Privacy as a human right

Edward Snowden and the control of power

Peter Schaar
27 February 2015

The Snowden revelations revealed just how far some states had departed from the guarantees of privacy enshrined in the human and civil rights agreements of the post-war era. The European Union can play the central role in setting enforceable data protection standards internationally, however resisting the logic of surveillance also depends on pressure from society, writes Peter Schaar.

In June 2013, Edward Snowden’s revelations about the massive surveillance programme of the NSA and the British GCHQ caused global outrage. Almost two years later, the burning question is whether effective means exist to prevent blanket surveillance by the security services. One thing is for sure: there will be no return to the analogue era. If we want to enjoy the blessings of information technology, we will have to come to terms with the fact that data – including personal data – is processed *en masse*. It would be illusory to hope to reduce state surveillance activities to zero.

However, it would also be wrong to stick one’s head in the sand and wait for things that may or may not come. There are more than a few ways we can stem the tide of surveillance and protect our privacy in the digital world – both at the legal and the political levels.

Laws provide protection only within their territorially defined sphere of validity. The construction of the Internet, on the other hand, is such that national and continental borders are technically irrelevant. For example, if a German web-user accesses the website of a German service provider, it is very possible that the data is routed via American networks nodes. International Internet companies save data on servers spread across several continents.

Hence, when it comes secret service activity, insisting on the national law is too simple. The US and British governments clearly had no problem with what their intelligence agencies were doing, so long as they claimed they were acting in line with national law. Since 2013, we know that this was a lie. Legitimating surveillance by invoking national law also ignores the universal legal principles developed over the last century. Though
these were a reaction to the atrocities of the Second World War – particularly the UN Declaration of Human Rights of 1948 – and do not address the handling of information as such, they offer a basis upon which to civilize the increasingly globalized information society.

Then there is the fact that, particularly with foreign intelligence, laws effective in the field of operations are systematically broken. The NSA may very well be acting in conformity with US law and the GCHQ with British law, yet still be breaking foreign law. This is precisely what happened. For example, if a foreign secret service infiltrates a German computer using Trojan horse software, then that is an offence. Secret services that obtain the private data of German citizens by intercepting their telecommunications, or via the electro-magnetic fields of data processing facilities, are acting criminally. Just because spying does not contravene international law does not mean that spies cannot be prosecuted. German criminal law prohibits working for the intelligence services of a foreign country, for example.

Recalling human rights

The German authorities were nevertheless notably restrained in their investigation of the spying affair. Questions of evidence aside, this clearly had to do with considerations about relations with the US and the UK. This argument is absurd, given that the governments of both countries, in so far as they were responsible for the interception of confidential information from Germany, had damaged international relations themselves. As countries with strong democratic traditions, the US and the UK ought to have understood when other countries investigate offences committed against them. The fact that it took Germany’s state prosecutor almost a year to launch an investigation into the interception of Angela Merkel’s mobile telephone does not suggest any great determination on the part of the German authorities to clarify the matter. The far greater scandal of the mass surveillance clearly prevented them from forming an initial suspicion.

A fundamental – though often forgotten – principle of international law is that all state authorities abide by its stipulations. These include inalienable human rights. The Nuremberg trials were eloquent proof of the American and British prosecutors’ resolve to institute internationally binding human rights and to enforce these through criminal law. Today, the US stubbornly resists subordinating itself to international legal norms. [1]

The territorial dilemma can only be solved by creating effective and enforceable legal instruments that make human rights a reality. This also goes for rights of privacy. Data protection campaigners have been demanding international privacy standards for years – without great success. [2] The Snowden leaks have kick-started the international discussion and reminded the broader public that data protection is about human rights. Article 12 of the Universal Declaration states that “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

The United Nations began concerning itself with the consequences of automated data processing back in the 1960s. The International Covenant on Civil and Political Rights (ICPPR) of 1966 made the protection of privacy binding in international law. Countries
that ratified the pact undertook “to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.”

In 1990, the UN General Assembly resolved upon a series of recommendations concerning the use of personal data in automatized databases. However, the member states remained responsible for implementing these in law. For the 167 states that ratified the ICPR, including the EU member states, the US and the Russian Federation – though not China – should have felt bound to article 12 of the UN Declaration on Human Rights as a matter of course.

However, Snowden’s revelations prove that this was far from the case. As Germany’s Federal Data Protection Commissioner, I recommended strengthening the foundation of data protection in international law on the basis of existing legal instruments. I proposed that the German government and the European Union campaign for an international treaty: “A supplementary protocol to article 17 of the ICPR would be a useful first step. For such a international protocol to become binding, it needs to be signed by 20 states – given the 27 EU member states, this is surely achievable. States that do not recognize it must show how they still guarantee data protection, privacy and secrecy of telecommunications.”

Angela Merkel took up the suggestion a few weeks later, stating that the foreign ministry would be pressing for negotiations on a supplementary protocol to art. 17 of the ICPR. The protocol would, according to Merkel, contain additional agreements on data protection that responded to contemporary technological developments – and also be binding on the activities of intelligence agencies.

The great climb-down

For a while it looked as if the initiative of the German government would meet with broad support in Europe and worldwide. However, in the following weeks and months numerous governments who had initially signalled their agreement began to climb down. When it became clear that a supplementary protocol to the ICPR had few chances of succeeding, and would anyway have been a lengthy undertaking, Germany and Brazil, which also had been targeted for massive surveillance by the NSA, proposed a draft resolution to the UN General Assembly. Central to the draft was the demand that the human right to privacy was to be guaranteed outside the person’s country, in other words independently of the territorial principle.

The Unites States opposed this. In a negotiating paper shown to Foreign Policy magazine, the US delegation emphasized that not every type of surveillance was to be condemned, but only that which “contravened laws”. [3] Since the US and the UK referred only to their own laws, any resolution based on such premises would have been worthless.

After massive intervention by the US government and other members of the Five Eyes club (the UK, Canada, Australia and New Zealand), the resolution was eventually watered down, according to a “UN insider” quoted by Der Spiegel. The inclusion of “extra-territorial” espionage – i.e. spying carried out by one country on another – was a “difficult
issue”. However, the resolution continued to state that surveillance must be subject to international and not solely national law. At the same time, the term “surveillance” was redacted to “unlawful surveillance” and its “negative effects”. [4]

Despite US pressure, the resolution adopted by the General Assembly, entitled “The right to privacy in the digital age”, contained a clear message: the protection of privacy is an international human right that, in the age of global communications, must be guaranteed worldwide. Nation states were to ensure their “full compliance with their obligations under international human rights law” and “take measures to put an end to violations of those rights and to create the conditions to prevent such violations”.

Most importantly, it was resolved that the issue surveillance would remain on the UN agenda. The Commissioner for Human Rights was tasked with reporting to the Human Rights Council and the General Assembly on “the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or interception of digital communications and collection of personal data, including on a mass scale”.

**European data protection law: A firewall against surveillance?**

Important as the unanimous opinion of the UN member states is, it is not enough. What are needed are binding international laws that place a firewall against unauthorized global surveillance. Europe must continue to press for internationally enforceable data protection standards, regardless of resistance from the US, Russia and China, and the various authoritarian regimes that follow their example.

While modern ideas about the protection of the private sphere originated predominantly in the US, it is in Europe where they are more strongly anchored today. At the same time, the differences between the European nations should not be overlooked. The relatively mild response of the British public to the Snowden revelations shows that state surveillance is accepted there to a greater degree than in Germany. British cities are almost entirely covered by CCTV, yet this meets with little criticism; in Germany, such measures would be highly controversial.

Despite these differences, the European data protection standards and laws formulated over the past decades provide a good basis for restricting surveillance. The Council of Europe established standards very early on – long before the European Union – for guarantees of basic rights and data protection. Referring to the UN’s Universal Declaration of Human Rights, the European Convention on Human Rights (1953) committed members of the Council of Europe to the universal and effective recognition of those rights. Like the Universal Declaration, the Convention granted every person “the right to respect for his private and family life, his home and his correspondence”. Unlike the Universal Declaration, the Convention is binding upon all its signatories. Although explicitly committing its signatories to granting these right only “within their jurisdiction”, the universality of the stipulations means that they are binding in legal relations between countries and therefore cover the activities of state instances outside their own territory.

The specific dangers arising from the international exchange of data are accounted for in
the Council of Europe’s Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981. This served as the blueprint for data protection laws in many states inside and outside Europe. Its preamble states that “it is desirable to extend the safeguards for everyone’s rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing”. Article 8 of the EU Charter of Fundamental Rights (2000) also contains an explicit right to data protection: “1) Everyone has the right to the protection of personal data concerning him or her. 2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3) Compliance with these rules shall be subject to control by an independent authority.” As a part of the Treaty of Lisbon, the Charter is directly enforceable European law. Data protection in Europe thus has a significantly stronger anchor than in the US or Asia.

Data protection and the Safe Harbour Agreement

The EU Data Protection Directive of 1995 also plays a crucial role. This commits the member states to guaranteeing high standards of privacy; all member states have transposed the directive into national law.

The Google decision of the European Court of Justice on the “right to be forgotten” in 2014 showed how important European data protection law is. The search engine was obliged to remove data from its search results in the case of overriding interest of the person concerned. The Court based its decision on the 1995 directive, according to which the operator of a search engine is responsible for the processing of the data.

The directive also stipulates that data may be exported only when an “adequate level of protection” is provided in the recipient country. The adequacy of the protection is decided by the European Commission; these criteria inform the Safe Harbour Principles, to which US companies receiving the data of European citizens must comply.

Negotiations had been going on with US government for years on how European data should be protected. The US had resolutely refused to introduce data protection laws compatible with European laws. In order to enable export of data from the EU to the US, the Safe Harbour Agreement was signed in 2000. Its basic idea was that, even without a general US data protection law, adequate protection could be assumed to be provided by US companies that had declared their commitment to the Safe Harbour principles. In return, the US government would ensure that the standards were upheld.

Companies belonging to the “safe harbour” were treated by the European data protection authorities similarly to companies handling personal data in Europe. European companies were therefore not obliged to obtain permits if they wished to transfer data to Safe Harbour members. Safe Harbour is now the most important instrument for the transfer of personal data into the US - over 4400 take part in the agreement, including all the big US Internet companies.

Criticism of Safe Harbour
From the start, the Data Protection Commissioners criticized the fact that the Safe Harbour Agreement lags significantly behind the requirements of European data protection law. The fact that US companies benefit from Safe Harbour as soon as they declare their acceptance of its conditions is a further problem. European companies transferring data to a Safe Harbour member do not require a permit from the Data Protection Authority in their own country; however the recipient company is not obliged before their inclusion on the Safe Harbour list to prove that they fulfil its requirements.

After the Snowden revelations, a further criticism came to the fore: that the safe harbour agreement excludes data processing in connection with national security. This derogation has been invoked by the US authorities as well as the companies who came under criticism for supplying data to the NSA - for example Google, Microsoft, Apple, Amazon, Apple and Yahoo.

If a US security authority investigating, for example, a terror suspect needs data from Europe, they should apply to the EU state in question for international legal assistance. Before the data is passed on, the responsible authority – in Germany it would be the ministry of justice – would then check whether the requirements have been fulfilled. This democratically correct, albeit laborious process is undermined when European data is automatically transferred to a US company, without being checked, on the basis of Safe Harbour, and from there ends up in the hands of a US intelligence agency. For this reason, pressure is building in Europe to cancel the Safe Harbour Agreement. The European Parliament has called for the agreement to be renegotiated and the German data protection authorities have declared it to be an unacceptable legal foundation for transferring data to the US.

Crucial to any replacement to Safe Harbour will be that it includes state access of data transferred from Europe to the US. It is no longer tolerable that US authorities should process and copy European data without appropriate democratic guarantees. A general derogation on the basis of “national security” cannot be accepted.

**EU data protection law: Tightening the screw**

Europe’s future role in setting international data protection standards will all depend on the fate of the forthcoming EU Data Protection Regulation, which would replace the 1995 Directive. The Regulation would harmonize data protection rules in the member states and improve cooperation between the Data Protection Authorities. An equally important, though less obvious, aspect of reform concerns the scope of application of EU data protection laws. Companies such as Google that provide their services from America are still largely able to avoid European law. This would no longer be possible under the terms of the Regulation. The EU Commission has proposed that European data protection law be applicable when companies offer services or products on the European market and thereby handle personal data from the European Union. Google and other companies active in Europe would then be obliged to observe European law just like companies based in Europe. Even though the 1995 Directive served as the basis for the ECJ ruling that EU law could be applied in the case of a search engine operating from outside Europe, there needs to be a general guarantee that companies active on the European market are unable to bypass EU data protection law. The reform would ensure this.
In March 2014, in order to do something to stem the massive surveillance by foreign agencies, the European parliament proposed the introduction of a further “thumbscrew” in EU data protection law: article 43a or the so-called “anti-FISA clause”. This states that in cases where the authorities or the courts of a non-EU country order data to be accessed that is subject to European data protection law, EU companies providing this data require permission from a European data protection authority. The parliament’s proposal is as follows: “No judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognized or be enforceable in any manner.” [5]

This new rule would be applicable if the FBI or the NSA were to order data to be accessed that were saved in the Google or Microsoft cloud. Companies that receive such orders would be obliged to register this to the responsible data protection authority in the EU. They would be allowed to provide the data only if doing so was judged to comply with European or international law. Moreover, the persons concerned must be informed about the request as well as the authorization. Participation in secret surveillance programmes would thereby be prohibited.

Were this rule to pass into European law, it would inevitably bring conflict with the US. According to US law, companies that supply data to the security agencies are bound to strict secrecy. They are even forbidden from publicizing the fact that any such request was made. Whether this conflict can be solved is impossible to predict. However, if economic or political pressure were to force Europe to abandon its data protection standards, the resulting loss of trust would be impossible to repair. [6]

This is another reason why a general data protection treaty between the EU and the US is urgently needed. It would guarantee that EU citizens receive effective legal protections against the US state. The US government continues to refuse EU citizens the same data protection guarantees provided to US citizens in Europe. The NSA affair has done nothing to alter this – despite Obama’s announcements that the US would in the future respect the rights of non-Americans abroad.

The US must guarantee that data of European provenance saved on American servers is protected from the state by means of the same legal mechanisms that protect the US in the EU. The negotiations of a High Level Contact Group have been held up for years because of resistance from the US; these need to be brought to an acceptable conclusion. If this fails to happen, then Safe Harbour cannot be allowed to continue: mass violations of the right to the protection of personal data contained in the European Charter of Fundamental Rights cannot simply be ignored. However, solution is not currently in sight because the US has been unwilling to make significant concessions on any of these central issues.

**The political check on power**

Breaking the cycle of surveillance is also a matter for society. Crucial is how we are going to deal with risk in the future. Hardly anyone would agree that 100 per cent security is possible. Yet this is exactly what our post-industrial society seeks when dealing with violence, crime and terrorism. When politicians such as George W. Bush declare security to be the topmost priority, they do so with the support of the majority of the population.
At the same time, the Snowden revelations have caused significant shift in public opinion. Just how far freedoms were curtailed after 9/11 has now become visible. As David Lyon argues, politics has remained territorially bound while power extends globally. Without political control, power becomes the source of insecurity, while politics loses meaning in relation to social problems and fears. [7]

For that reason, it is crucial that greater transparency is introduced into the anti-terrorism activities of the secret services. The measures and the laws that are supposed to improve our security urgently need to be reviewed. Claims that mass surveillance measures have prevented terrorist attacks can no longer be accepted without evidence. This is generally withheld, very often under pretext of national security. Academics and independent data protection authorities analysing the results of mass surveillance have come to a sobering conclusion: that its impact on security has been practically nil. [8] Classical, targeted investigations bring far greater improvements. This doesn’t exclude the possibility that innocent people enter the sights of the security services, however they do so far less than in mass surveillance.

**A new civil rights movement**

Also certain is that better data protection will not happen of its own accord. Only when the dangers posed by surveillance are brought to public attention and debated politically will it be possible to counter the interests in favour of ever more refined instruments for the registration and control of our behaviour. The struggle over data protection is a political struggle. Law is not extraneous to society but it is the result and motor of social development. The series of judgments of the German constitutional court on rights of privacy since the early 1980s were not merely expressions of legal exegesis but the result of social debate about the balance between freedom and security.

Today, civil society is no longer prepared to accept violations of privacy as inevitable. Cracks are appearing in the hermetic system of secret surveillance established after 2001. The Snowden leaks have shaken this edifice to its foundations. However its walls still stand. The struggle remains essential.

We should not forget whom we have to thank for what we know about these immense human rights violations. Edward Snowden is a classic whistle-blower: someone who raises the alarm when confronted with immoral behaviour. The fact that he has “got stuck” in Moscow does him no discredit. If western democracies intend to remain true to their values, then they must offer him asylum. Ultimately, it is their treatment of individuals that proves whether governments take civil and human rights seriously – whether it is a matter of real political will or mere lip service.

**Footnotes**

1. The United States is one of the strongest opponents of the International Criminal Court, which began operating in 2002. Although US signed its statute in 2000, it withdrew this two years later. Since then, the US has attempted by means of bilateral treaties with countries that have recognized the authority of the ICC to prevent US citizens being brought before the Court.
2. See the resolution of the 31st International Conference of Data Protection and Privacy Commissioners from 4-6 November 2009 on international standards for the protection of privacy.


4. "Resolution gegen Abhöraktionen: Die Uno kuscht vor der NSA" [Resolution against surveillance: The UN submits before the NSA], www.spiegel.de, 26.11.2013


8. See e.g. the Report of the Privacy and Civil Liberties Oversight Board, 23 January 2014

Published 27 February 2015

Original in German
Translation by Simon Garnett
First published in Blätter für deutsche und internationale Politik 7/2014 (German version), Eurozine (English version)
Downloaded from eurozine.com (https://www.eurozine.com/privacy-as-a-human-right/)
© Peter Schaar / Blätter für deutsche und internationale Politik / Eurozine