and the protection of whistleblowers uncovering public interest information such as evidence of human rights violations.

The following 7-point plan is a call to action for civil society, technologists, experts, companies and governments who want to preserve the ideals the internet was built on: freedom, openness and accessibility. We believe that these steps are essential to guarantee the protection of human rights in our digital age.

Legal and policy reform:

1. National laws should be reformed to ensure that they comply with international human rights law and standards, including by not allowing for indiscriminate mass surveillance. Key principles that must be upheld include:

---

[90] See Amnesty International, *Egypt's plan for mass surveillance of social media an attack on internet privacy and freedom of expression*, 4 June 2014, online at www.amnesty.org/en/articles/news/2014/06/egypt-s-attack-internet-privacy-tightens-noose-freedom-expression/ and *'You are being watched!' Egypt's mass Internet surveillance*, Mada Masr, 29 September 2014, online at www.amnesty.org/en/articles/news/2014/06/egypt-s-attack-internet-privacy-tightens-noose-freedom-expression/ (both accessed 28 May 2015)

[91] See Amnesty International, *France: Halt rush towards surveillance state*, 4 May 2015, online at: www.amnesty.org/en/articles/news/2015/05/france-surveillance-state/ and Amnesty International, *France: les députés approuvent la surveillance de masse*, 5 May 2015, online at: www.amnesty.fr/Nos-campagnes/Liberte-expression/Actualites/France-les-deputes-approuvent-la-surveillance-de-masse-15061 (both accessed 28 May 2015)

[92] See Privacy International, *International human rights organisations seriously concerned about the prevention of electronic crimes bill 2015 Pakistan*, 20 April 2015, online at: www.privacyinternational.org/?q=node/566 (accessed 28 May 2015)

[93] Bill Schneier, *Over 700 Million People Taking Steps to Avoid NSA Surveillance*, 15 December 2014, online at: www.schneier.com/crypto-gram/archives/2014/1215.html#7 (accessed 28 May 2015)

a. Ensuring that surveillance of communications only happens when it is targeted, based on sufficient evidence of wrongdoing, and authorised by a strictly independent authority, such as a judge;
b. Ensuring there is transparent and independent parliamentary and judicial oversight of surveillance powers;
c. Making rules and policies about surveillance publicly available, including how governments are sharing information with other states;
d. Ensuring equal privacy protections apply for nationals and non-nationals, those within the territory of the state, and those outside it.
e. Intelligence sharing should be strictly regulated and conducted in a manner compliant with states' human rights obligations;

2. Governments should not make encryption and anonimization technologies, or their use, illegal;
3. Whistleblowers, including those working on national security issues, should be afforded strong legal protection from any form of retaliation, including by way of prosecution, for having disclosed public interest information such as on human rights violations.[94]

Corporate due diligence

In line with companies' responsibility to respect human rights:

4. Companies that own and/or operate telecommunications or internet infrastructure, including undersea telecommunications cables, and internet companies, must ensure that access to data is permitted only when it conforms to international law and standards on human rights, including by taking legal action to challenge government requests that seek bulk/wholesale access to communications traffic;
5. Major internet and telecommunications companies should lead the way in using strong encryption and other privacy technologies, including through implementing end-to-end encryption by default, where possible;
6. Internet service providers, telecommunications companies and internet companies should clearly inform users about legal requirements that they have to comply with, particularly in relation to handing over user information or content.

International standards

7. Further explore and develop means and measures needed to ensure better implementation of the international human rights standards applicable to communications surveillance, building on efforts towards identifying relevant elements that have started in the past two years, including reports by the UN Special Rapporteur on Freedom of Expression,[95] the UN High Commissioner of Human Rights the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism,[96] as well as civil society initiatives such as the Necessary and Proportionate Principles.[97]

---

[94] See The Global Principles on National Security and the Right to Information (The Tshwane Principles), online at: www.opensocietyfoundations.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles see also Parliamentary Assembly of the Council of Europe, *National security and access to information*, Resolution 1954 (2013), online at: http://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=20190&lang=en (both accessed 28 May 2015) which welcomed the adoption of the Tschwane Principles.

[95] United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, A/HRC/23/40, 17 April 2013 online at: www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (accessed 28 May 2015)

[96] General Assembly, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, A/69/397, 23 September 2014, online at: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf?OpenElement (accessed 28 May 2015)

[97] International Principles on the Application of Human Rights to Communications Surveillance, May 2014, online at: https://en.necessaryandproportionate.org/ (accessed 28 May 2015)