TWO YEARS AFTER SNOWDEN

PROTECTING HUMAN RIGHTS IN AN AGE OF MASS SURVEILLANCE
“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

EXECUTIVE SUMMARY

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 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. In 2015, the UN Human Rights Council established the first time a permanent mandate for a Special Rapporteur on the promotion and protection of all human rights for all situations or on any particular country. The mandate will ensure privacy issues are at the forefront of political discussion.

Courts in a number of countries ruled against mass surveillance and intelligence-gathering practices. In the United Kingdom, the Investigatory Powers Tribunal ruled that the methods of GCHQ had been obtained by US authorities pursuant to the USA Freedom Act of 2015, the regime governing the soliciting, receiving, storing and transmitting by UK authorities on their platforms and services, so the regime cannot be said to be unaccountable under the new law. The Guardian, 1 July 2015

In 2015, the USA Freedom Act, which was passed by the House of Representatives in May, attempted to end government bulk collection of US phone records. However, the law would also require companies to hold, search, and analyze 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. Privacy is needed to ensure that governments dismantle these extraordinarily invasive surveillance systems at home and abroad. A first step in this regard is to recognize that privacy rights are owed equally to persons abroad as to those present in one’s own country.

Several major companies took more tangible steps against surveillance, increasing the default security and encryption provided on their products 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, attempted to end government bulk collection of US phone records. However, the law would also require companies to hold, search, and analyze 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. Privacy is needed to ensure that governments dismantle these extraordinarily invasive surveillance systems at home and abroad. A first step in this regard is to recognize 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 rights of individuals. To live up to this responsibility they should take far bolder steps to increase security on their platforms and services, so that individuals user data is not frivolously 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 in the Netherlands, the US and UK are set to present new intelligence bills in the near future.

Preserving privacy, and ultimately freedom of expression, will require concerted action of individuals, technologists, legal experts, civil society, international 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.

We now know, through the Snowden revelations, that intelligence agencies have been operating indiscriminate mass surveillance programmes on a global scale, enabled by a large proportion of the world’s internet traffic as well as the 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. Taken alongside the PRISM programme run by the NSA and GCHQ, we have been revealed since 2013.

1 – Tapping into global telecommunications networks

The NSA and GCHQ are directly intercepting transatlantic undersea internet cables in their respective Upstream and TEMPORA programmes. These programmes intercept huge quantities of internet traffic, scanning and filtering every communication passing through these cables and records up to 15 million downloads of data from any sharing websites like RapidShare or Megaupload. CSE also monitors metadata of emails, storing them for “days to months” as it applies analysis technology.

In Canada, the Communications Security Establishment Canada (CSEC) intercepts cables, collecting over 5 million downloading of data from their sharing websites like RapidShare or Megaupload. The CSEC also monitors metadata of emails, storing them for “days to months” as it applies analysis technology.

We now know, through the Snowden revelations, that intelligence agencies have been operating indiscriminate mass surveillance programmes on a global scale, enabled by a large proportion of the world’s internet traffic as well as the 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. Taken alongside the PRISM programme run by the NSA and GCHQ, we have been revealed since 2013.

1 – Tapping into global telecommunications networks

The NSA and GCHQ are directly intercepting transatlantic undersea internet cables in their respective Upstream and TEMPORA programmes. These programmes intercept huge quantities of internet traffic, scanning and filtering every communication passing through these cables and records up to 15 million downloads of data from their sharing websites like RapidShare or Megaupload. The CSEC also monitors metadata of emails, storing them for “days to months” as it applies analysis technology.

In Canada, the Communications Security Establishment Canada (CSEC) intercepts cables, collecting over 5 million downloading of data from any sharing websites like RapidShare or Megaupload. CSE also monitors metadata of emails, storing them for “days to months” as it applies analysis technology.

We now know, through the Snowden revelations, that intelligence agencies have been operating indiscriminate mass surveillance programmes on a global scale, enabled by a large proportion of the world’s internet traffic as well as the 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. Taken alongside the PRISM programme run by the NSA and GCHQ, we have been revealed since 2013.

1 – Tapping into global telecommunications networks

The NSA and GCHQ are directly intercepting transatlantic undersea internet cables in their respective Upstream and TEMPORA programmes. These programmes intercept huge quantities of internet traffic, scanning and filtering every communication passing through these cables and records up to 15 million downloads of data from any sharing websites like RapidShare or Megaupload. CSE also monitors metadata of emails, storing them for “days to months” as it applies analysis technology.

In Canada, the Communications Security Establishment Canada (CSEC) intercepts cables, collecting over 5 million downloading of data from their sharing websites like RapidShare or Megaupload. The CSEC also monitors metadata of emails, storing them for “days to months” as it applies analysis technology.

We now know, through the Snowden revelations, that intelligence agencies have been operating indiscriminate mass surveillance programmes on a global scale, enabled by a large proportion of the world’s internet traffic as well as the 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. Taken alongside the PRISM programme run by the NSA and GCHQ, we have been revealed since 2013.

1 – Tapping into global telecommunications networks

The NSA and GCHQ are directly intercepting transatlantic undersea internet cables in their respective Upstream and TEMPORA programmes. These programmes intercept huge quantities of internet traffic, scanning and filtering every communication passing through these cables and records up to 15 million downloads of data from any sharing websites like RapidShare or Megaupload. CSE also monitors metadata of emails, storing them for “days to months” as it applies analysis technology.

In Canada, the Communications Security Establishment Canada (CSEC) intercepts cables, collecting over 5 million downloading of data from their sharing websites like RapidShare or Megaupload. The CSEC also monitors metadata of emails, storing them for “days to months” as it applies analysis technology.

We now know, through the Snowden revelations, that intelligence agencies have been operating indiscriminate mass surveillance programmes on a global scale, enabled by a large proportion of the world’s internet traffic as well as the 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. Taken alongside the PRISM programme run by the NSA and GCHQ, we have been revealed since 2013.

1 – Tapping into global telecommunications networks

The NSA and GCHQ are directly intercepting transatlantic undersea internet cables in their respective Upstream and TEMPORA programmes. These programmes intercept huge quantities of internet traffic, scanning and filtering every communication passing through these cables and records up to 15 million downloads of data from any sharing websites like RapidShare or Megaupload. CSE also monitors metadata of emails, storing them for “days to months” as it applies analysis technology.

In Canada, the Communications Security Establishment Canada (CSEC) intercepts cables, collecting over 5 million downloading of data from their sharing websites like RapidShare or Megaupload. The CSEC also monitors metadata of emails, storing them for “days to months” as it applies analysis technology.

We now know, through the Snowden revelations, that intelligence agencies have been operating indiscriminate mass surveillance programmes on a global scale, enabled by a large proportion of the world’s internet traffic as well as the 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. Taken alongside the PRISM programme run by the NSA and GCHQ, we have been revealed since 2013.

1 – Tapping into global telecommunications networks

The NSA and GCHQ are directly intercepting transatlantic undersea internet cables in their respective Upstream and TEMPORA programmes. These programmes intercept huge quantities of internet traffic, scanning and filtering every communication passing through these cables and records up to 15 million downloads of data from any sharing websites like RapidShare or Megaupload. CSE also monitors metadata of emails, storing them for “days to months” as it applies analysis technology.

In Canada, the Communications Security Establishment Canada (CSEC) intercepts cables, collecting over 5 million downloading of data from their sharing websites like RapidShare or Megaupload. The CSEC also monitors metadata of emails, storing them for “days to months” as it applies analysis technology.

We now know, through the Snowden revelations, that intelligence agencies have been operating indiscriminate mass surveillance programmes on a global scale, enabled by a large proportion of the world’s internet traffic as well as the 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. Taken alongside the PRISM programme run by the NSA and GCHQ, we have been revealed since 2013.

1 – Tapping into global telecommunications networks

The NSA and GCHQ are directly intercepting transatlantic undersea internet cables in their respective Upstream and TEMPORA programmes. These programmes intercept huge quantities of internet traffic, scanning and filtering every communication passing through these cables and records up to 15 million downloads of data from any sharing websites like RapidShare or Megaupload. CSE also monitors metadata of emails, storing them for “days to months” as it applies analysis technology.

In Canada, the Communications Security Establishment Canada (CSEC) intercepts cables, collecting over 5 million downloading of data from their sharing websites like RapidShare or Megaupload. The CSEC also monitors metadata of emails, storing them for “days to months” as it applies analysis technology.
In order to acquire more information from their overseas partners, the Five Eyes employ equipment and techniques that enable them to tap undersea cables in their territories. The technology enables partners to “eavesdrop” massive amounts of data in a manner that facilitates processing, and provides a cap 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. In Germany, the Bundesnachrichtendienst (BND) intercepts satellite and cables communications, and was reportedly sharing 220 million phone metadata records every day with the NSA.

7 – Undermining encryption standards

The NSA and GCHQ have been sabotaging encryption standards, working to undermine the ability to securely communicate through their encryption programmes, Bulfinn (NSA) and Edgelift (GCHQ). A 2010 GCHQ document explained that “For 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.” Meanwhile, GCHQ was revealed to be exploring ways to break into the encrypted data of Facebook, Google’s Hotmail and Yahoo.

GCHQ also established a Humint (human intelligence) Operations Team, which according to an internal GCHQ document “is responsible for identifying, recruiting and running covert agents in the global telecommunications industry.”

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.” UK and US spies have boasted that “If its [sic] on the phone, we can get it.” 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. Canada’s CSEC even spied on the computers and smartphones that connected Brazil’s mining and energy ministry, in order to gather economic intelligence. 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?”

9 – Controlling core communications

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. When that fails, the Five Eyes secretly deploy malware into core telecommunications networks to enable them to tap 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.”

In essence, in addition to tapping the telecommunications 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 internet 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. With these stolen encryption keys, intelligence agencies can unlock mobile communications without needing 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.

The poll was undertaken in February 2015. Amnesty International, which questioned 15,000 people in 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 data. 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 (81 per 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.

---


18 Kai Biermann, BND intercepts satellite and cables communications, and was reportedly sharing 220 million phone metadata records every day with the NSA.


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.”


22 Kai Biermann, BND intercepts satellite and cables communications, and was reportedly sharing 220 million phone metadata records every day with the NSA.

23 Kai Biermann, BND intercepts satellite and cables communications, and was reportedly sharing 220 million phone metadata records every day with the NSA.

24 Kai Biermann, BND intercepts satellite and cables communications, and was reportedly sharing 220 million phone metadata records every day with the NSA.


26 Kai Biermann, BND intercepts satellite and cables communications, and was reportedly sharing 220 million phone metadata records every day with the NSA.

27 Kai Biermann, BND intercepts satellite and cables communications, and was reportedly sharing 220 million phone metadata records every day with the NSA.

28 Kai Biermann, BND intercepts satellite and cables communications, and was reportedly sharing 220 million phone metadata records every day with the NSA.

29 Kai Biermann, BND intercepts satellite and cables communications, and was reportedly sharing 220 million phone metadata records every day with the NSA.

---
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 to be incompatible with the principles of privacy 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 age of surveillance", pronounced the "varied existence of mass surveillance programmes...creates an interference with privacy." Her findings were reinforced in October 2014 by the UN Special Rapporteur on counter-terrorism and human rights who condemned mass surveillance, saying, "The hard truth is that the use of mass surveillance technology effectively dozes away the right to privacy of communications on the internet altogether." A second UN General Assembly resolution in December 2014 reiterated the sentiments of its 2013 resolution, expressing "deep concern at the negative impact that surveillance and other interception and communication...in particular when carried out on a mass scale, may have on the exercise of human rights.

The Council of Europe’s Commissioner for Human Rights also weighed in, issuing an issue paper entitled The rule of law on the Internet and in the wider digital world, stating: "It is becoming increasingly clear that mass and 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.

In April 2015, the Parliamentary Assembly of the Council of Europe adopted its own resolution, with perhaps the strongest condemnation of surveillance to date. The resolution stated: "The surveillance programmes...undermine the protection of 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 principles of necessity and proportionality are ignored. These rights are cornerstones of democracy. Their infringement without adequate judicial control also jeopardizes the rule of law.

Finally, and most significantly, the UN Human Rights Council took decisive action in adopting a consensus May 2015 resolution that established a permanent independent expert on the right to privacy. 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.

Since June 2013, civil society organizations, companies and lawyers have launched a number of legal challenges against mass surveillance in all Five Eyes countries believed to have extensive mass surveillance programmes. Notably, judgments in the UK in 2014, in Germany and Switzerland all held that the challenge was not brought by GCHQ and NSA practices to be unlawful. Several important cases are pending in domestic courts and the European Court of Human Rights.

Since June 2013, civil society organizations, companies and lawyers have launched a number of legal challenges against mass surveillance in all Five Eyes countries believed to have extensive mass surveillance programmes. Notably, judgments in the UK in 2014, in Germany and Switzerland all held that the challenge was not brought by GCHQ and NSA practices to be unlawful. Several important cases are pending in domestic courts and the European Court of Human Rights. Judicial scrutiny of mass surveillance practices worldwide

A coalition of citizens and civil society organisations in the Netherlands challenged the legality of the Dutch General Intelligence and Security Service and Dutch Military Intelligence and Security Services. In a battle before the Administrative Court, the claimants argued that the receipt and use of foreign intelligence collected through US mass surveillance practices was unlawful. The Administrative Court ruled in March 2015 that the claimants could not be refused access to the Americans’ emails.

In the UK, in 2013, Privacy International, Amnesty International and eight other human rights and legal aid organizations and legal aid 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.

During the legal proceedings the UK government were compelled to disclose information about the intelligence sharing relationship with the USA. While the Tribunal concluded that following these disclosures the UK became compliant with Article 8 (right to privacy) of the European Convention, the claimants organisations and legal aid challenge to the UK’s surveillance activities at the ECHR, including claims filed in March 2015. The case was dismissed on procedural grounds – the Court found that Mr Härting lacked standing to bring the claim.

The Five Eyes Alliance is a secretive, global surveillance arrangement of States comprised of the United States, Canada, Australia, New Zealand and the United Kingdom. These States share[][]

CHALLENGES IN OTHER COUNTRIES

A coalition of citizens and civil society organisations in the Netherlands challenged the legality of the Dutch General Intelligence and Security Service and Dutch Military Intelligence and Security Services. In a battle before the Administrative Court, the claimants argued that the receipt and use of foreign intelligence collected through US mass surveillance practices was unlawful. The Administrative Court ruled in March 2015 that the claimants could not be refused access to the Americans’ emails.

In the UK, in 2013, Privacy International, Amnesty International and eight other human rights and legal aid organizations and legal aid 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.

During the legal proceedings the UK government were compelled to disclose information about the intelligence sharing relationship with the USA. While the Tribunal concluded that following these disclosures the UK became compliant with Article 8 (right to privacy) of the European Convention, the claimants organisations and legal aid challenge to the UK’s surveillance activities at the ECHR, including claims filed in March 2015. The case was dismissed on procedural grounds – the Court found that Mr Härting lacked standing to bring the claim.

The Five Eyes Alliance is a secretive, global surveillance arrangement of States comprised of the United States, Canada, Australia, New Zealand and the United Kingdom. These States share[][]

WHAT IS THE FIVE EYES ALLIANCE?

The Five Eyes Alliance is a secretive, global surveillance arrangement of States comprised of the United States, Canada, Australia, New Zealand and the United Kingdom. These States share[][]

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 believed to have extensive mass surveillance programmes. Notably, judgments in the UK in 2014, in Germany and Switzerland all held that the challenge was not brought by GCHQ and NSA practices to be unlawful. Several important cases are pending in domestic courts and the European Court of Human Rights.

Since June 2013, civil society organizations, companies and lawyers have launched a number of legal challenges against mass surveillance in all Five Eyes countries believed to have extensive mass surveillance programmes. Notably, judgments in the UK in 2014, in Germany and Switzerland all held that the challenge was not brought by GCHQ and NSA practices to be unlawful. Several important cases are pending in domestic courts and the European Court of Human Rights.

Since June 2013, civil society organizations, companies and lawyers have launched a number of legal challenges against mass surveillance in all Five Eyes countries believed to have extensive mass surveillance programmes. Notably, judgments in the UK in 2014, in Germany and Switzerland all held that the challenge was not brought by GCHQ and NSA practices to be unlawful. Several important cases are pending in domestic courts and the European Court of Human Rights.

Since June 2013, civil society organizations, companies and lawyers have launched a number of legal challenges against mass surveillance in all Five Eyes countries believed to have extensive mass surveillance programmes. Notably, judgments in the UK in 2014, in Germany and Switzerland all held that the challenge was not brought by GCHQ and NSA practices to be unlawful. Several important cases are pending in domestic courts and the European Court of Human Rights.

Since June 2013, civil society organizations, companies and lawyers have launched a number of legal challenges against mass surveillance in all Five Eyes countries believed to have extensive mass surveillance programmes. Notably, judgments in the UK in 2014, in Germany and Switzerland all held that the challenge was not brought by GCHQ and NSA practices to be unlawful. Several important cases are pending in domestic courts and the European Court of Human Rights.

Since June 2013, civil society organizations, companies and lawyers have launched a number of legal challenges against mass surveillance in all Five Eyes countries believed to have extensive mass surveillance programmes. Notably, judgments in the UK in 2014, in Germany and Switzerland all held that the challenge was not brought by GCHQ and NSA practices to be unlawful. Several important cases are pending in domestic courts and the European Court of Human Rights.
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 ‘watchlists’. Amongst those who have been targeted are:

**MEDICINS DU MONDE (DOCTORS OF THE WORLD)**

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.”

“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

**THE UNITED NATIONS CHILDREN’S FUND (UNICEF)**

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.

Ahmad Muaqfaq Zaidan, Al Jazeera’s Pakistan Bureau Chief

The NSA placed Ahmad Muaqfaq 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 Muaqfaq Zaidan, Al Jazeera

**FAISAL GUL**

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 US 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 Gul

---


13 Leigh Daynes, Doctors of the World. How we discovered GCHQ was spying on us, 20 April 2013, online at: www.opendemocracy.net/leigh-daynes/2013/04/the-uncovered-how-we-discovered-gchq-was-spying-on-our-operations (accessed 28 May 2015)

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


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


19 Glenn Greenwald and Martha Hassani, Meet the Muslim American Leader the FBI and NSA Have Been Spying On, The Intercept, 9 June 2014, online at: https://firstlook.org/theintercept/2014/06/09/NSA-FBI-FBI-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 revive 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 blanketed retention of communications data of UK residents, in direct contradiction with the ECJ rulings, 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.63

In addition, the Draft Communications Data Bill, or so-called “Snatchers’ 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.64

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 restrict the government’s collection of data.65 Moreover, Congress debated surveillance reform and, as publication of the House of Representatives Intelligence Committee report, the NSA, without the need for judicial authorization. The bill contains broad and insufficiently defined powers to “seize” data (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 new surveillance powers in a new intelligence law. The draft law, which the government says is a tool needed to prevent terrorism (without clearly defining this term in the legislation), allows the prime minister to authorize intrusive surveillance measures for several other broad and equally undefined goals such as “promoting” 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.66

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. Instead, the draft law empowers the Prime Minister to authorise the interception of communications “sight 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 pass 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 would 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 Dossiers Commission in December 2013.67 In its formal response to the commission, the Dutch government proposed plans for the intelligence agencies to have access to internet cable traffic passing through the Netherlands (much like the USA’s Upstream and UK’s TEMPORA programmes).68 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’ in 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 authorise wide powers for communications surveillance, including cross-border internet cable tapping, to the security, police and defence forces.

People don’t use technology because they want to know exactly where their data is being housed.88 A number of governments called on tech companies to allow them to access communication data on local servers rather than in the USA and encouraged the use of services that do not send data to the USA.89 This included Germany’s Prime Minister Angela Merkel, who declared that, whereas her country’s communication is being intercepted in any way should use services that do not go through American servers.90 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.”91

Revealing positions 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.92

US TECHNOLOGY COMPANIES PUSH BACK AGAINST MASS SURVEILLANCE

Okay, here is the plain text representation of the document:

88 Bruce Schneier, iPhone Encryption and the Return of the Crypto Wars (accessed 28 May 2015)
89 Cory Doctorow, “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 “just do not trust the security services with all of our communications. That includes things like the pictures of your kids in your bath... secrets you send to your co-workers.” (accessed 28 May 2015)

20 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 government surveillance, criminal and criminal attacks. Companies that fail to do so do not simply flout 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, by providing transparency and clearly communicating the legal requirements for holding user data to governments in every jurisdiction they operate in.

36 Reactions 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 just do not trust the security services with all of our communications. That includes things like the pictures of your kids in your bath – secrets you send to your co-workers.”

20 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 government surveillance, criminal and criminal attacks. Companies that fail to do so do not simply flout 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, by providing transparency and clearly communicating the legal requirements for holding user data to governments in every jurisdiction they operate in.

36 Reactions 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 just do not trust the security services with all of our communications. That includes things like the pictures of your kids in your bath – secrets you send to your co-workers.”

20 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 government surveillance, criminal and criminal attacks. Companies that fail to do so do not simply flout 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, by providing transparency and clearly communicating the legal requirements for holding user data to governments in every jurisdiction they operate in.

36 Reactions 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 just do not trust the security services with all of our communications. That includes things like the pictures of your kids in your bath – secrets you send to your co-workers.”

20 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 government surveillance, criminal and criminal attacks. Companies that fail to do so do not simply flout 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, by providing transparency and clearly communicating the legal requirements for holding user data to governments in every jurisdiction they operate in.

36 Reactions 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 just do not trust the security services with all of our communications. That includes things like the pictures of your kids in your bath – secrets you send to your co-workers.”

20 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 government surveillance, criminal and criminal attacks. Companies that fail to do so do not simply flout 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, by providing transparency and clearly communicating the legal requirements for holding user data to governments in every jurisdiction they operate in.

36 Reactions 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 just do not trust the security services with all of our communications. That includes things like the pictures of your kids in your bath – secrets you send to your co-workers.”

20 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 government surveillance, criminal and criminal attacks. Companies that fail to do so do not simply flout 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, by providing transparency and clearly communicating the legal requirements for holding user data to governments in every jurisdiction they operate in.

36 Reactions 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 just do not trust the security services with all of our communications. That includes things like the pictures of your kids in your bath – secrets you send to your co-workers.”

20 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 government surveillance, criminal and criminal attacks. Companies that fail to do so do not simply flout 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, by providing transparency and clearly communicating the legal requirements for holding user data to governments in every jurisdiction they operate in.

36 Reactions 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 just do not trust the security services with all of our communications. That includes things like the pictures of your kids in your bath – secrets you send to your co-workers.”

20 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 government surveillance, criminal and criminal attacks. Companies that fail to do so do not simply flout 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, by providing transparency and clearly communicating the legal requirements for holding user data to governments in every jurisdiction they operate in.
Two years on from Edward Snowden’s revelations, the vast mass surveillance apparatus operated by the US and UK intelligence agencies remains 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 TEMORA, the hypothetical scenarios – this has meant that actual programmes such as TEMPORA, the government’s policy of “neither confirm nor deny” of human rights violations.

There are no indications on the horizon 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:
   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 anonymisation 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.96

CORPORATE DUE DILIGENCE

In line with companies’ responsibility to respect human rights:

4. Companies that own 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, wherever 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.97 The UN High Commissioner of Human Rights the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, as well as civil society initiatives such as the Necessary and Proportionate Principles.98


© JASON REED/Reuters/Corbis

© HOANG DINH NAM/AFP/Getty Images

© HOANG DINH NAM/AFP/Getty Images
Privacy International investigates the secret world of government surveillance and exposes the companies enabling it. We litigate to ensure that surveillance is consistent with the rule of law. We advocate for strong national, regional, and international laws that protect privacy. We conduct research to catalyse policy change. We raise awareness about technologies and laws that place privacy at risk, to ensure that the public is informed and engaged.

PRIVACYINTERNATIONAL.ORG
62 Britton Street, London,
United Kingdom, EC1M 5UY GB

Amnesty International is a global movement of more than 7 million people who campaign for a world where human rights are enjoyed by all.

Our vision is for every person to enjoy all the rights enshrined in the Universal Declaration of Human Rights and other international human rights standards.

We are independent of any government, political ideology, economic interest or religion and are funded mainly by our membership and public donations.

AMNESTY.ORG
Amnesty International, International Secretariat,
Pole Bretonnière House, 3 Easton Street,
London WC1X 0DW, United Kingdom
Index: ACT/30/1795/2015, English, June 2015