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 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." In March 2015, the UN Human Rights Council established the first time a permanent mandate for a Special Rapporteur on the Right to Privacy, a historic development 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-gathering practices. In the United Kingdom, the Investigatory Powers Tribunal ruled that GCHQ’s mass surveillance programmes 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 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 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. 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. 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 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 their users. To give up to the privacy rights they should take far bolder steps to increase security on their platforms and services, so that data user upload, not 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 now 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 and companies and governments. No 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.

Not a law on information about US and UK surveillance practices. The vast majority of information on mass surveillance practices by the USA and the UK in this paper is based on documents leaked by whistle-blower and former NSA analyst Edward Snowden. Documents leaked contain internal NSA and GCHQ documents. Some of the documents are reported to be from various news organizations in several countries.

The US government has confirmed the existence of some of the programmes exposed by the documents, such as the Prism programme, however the information in the revelations has not been confirmed—only that the US or the UK governments. In the absence of rejection by the US or the UK government 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.

We now know, through the Snowden revelations, that surveillance agencies have been operating indiscriminate mass surveillance programmes on a global scale. This is enabled, in part, 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-gathering practices between members of the Five Eyes Alliance, as well as with a web of intelligence agencies in dozens of countries around the world. At the heart of some of these programmes run by the NSA and GCHQ that 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 TEMPORARY programmes. These programmes intercept huge quantities of internet traffic, scanning and filtering every communication passing through them along the backbone of the internet. Undersea cable tapping provides them with unprecedented surveillance powers.

In an October six-month period, GCHQ, under its OPTIC NERVE programme, intercepted 1.8 billion Yahoo video chats, capturing images, that telegrams up to 5 per cent of which contained “undeniable nudity,” before processing them through facial recognition technology.

In Canada, the Communications Security Establishment Canada (CSEC) intercepts and analyzes nearly 5 million downloads daily from this sharing websites like RapidShare or Megaupload. The CSEC also monitors more than 100 phone numbers for “days to months” as it applies analysis technology.

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, and then 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.

2 – Accessing companies’ data: cloud services 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, while being gagged from publicly talking about it.

The NSA and GCHQ then broke to block the main telecommunications links that connect the data centres of some of these companies around the world. Under this programme, code-named MUSCULAR, hundreds of millions of records are captured every day from internet! Yahoo! and Google networks.

Meanwhile, GCHQ targeted Belgacom, the largest internet telecommunication provider. The UK agency hacked internet employee computers in order to be able to grab private communications handled by the company. Belgacom has millions of customers including officials of the European Commission, the European Parliament, and the European Council.

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 system known collectively as CO-TRAVELLER. According to a 2012 NSA internal briefing, the NSA government’s interception of phone calls made over mobile phones worldwide.

The NSA and GCHQ are directly intercepting transatlantic undersea internet cables in their respective Upstream and TEMPORARY programmes. These programmes intercept huge quantities of internet traffic, scanning and filtering every communication passing through them along the backbone of the internet. Undersea cable tapping provides them with unprecedented surveillance powers.

In an October six-month period, GCHQ, under its OPTIC NERVE programme, intercepted 1.8 billion Yahoo video chats, capturing images, that telegrams up to 5 per cent of which contained “undeniable nudity,” before processing them through facial recognition technology.

In Canada, the Communications Security Establishment Canada (CSEC) intercepts and analyzes nearly 5 million downloads daily from this sharing websites like RapidShare or Megaupload. The CSEC also monitors more than 100 phone numbers for “days to months” as it applies analysis technology.

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, and then 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.

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 system known collectively as CO-TRAVELLER. According to a 2012 NSA internal briefing, the NSA government’s interception of phone calls made over mobile phones worldwide.

The NSA and GCHQ are directly intercepting transatlantic undersea internet cables in their respective Upstream and TEMPORARY programmes. These programmes intercept huge quantities of internet traffic, scanning and filtering every communication passing through them along the backbone of the internet. Undersea cable tapping provides them with unprecedented surveillance powers.

In an October six-month period, GCHQ, under its OPTIC NERVE programme, intercepted 1.8 billion Yahoo video chats, capturing images, that telegrams up to 5 per cent of which contained “undeniable nudity,” before processing them through facial recognition technology.

In Canada, the Communications Security Establishment Canada (CSEC) intercepts and analyzes nearly 5 million downloads daily from this sharing websites like RapidShare or Megaupload. The CSEC also monitors more than 100 phone numbers for “days to months” as it applies analysis technology.

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, and then 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.

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 system known collectively as CO-TRAVELLER. According to a 2012 NSA internal briefing, the NSA government’s interception of phone calls made over mobile phones worldwide.

The NSA and GCHQ are directly intercepting transatlantic undersea internet cables in their respective Upstream and TEMPORARY programmes. These programmes intercept huge quantities of internet traffic, scanning and filtering every communication passing through them along the backbone of the internet. Undersea cable tapping provides them with unprecedented surveillance powers.

In an October six-month period, GCHQ, under its OPTIC NERVE programme, intercepted 1.8 billion Yahoo video chats, capturing images, that telegrams up to 5 per cent of which contained “undeniable nudity,” before processing them through facial recognition technology.

In Canada, the Communications Security Establishment Canada (CSEC) intercepts and analyzes nearly 5 million downloads daily from this sharing websites like RapidShare or Megaupload. The CSEC also monitors more than 100 phone numbers for “days to months” as it applies analysis technology.

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, and then 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.

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 system known collectively as CO-TRAVELLER. According to a 2012 NSA internal briefing, the NSA government’s interception of phone calls made over mobile phones worldwide.

The NSA and GCHQ are directly intercepting transatlantic undersea internet cables in their respective Upstream and TEMPORARY programmes. These programmes intercept huge quantities of internet traffic, scanning and filtering every communication passing through them along the backbone of the internet. Undersea cable tapping provides them with unprecedented surveillance powers.

In an October six-month period, GCHQ, under its OPTIC NERVE programme, intercepted 1.8 billion Yahoo video chats, capturing images, that telegrams up to 5 per cent of which contained “undeniable nudity,” before processing them through facial recognition technology.

In Canada, the Communications Security Establishment Canada (CSEC) intercepts and analyzes nearly 5 million downloads daily from this sharing websites like RapidShare or Megaupload. The CSEC also monitors more than 100 phone numbers for “days to months” as it applies analysis technology.

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, and then 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.
In order to acquire more information from their overseas partners, the Five Eyes provide equipment to help their spy partners tap into transatlantic cables and communications, and are reportedly sharing 220 million phone metadata records each day with the NSA.14

9 – Controlling core communications

The NSA and GCHQ have been sabotaging encryption standards, working to undermine the ability to securely communicate through their encryption programmes.15

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.16

With these stolen encryption keys, intelligence agencies can unlock mobile communications without needing approval from telecom companies and subverting the need to get a warrant, while leaving no trace on the wireless provider’s network that the communications were intercepted.17

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 and analyze their phone and internet communications. The largest opposition was recorded in Italy (80 percent) and Brazil (80 percent).
  - Even in the country with least opposition, France, the majority of people opposed US surveillance (55 percent).
  - Most opposed to mass surveillance by their own government are people in Brazil (65 percent) and Germany (65 percent). Spain (67 percent), 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 percent) are against their government’s surveillance scheme compared to only 20 percent in favour.

With regard to US mass surveillance of other countries:

- 71 percent of respondents were strongly opposed to the United States of America monitoring their internet use.
- Strongest opposition to the USA intercepting, storing and analyzing internet use came from Germany (81 percent against) and Brazil (80 percent).
- Even in the country with least opposition, France, the majority of people opposed US surveillance (55 percent).
- Most opposed to mass surveillance by their own government are people in Brazil (65 percent) and Germany (65 percent). Spain (67 percent), 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 percent) are against their government’s surveillance scheme compared to only 20 percent in favour.

With regard to the role of companies:

- 60 percent of people think technology companies have a duty to help them secure their personal information from governments, opposed to only 12 percent who agree with firms providing authorities with access to data.

© RADiUS-TWC

JUNE 2015

JUNE 2015 TWO YEARS AFTER SNOWDEN JUNE 2015

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 percent of people are strongly opposed to their governments spying on their internet and phone communications. The poll was undertaken in February 2015.

22 Nick Hopkins and Julian Borger, Century: NSA pays £100m in secret funding for GCHQ, The Guardian, 1 August 2013, online at: www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-secret-funding (accessed 28 May 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 and analyze their phone and internet communications. The largest opposition was recorded in Italy (80 percent) and Brazil (80 percent).
  - Even in the country with least opposition, France, the majority of people opposed US surveillance (55 percent).
  - Most opposed to mass surveillance by their own government are people in Brazil (65 percent) and Germany (65 percent). Spain (67 percent), 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 percent) are against their government’s surveillance scheme compared to only 20 percent in favour.

With regard to US mass surveillance of other countries:

- 71 percent of respondents were strongly opposed to the United States of America monitoring their internet use.
- Strongest opposition to the USA intercepting, storing and analyzing internet use came from Germany (81 percent against) and Brazil (80 percent).
- Even in the country with least opposition, France, the majority of people opposed US surveillance (55 percent).
- Most opposed to mass surveillance by their own government are people in Brazil (65 percent) and Germany (65 percent). Spain (67 percent), 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 percent) are against their government’s surveillance scheme compared to only 20 percent in favour.

With regard to the role of companies:

- 60 percent of people think technology companies have a duty to help them secure their personal information from governments, opposed to only 12 percent 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 prospered conclusions that such programs 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.

Her findings were reinforced in October 2014 by the UN Special Rapporteur on counter-terrorism and human rights who condemned mass surveillance programs saying: "The hard truth is that use of mass surveillance technology effectively does away with 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/or interception of communications...in particular when carried out on a mass scale, may have on the exercise of human rights.

The resolution stated: "The surveillance programmes...coupled with the underlying 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 principled judicial oversight of lawyers and religious ministers are intercepted and when digital evidence is manipulated. These rights are cornerstones of democracy. Their injunction without adequate judicial control also jeopardizes the rule of law."

Finally, and most significantly, the UN Human Rights Co-operation Council, in December 2014, adopted a 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 relating to new technologies."

The case is ongoing.

What is the Five Eyes Alliance?

The Five Eyes Alliance is a secretive, global surveillance arrangement of States comprised of the United States, the United Kingdom, Australia, New Zealand and Canada (the "Five Eyes").

Their agreement is wide in scope and lacks standing, given that the Five Eyes are not parties to the European Convention on 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 spying ‘watchlists’. Amongst those who have been targeted are:

MEDECINS 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

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.”

“They 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 Ahrenklöf Hansen, European Commission Spokesperson

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 provides girls’ education, works on children’s immunization and nutrition and to prevent the spread of HIV/AIDS among young people.

Ahmad Muwaffaq Zaidan, Al Jazeera’s Pakistan Bureau Chief

The NSA placed Ahmad Muwaffaq 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 Muwaffaq Zaidan, Al Jazeera

Faisal Gill

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

## UnfollowMe

STOP À LA SURVEILLANCE DE MASSE

© Amnesty International


[9] Leigh Daynes, Doctors of the World. How we discovered GCHQ was spying on us. 20 April 2013, online at: www.opendemocracy.net/digitaliberties/leigh-daynes/doctors-of-the-world-how-we-discovered-gchq-was-spying-on-us-operation (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 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.12

In addition, the Draft Communications Data Bill, 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 curtail the government’s collection of online communications data.13 Moreover, Congress debated surveillance reform and, in direct contradiction with the ECJ ruling, it also extended the reach of UK interception powers and provide access to bulk communications data by other agencies within the UK, such as the police.

The threat to privacy, and ultimately freedom of expression, has also increased as countries outside of the Five Eyes Alliance have sought to legislate 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 cyber 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.14 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 (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 terror (without even defining this term in the legislation), allows the prime minister to authorize intrusive surveillance measures for several other forms of internet use. Indeed, the draft law could pave the way for indiscriminate mass surveillance of all forms of internet use.15

In Switzerland, the second law would introduce wide powers for communications surveillance, including cross-border internet cable tapping, 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 has set to present its new draft “bulk interception” within the next few months. The bill 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 capitalise on the “explosive growth in international cable networks”, as recommended by the Deens Commission in December 2013.16 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).17 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 defense forces.

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 miles.

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 telecom 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 miles.

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 “sверt 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.

Further, 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 capitalise on the “explosive growth in international cable networks”, as recommended by the Deens Commission in December 2013. 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). 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 defense forces.

US TECHNOLOGY COMPANIES PUSH BACK AGAINST MASS SURVEILLANCE

“People won’t use technology they think government will control, learn how to use, and governments need to help restore it.”

Brad Smith, General Counsel and Executive Vice President, Microsoft Corporation

Microsoft, Apple, Google, Facebook and Yahoo! were among a list of nine US technology companies to be implicated in the first wave of NSA disclosures. The revelation that the NSA had accessed their users’ data, based on secret court orders through the Prism program, was met with shock and anger throughout the industry. In addition to cooperating with the US government, some of these companies revealed the existence of secret programs that provided the NSA with wholesale access to data from Microsoft and Yahoo! servers. 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 had been working to eliminate. Further leaked documents suggested that the NSA had access to Microsoft encrypted emails and Skype videos. Further, the NSA had worked on programmes to be able to remotely access data on Apple, Android and BlackBerry smartphones.

US companies faced a consumer backlash on news of the leaks eroding trust and threatened revenues – especially with customers outside of the USA. In a survey, Canadian businesses released by PEER 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.”

A number of governments called for internet companies to encrypt data on local servers rather than in the USA and encouraged the use of services that did not send data to the US. In his book, The German Interior Minister Hans-Peter Friedrich declared that, “whether their communication is being intercepted in any way should use services that don’t go through American servers.”

In May 2014, after it was revealed that the NSA was harvesting Bulk Data that included information from the Internet Economy similarly insisted that it was now necessary to “locate data centers and servers in (French) hands in order to better ensure data security.”

“Restless 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!

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 intelligence. In response to the NSA’s activities, Facebook, Google and Microsoft had filed a lawsuit in January 2014 to compel the US government to release how many times both companies had been ordered to disclose data under FISA. In February 2014, the US court of appeals in San Francisco, allowed Facebook, Google and Yahoo! to disclose information about the type and volume of data they had been legally obliged to provide to the NSA. The FISA court issued an order declaring that they could not disclose the precise number and types of requests they received.

In December 2013, eight companies – Google, Microsoft, Facebook, Twitter, Yahoo!, AOL, LinkedIn, and Apple, launched the Reform Government Global Surveillance Coalition calling for “the world’s governments to address the practices and laws regulating government surveillance of individuals and access to their information.”

In March 2014, the Coalition 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 framework for surveillance practices under the USA PATRIOT ACT”, the law which authorizes some of the bulk collection.

Other technology companies like Cisco, which makes core routing and switching equipment, have introduced more drastic measures to avoid NSA interception of their data. In fact, a new policy as a result of Snowden’s disclosures, Cisco is offering sensitive customers a way to request fake addresses in an attempt to foil the NSA.

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.

This new 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 any warrant order if it had iOS 8.”

Google has followed suit by offering full-disk encryption for new devices loaded with its OS, which means 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 from governments and 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

“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 have access to all your communications. That includes things like the pictures of your kid’s bath that you send to your parents to the intimate secrets you send to your co-workers.”

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 both foreign and criminal attacks. Companies that fail to do so are 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 knowing everything is a delusion. They know that the government has to 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

88 Bruce Schneier, “If you open an iPhone, it wouldn’t be able to comply with any warrant order if it had iOS 8.”

89 “If your WhatsApp or Google Hangouts has a deliberately introduced flaw in it, then foreign spies, criminals, crooked police… will eventually discover this vulnerability.” 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 both foreign and criminal attacks. Companies that fail to do so are 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 knowing everything is a delusion. They know that the government has to 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
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 practices 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 UK and US 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 messages 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,16 France17 and Pakistan18 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.19

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 those 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.

2. Governments should not make technology illegal; encryption and anonymisation technologies, or their use, illegal; intelligence sharing should be strictly regulated and conducted in a manner compliant with states’ human rights obligations;

3. Governments should not make access to encryption and anonymisation technologies, or their use, illegal;

4. 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 human rights violations.20

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, 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, 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.21
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,
Pete Benenson House, 1 Easton Street,
London WC1X 0DW, United Kingdom
Index: ACT-30/1795/2015, Eighth, June 2015