Q&A: #UnfollowMe campaign against mass surveillance

Why is Amnesty International launching a global campaign against mass surveillance?

The Internet has revolutionized the way we communicate. Every day, three billion Internet users connect to the web to publish, share and access billions of pieces of information and communicate with each other instantaneously across the world. But it also allows governments to record and store all this information, giving them unprecedented knowledge about what we do, think and say.

Everyone who uses the internet today is at risk of having their communications monitored by their government and in some cases, by foreign governments.

As everyday appliances, from TVs and watches to fridges and cars become connected to the Internet, governments will have access to data about everything we do. As computers become more powerful and algorithms become more intelligent, so will governments' ability to make assumptions about us based on our actions, from large-scale profiling to predictive analysis.

If we don't act now, we risk living in societies where privacy doesn't exist.

Why should I care about mass surveillance if I have nothing to hide?

The question should be: if I have done nothing wrong, why is my privacy being violated?

Ordinarily, governments conduct targeted surveillance - the monitoring of a person's communications, actions or movements. Governments can only lawfully conduct surveillance if it is targeted at a person or a group for specified legitimate reasons. To do this, the authorities would obtain permission from a judge, for example, to monitor the phone or internet use of a target person or group they suspect of criminal activities.

If surveillance takes place on a widespread indiscriminate basis, with people's communications monitored without reasonable suspicion that they are engaged in criminal activity, then the assumption is that everyone is potentially guilty until proven innocent.

A society that respects freedom and the rule of law must respect people's privacy. We would never accept governments installing voice recorders and CCTV cameras in our homes, opening every letter we send, recording every conversation we have with a friend over a coffee and following us wherever we go. Yet this is the physical-world equivalent of online mass surveillance.

What is the extent of mass surveillance today?

According to US government data leaked by US whistle-blower Edward Snowden in 2013 governments are collecting, storing and analysing hundreds of millions of people's private communications in secret and with little – if any – oversight and accountability.

Edward Snowden provided evidence of mass surveillance programmes operated by the UK and US in alliance with their partners Canada, Australia and New Zealand – the Five Eyes alliance. These programs unlawfully and indiscriminately monitor the personal emails, phone calls and web traffic of ordinary people from across the world. .

What should governments do?

Amnesty International is asking governments to ban mass surveillance programmes. All countries should have strong legal safeguards to protect people against unlawful interception of their communications and their private lives.

Surveillance should take place only when it is absolutely necessary, based on sufficient evidence of wrongdoing, and authorised by a strictly independent authority, such as a judge.

Sign Amnesty International's petition here [link].

How does mass surveillance violate human rights?

Everyone has the right to private life free from government intrusion. Today, security agencies can use surveillance to intrude deep into our most intimate moments, following our emails, our internet activity and where we go.

International human rights law protect the rights to privacy and freedom of expression – states have a legal obligation to protect them. For example, article 17 of the International Covenant on Civil and Political Rights protects people from "arbitrary or unlawful interference with [their] privacy, family, home or correspondence".

International law allows governments to undertake actions that interfere with these rights in some limited circumstances, with legitimate communications surveillance being one of them. Any interference that is not in accordance with states' obligations is a violation of human rights.

We also know that some governments are starting to import the latest surveillance technology and using it to repress political opposition and people fighting for human rights. The technology for undertaking such surveillance is getting cheaper and is widely available to any government to buy.

In some countries, private data is used to target journalists, persecute activists, profile and disciminate against minorties and crack down on free speech. For example, in Bahrain, electronic surveillance has been used to target human rights activists and Ethiopia has targetted activists and journalists in Ethiopia and abroad.

Am I under surveillance?

If you use the internet or a mobile phone, the answer is probably 'yes'.

Secret Government surveillance Programmes like Prism and Upstream (run by the NSA) and Tempora (run by GCHQ) are believed to spy on you both by obtaining data from Google, Microsoft, Facebook and other major Internet companies, and by directly tapping into fibre-optic cables that carry global internet communications. The breath-taking scope of these programmes and the way in which global electronic communications are routed mean that people in nearly every country on earth can be spied on.

For these programmes you are just another phone number, email, computer or IP address that is being

swept up into their data centres.

Many other countries around the world are believed to run smaller mass surveillance programs, monitoring communications at a domestic level.

What happens to my data?

Your data can be intercepted through your mobile network, internet service provider or data cables running the internet in your country or even the undersea fibre optic cables that transport global internet traffic. It is then stored in large data centres.

US and UK security agencies NSA and GCHQ are believed to have some of the largest surveillance data centres in the world. The data can then be searched and analysed by computer algorithms and is made available to security agencies from Australia, Canada and New Zealand through X-Keyscore, a powerful database of billions of private records.

In addition to the Five Eyes, the NSA has other partners with which it has more restricted intelligence-sharing. Some of the coalitions are:

The 9 Eyes: adding to the Five Eyes Denmark, France, the Netherlands and Norway

The 14 Eyes: including Belgium, Germany, Italy, Spain and Sweden

The 41 Eyes: including the 14 Eyes and the allied coalition in Afghanistan

For more information see Privacy International https://www.privacyinternational.org/?q=node/51

Isn't mass surveillance necessary to stop terrorists?

There is no evidence that mass surveillance helps to prevent terrorism. Indeed, it may hinder efforts to identify terrorist activities by overloading security agents with haystacks of unprocessed data.

Mass surveillance increases the risk that intelligence and law enforcement agencies will miss real, credible threats as they are distracted by false positives. Intelligence comes out of mass surveillance programmes like a firehose - and you can't get a sip from a fire hose.

Governments already had more than adequate means for legitimate law enforcement and intelligence gathering purpose. The fact is they are gathering information that they couldn't have dreamed of a decade ago and they will always tell us they need more. There need to be limitations set to ensure that surveillance is carried out only when there is a legitimate legal basis to do so and using the least intrusive means possible.

When is surveillance legal?

Some surveillance is patently unlawful even under domestic law, for example when it happens with no lawful authority. Surveillance powers may be authorised by domestic legal frameworks. However, surveillance that looks legal on the surface is not necessarily lawful under international law. States have human rights obligations under international law and their domestic legal systems. Surveillance that is not

compatible with human rights is unlawful under international law and under most domestic legal systems.

Surveillance of communications interferes with privacy and freedom of expression, rights found in the Universal Declaration of Human Rights and guaranteed by international human rights law. Surveillance is only lawful in the following circumstances:

- It is **authorised by law**; i.e. it is done according to clear laws and policies that are publically available;
- It is **authorised by a warrant** issued by an independent authority, such as a judge;
- It is used to achieve a **legitimate purpose**, e.g. in the context for a criminal investigation or national security purposes;
- **targeted** at an individual, a defined group of individuals or a specific location that is directly relevant to the achievement of a legitimate aim;
- It is **necessary**, i.e. surveillance is needed to achieve a legitimate purpose such as investigating and preventing crime
- It is **proportionate**; i.e. the extent of the surveillance is proportional to the (legitimate) purpose for which it is conducted and is balanced with its interference with human rights. The least intrusive means possible to achieve this purpose must be used

For example, surveillance of the phone and Internet communications of a suspected money laundering network for the purpose of mounting a criminal case can be legitimate if undertaken according to these rules.

However, the mass surveillance of the communications of entire countries such as that conducted by the US' National Security Agency (NSA) and the UK's Government Communications Headquarters (GCHQ) is unlawful. It is disproportionate and the governments have not presented any compelling evidence to its necessity. Furthermore, much of these surveillance programmes – and similar programmes that other countries may be running – are authorised by vague laws that even lawmakers and judges would find hard to interpret. In many cases, the process for authorizing surveillance is done without adequate oversight.

For example, in the USA, a programme collecting US phone records has to be renewed every 90 days. The Foreign Intelligence Surveillance Court (known as the FISA Court) decides on these requests as well as other requests for electronic surveillance, physical search, and other investigative actions for foreign intelligence purposes. The court's operations are largely secret, its process is mostly non-adversarial, records from hearings are not made public and it has discretion to publish its opinions.

In the UK, warrants authorizing indiscriminate mass surveillance can be issued – and renewed – by the Secretary of State for the Home Department and do not require judicial authorization.

Is there such a thing as legal mass surveillance?

No. Amnesty International considers that all indiscriminate mass surveillance fails the test of constituting a necessary and proportionate interference with human rights.

In some cases, a state can legitimately conduct surveillance on a large number of individuals – for example people believed to be members of a criminal group, or all visitors to an illegal website (for example a website used to sell illicit weapons or with child pornography). In these cases, the surveillance is considered to be targeted.

How can I protect myself from surveillance online?

There are many practical things you can do. For example, the Electronic Frontier Foundation has very useful tips, tools and how-tos for safer online communications https://ssd.eff.org/ as well as a handy scorecard for messaging apps https://www.eff.org/secure-messaging-scorecard

Check out also security-in-a-box https://securityinabox.org/ and guides from Access https://www.accessnow.org/pages/tech

But even if you take precautions to protect yourself, states might be a step or two ahead. We also need strong legal protections against unlawful surveillance, so join us and sign the petition [link].