THE AGE OF SECURITY POPULISTS

ARTICLE BY
ESTELLE MASSÉ &
FANNY HIDVEGI

In a context where acts of terrorism and violence provide justification for increasingly intrusive interference with the rights of citizens, what international frameworks exist to limit government surveillance and how effective are they? What can be done at the EU level to complement those safeguarding mechanisms?

« La sécurité est la première des libertés », Jean-Marie Le Pen, 1992. Manuel Valls, 2015.

"Security is the first among freedoms"[1]. With this sentence, former French Prime Minister Manuel Valls opened his statement to advocate for the adoption of the privacy-invasive law on intelligence that significantly expanded the surveillance powers and capacities of French authorities. This law was adopted shortly after the January 2015 *Charlie Hebdo* attack. Fear-based political actions lead to unlawful and ineffective policies as well as disproportionate restrictions on the fundamental rights to privacy and data protection.

THE SECURITY THEATRE

Terrorism has been a part of the daily life of millions of Europeans for a long time. Groups like ETA and the IRA were particularly active from the 1960s onwards, resulting in the deaths of thousands of people in Spain, France, Ireland, and the UK. The terrible events of 9/11 were followed by the horrific bombings in European capitals: London and Madrid. In 2011, Norway was hit by unprecedented attacks in Oslo and on the island of Utøya. Most recently, Europe has been impacted

1 Motto of Jean-Marie Le Pen, former leader and 1992 presidential candidate of French far-right party, the Front National. Former Prime Minister Manuel Valls used this same sentence on 19 November 2015

by terrorist attacks at the *Charlie Hebdo* offices, Copenhagen, Paris, Brussels, Nice, and Berlin. These attacks differ greatly in motive and *modus operandi* but have in common the breadth of their impact.

People gather to mourn and deliver a clear message: to not give in to fear and not let hate win. In practice, however, people often do give in to fear, but not the one spread by the terrorists. As cynical as it may seem, governments have recurrently used the aftermath of terrorist events to advance their security agenda and pass sweeping measures in record time – measures that would perhaps never have been adopted at a time of peace. This is how the French intelligence and international surveillance laws were adopted. Similarly, at the EU level, some mass surveillance laws have been adopted in the aftermath of terrorist attacks, such as the Data Retention law – which has since been invalidated by the EU court for violating fundamental rights – and the Passenger Name Record law. The infographic to the right illustrates the process leading to the adoption of these laws.

This is the security theatre, where fear-based policy-making is used to provide the population with a false sense of national security. In France for instance, the government repeatedly called for a limitation of freedoms for the sake of security. This discourse is not new but was first made mainstream by the far-right extremists of the Front National.

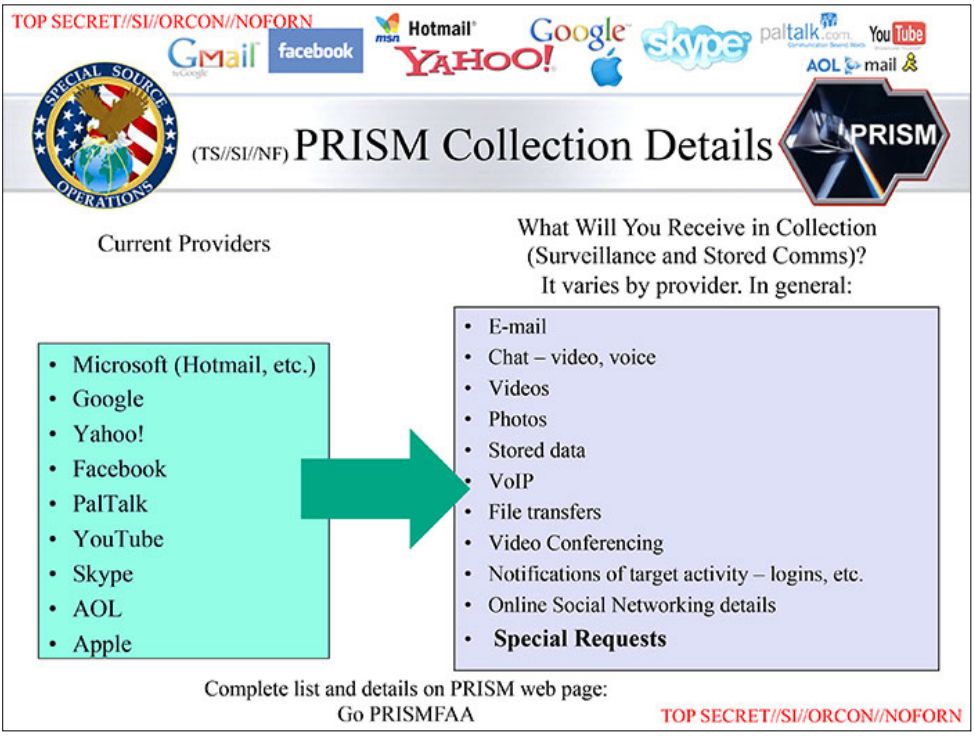
THIS IS THE SECURITY THEATRE, WHERE FEAR-BASED POLICY-MAKING IS USED TO PROVIDE THE POPULATION WITH A FALSE SENSE OF NATIONAL SECURITY

On top of the national security agenda was the expansion of surveillance powers. France, the UK, Belgium, and Germany have all undergone massive reforms over the past few years in that direction, whilst of course simultaneously expressing outrage at the reach of U.S. surveillance. In a context where security means mass surveillance, governments have developed a special interest in tech companies or, more specifically, in the volume of personal data they hold and the technological capabilities they can offer, such as facial recognition and predictive policing, to name a few. From phone records, activity metadata, to webcam feeds and internet searches, the EU governments want it all and want to keep it all. Again, they have learnt from the best (or, as it were, the worst) here. It was not so long ago that we discovered the extent of U.S. mass surveillance programmes, such as PRISM, through which the U.S. authorities can gain access to emails, chat, videos, photos, and more from Gmail, Hotmail, Yahoo!, Skype, or Facebook. The slide on the next page is part of the documents Snowden released and shows how the PRISM programme works and on which companies' data it relies.

The legitimacy of the 'collect it all' discourse is, however, called into question by the fact that in nearly all the terrorist attacks to have hit Europe, the perpetrators were known to the intelligence services of at least one EU country. In several cases, the failure to share information between different law enforcement or intelligence agencies has led to serious security failures. But in a discourse where everything is for and about security, with little to no consideration for human rights, governments have difficulties explaining why attacks still happen.

A TALE OF SURVEILLANCE, SECURITY, AND FREEDOMS

The extent of the collection, use of, and access to personal data for law enforcement and national security purposes should be subject to public debate in an open and democratic society. To have that public debate there is a need to shift from the political exploitation of emotions to proper evidence-based policy-making.



Up until today, success stories of surveillance measures have been anecdotal and limited. Governments have not provided any evidence that bulk collection of personal data has been key to solving crimes or terror attacks, or been any more effective than human intelligence gathering or effective cooperation between agencies. If we are in the golden age of surveillance, then why aren't we in the golden age of safety and security? The lack of evidence showing that more data and more surveillance lead to higher levels of security has consequences going beyond the practicalities of politics.

What we call evidence in this context is part of the widely applied legal standard any human right restriction by a state must pass: the necessity and proportionality test. These principles were developed under the jurisprudence of the European Court of Human Rights in Strasbourg to enforce the European Convention of Human Rights.

Any government that wants to impose limitations on fundamental rights, such as the right to private life, must meet the following criteria under the Convention: the restriction must be prescribed by law and in accordance with the law; it must achieve a legitimate aim; it must be deemed necessary in a democratic society given the circumstances; and finally, it must be a proportionate response to the pressing social need identified, and justified by sufficient relevant reasons by the authorities. This set of requirements establishes what constitutes a lawful interference.

This brief overview of the European Court of Human Rights' legal standard shows that evidence comes into question twice. First, during the assessment of necessity and then second, as part of the proportionality test. The Court of Justice of the EU, the highest court in the European Union is also following this standard for the application of the EU Charter of Fundamental Rights. The question of efficiency or capability of a measure is, more often than not, overlooked in rulings. The recent data retention ruling of the Court of Justice has taken a first step to declare that "national legislation must be based on objective evidence". It is high time for these courts to hold governments accountable for not demonstrating clearer evidence on the efficiency and necessity of surveillance measures.

As Edward Snowden has explained, the mass surveillance revelations point to questions not only about privacy but also the values of a democratic society. People must take over the public discourse and discredit politicians, governments, and policies that exploit people's emotions and deaths. A less cynical interpretation of the same situation would read this not as exploitation but acting in extreme and highly emotive circumstances. Yet perhaps there should be mechanisms in place to prevent politicians from drafting surveillance laws 'under the influence' of such emotional pressure, such as when the fictional president of the *West Wing* series temporarily steps aside after realising that he cannot make unbiased decisions about his daughter's kidnapping.

PRIVACY HEROES AND VILLAINS

Protecting the right to privacy and data protection can be Europe's success story. In addition to international frameworks, the EU also has an important role in curbing mass surveillance. While the EU still exercises little to no control over surveillance programmes as it technically remains a full competence of Member States, the fundamental rights to privacy and data protection are enforceable through a critical EU legal instrument, the EU Charter of Fundamental Rights. Member States must respect it and EU institutions should increase their engagement in enforcement.

IF WE ARE IN THE GOLDEN AGE OF SURVEILLANCE, THEN WHY AREN'T WE IN THE GOLDEN AGE OF SAFETY AND SECURITY?

Both from a commercial and government perspective, the EU has a significant role and capacity to limit companies' collection of information. A major first step was concluded in 2016 with the adoption of the General Data Protection Regulation that updated Europe's data protection rules dating back to 1995.

This law will enter into force in May 2018. From that date, companies will for instance have to limit the amount of data they collect to what is strictly necessary for a specifically defined purpose, and ensure that users have the right to delete or correct any information they collect. If not, they might face fines of up to 4% of their worldwide turnover. This regulation also introduces the concepts of data protection by design and by default in law. These concepts require companies to take a proactive approach to protecting privacy and data protection at every stage of the creation of their products. This approach to data protection should lead to greater consideration for human rights within companies, at the earliest stage of the conception of a product or service. This means that engineers and designers would ask themselves: what is the minimum amount of personal information that need to be collected for the product to function? Can the privacy settings be improved? The potential benefits for users are significant as the industry would finally stop seeing the right to data protection as a burden.

To complete this regulation, the EU is currently initiating the review of the e-Privacy Directive from 2002.[2] This law protects the right to privacy and has the potential to establish binding requirements on hardware and software providers to implement the privacy by design and default concepts. Such requirements would guarantee the protection of information that might be stored on our devices, such as computers and

2 A Directive is an EU law that establishes minimum rules that each Member State must comply with by adopting a national law that implements them. The States can also develop additional rules as long as these always respect the ones provided by the EU. In contrast, a Regulation is an EU law that establishes a single set of rules for all Member States and is directly applicable, without having the need to adopt a national law to implement it.

IF UNDER-MINING PRIVACY DID NOT MAKE US SAFER, PERHAPS PROTECTING IT WILL

phones, and promote the use of anonymity tools, such as encryption. Nowadays, nearly half of the most popular websites on the internet have implemented a protocol for secure communications called "https". Additionally, more and more messaging services such as WhatsApp and Signal offer end-to-end encrypted communications, though the level of protection varies significantly. The law is also crucial to protect the confidentiality of communications, both the content and the associated metadata, which refers to all the information about a call such as time, length, location, and more.

There is of course always a 'but' and this scenario is no different. When negotiating those laws, the EU Member States represented in the Council of the EU usually seek broad exceptions and flexibility, in order to bypass basic data protection and privacy rules and use data for surveillance. This is why it is crucial for companies to limit their data collection, as anything less would make them willing partners and complicit of the surveillance ecosystem. Robust rules on access to data should also be developed by the EU to avoid government snooping into our private lives. Member States must also stop attempts to use EU legislations on privacy, migration, free movement of people, or consumer protection as surveillance tools. These are the necessary steps to end the vicious security theatre we have been witnessing on repeat.

WHERE DOES THIS TAKE US?

If mass surveillance is not the answer, what will bring security? Our security challenges are not new, and so far, our society as a whole has not been able to find the correct answer. It would be unwise, or even dangerous, to attribute a single cause – like the lack of available data – to the security failures we encounter. This means that any solution also has to be multi-faceted.

What we do know is that whatever the approach lawmakers decide to take, it must be unbiased, fact-based, and above all uphold human rights. If undermining privacy did not make us safer, perhaps protecting it will. The benefits of privacy for society are invaluable as this right not only protects people's private lives but is also an enabler for freedom of expression, association, and religion; values that thrive in open and democratic societies free from government suppression and mass surveillance.

ESTELLE MASSÉ
is a senior policy analyst at Access Now's Brussels office, working on data protection, privacy and surveillance. Over the past four years, her work particularly focused on the development and implementation of the General Data Protection Regulation. Prior to joining Access Now, Estelle was part of European Digital Rights (EDRi), an association of 31 privacy and civil rights groups across Europe and at the UNESCO in Barcelona.

FANNY HIDVEGI
is Access Now's European policy manager based in Brussels. Previously, Fanny was International Privacy Fellow at the Electronic Privacy Information Center in Washington, D.C. where she focused on EU-U.S. data transfers. For three years Fanny led the Freedom of Information and Data Protection Program of the Hungarian Civil Liberties Union.
@infofannny