INTERNET POLICY REVIEW
Journal on internet regulation

Volume 3 | Issue 1

Can human rights law bend mass surveillance?

Rikke Frank Joergensen
The Danish Institute for Human Rights, Copenhagen, Denmark, rfj@humanrights.dk

Published on 27 Feb 2014 | DOI: 10.14763/2014.1.249

Abstract: There is an increasing gap between the right to privacy and contemporary surveillance schemes. As a concrete example, the US surveillance operation PRISM and its impact on European citizens' right to privacy is discussed. This paper provides a brief introduction to PRISM, continues with an outline of the right to privacy as stipulated in the International Covenant on Civil and Political Rights (ICCPR), the European Convention on Human Rights and the EU Directive on Data Protection, and moves on to discuss whether international human rights law may be used to bend mass surveillance.

Keywords: Privacy, Human rights, Data protection, Surveillance, PRISM, International Covenant on Civil and Political Rights (ICCPR)

Article information

Received: 18 Jan 2014 **Reviewed:** 10 Feb 2014 **Published:** 27 Feb 2014
Licence: Creative Commons Attribution 3.0 Germany
Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL: http://policyreview.info/articles/analysis/can-human-rights-law-bend-mass-surveillance

Citation: Joergensen, R. F. (2014). Can human rights law bend mass surveillance?. *Internet Policy Review, 3*(1). https://doi.org/10.14763/2014.1.249

> We have seen how new technologies are facilitating the violation of human rights, with chilling 21st Century efficiency. In breach of international law, mass electronic surveillance and data collection are threatening both individual rights, and the free functioning of a vibrant civil society (Pillay, December 10, 2013).

The notion of internet freedom has frequently been iterated by policy makers, not least when speaking of the potential to use the internet for promoting human rights and democracy. At the 2011 G8 summit, the internet was addressed in the outcome document, the Deauville Declaration, stressing that the leaders of the group of eight will 'encourage the use of the internet as a tool to advance human rights and democratic participation throughout the world' (II Internet: Article 13). In 2012 this was followed by the first UN Human Rights Council resolution on the promotion, protection, and enjoyment of human rights on the internet, which affirms that 'the same rights people have offline must also be protected online' (United Nations Human Rights Committee, July 5, 2012). In 2013 – more or less at the same time as when the

Snowden leaks became publicised – the US, along with other OECD countries launched the new OECD Privacy Framework stressing the need for increased privacy protection in the digital environment (OECD, 2013).

Bearing in mind these recent policy commitments, this paper will examine the increasing gap between the right to privacy and contemporary surveillance schemes. As a concrete example, the US surveillance operation PRISM and its impact on European citizens' right to privacy will be discussed. The paper will start off with a brief introduction to PRISM, continue with an outline of the right to privacy as stipulated in the International Covenant on Civil and Political Rights (ICCPR), the European Convention on Human Rights and the EU Directive on Data Protection, and move on to discuss whether international human rights law such as the ICCPR may be used to bend mass surveillance.

PRISM IN SHORT

On 5 June 2013, whistleblower and former NSA[1]-contractor Edward Snowden revealed the first in a series of disclosures addressing digital surveillance programmes operated by US government entities[2]. The revelations addressed one codename in particular, namely PRISM. PRISM (2007) refers to a "special source operation" run by the United States National Security Agency (NSA) with the aim of collecting and mining a wide range of internet communication content and metadata. PRISM includes a number of surveillance programmes, such as Upstream, XKeyscore and BULLRUN (Casper Bowden for the LIBE Committee 2013: 13-14). In Upstream data collection, data is copied from both public and private networks and sent to the NSA from international fibre-optic cables, and from central exchanges which switch internet traffic between major carriers. The XKeyscore system enables the searching of a "3 day rolling buffer" of "full take" data stored at 150 global sites on 700 database servers (Ibid). The system integrates data collected from US embassy sites, foreign satellite and microwave transmissions (i.e. the system formerly known as ECHELON), and the Upstream sources above. What's more, Bullrun is the codename for a "multi-pronged effort to break into widely used encryption technologies" (Ibid)[3]. According to the US Foreign Intelligence Surveillance Act (FISA, section 702), the NSA may require a service provider to "immediately provide the government with all information, facilities, or assistance necessary to accomplish the acquisition" of foreign intelligence information. This potentially includes disclosure of keys used to secure data-in-transit by major internet companies. Personal data collected through PRISM and other programmes is shared in bulk between the intelligence communities of the US, the UK, Canada, Australia, and New Zealand under the "Five Eyes" agreement (Moraes, December 12, 2013). Other intelligence sharing agreements exist to varying degrees between these countries and EU member states.

THE RIGHT TO PRIVACY

The right to privacy is stipulated in Article 12 of the Universal Declaration of Human Rights (United Nations, 1948) and in Article 17 of the International Covenant on Civil and Political Rights (United Nations, 1966), binding upon 167 states in the world. Moreover, it is part of numerous international and regional human rights treaties and conventions. Article 17 of the International Covenant on Civil and Political Rights (ICCPR) prohibits arbitrary or unlawful interference with anyone's privacy or correspondence and establishes for all state parties a

positive obligation to create a legal framework for the effective protection of privacy rights against interference or attacks, irrespective of whether such interference or attacks come from the state itself, foreign states, or private actors (Scheinin, October 14, 2013). The right to privacy protects specific private domains such as a person's body, family, home, and correspondence and restricts the collection, use and exchange of personal data about the individual, often referred to as informational privacy (Westin, 1967)[4].

In a European context, the right to privacy ('private life') is stipulated in Article 8 of the European Convention on Human Rights (ECHR), binding upon Council of Europe states. The first paragraph sets out the rights which are to be guaranteed to the individual by the state, whereas the second part stipulates the conditions under which its interference with these rights may be legitimate. The collection of information about an individual without his consent will always fall within the scope of Article 8. The European Court of Human Rights (ECtHR) has stated that the protection of personal data is of fundamental importance to a person's enjoyment of his right to privacy (S. and Marper v. the UK, December 4, 2008). Interceptions of correspondence and telecommunications interfere with Article 8 and must meet the conditions of paragraph 2 as interpreted by the ECtHR. The ECtHR has accepted that an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting them, without having to allege that such measures were in fact applied to him or her[5]. It has also affirmed that the states may not, in the name of fighting terrorism and espionage, adopt whatever measure they deem appropriate[6]. Moreover, the court has developed some general principles that the law providing for covert measures of surveillance of communications by public authorities should meet[7]. First, the law must be accessible and the person concerned able to foresee its consequences for him/her, i.e. the law must be formulated with sufficient clarity and precision to give citizens an adequate indication of the conditions and circumstances under which the authorities are empowered to resort to this secret and potentially dangerous interference with the right to privacy. Second, there must be minimum safeguards for the exercise of discretion by public authorities, meaning that the law should have detailed rules on the nature of the offences which may give rise to an interception order. Third, there should be supervision and review by competent authorities, i.e. adequate and effective guarantees against abuses[8].

Data protection is also a binding fundamental right under Article 8 of the Charter of Fundamental Rights of the European Union (The European Parliament, the European Council et al., 2007), which reflects Article 8 of the ECHR and has a specific legal basis in Article 16 of the Treaty of the European Union (TEU). Moreover, the EU Data Protection Directive (European Commission, 1995) stipulates the rules for data protection in the private and public sector based on the principles of purpose limitation, data minimisation, and the rights of the data subject[9]. Both the TEU and the data protection directive provide for national security exemptions; however, national intelligence services must be in full compliance with the ECHR and the rule of law (Moraes, December 12, 2013:4). Regarding the transfer of data to the US, this is regulated in the Safe Harbour decision of 2000[10] specifying the circumstances under which limitations on the rights of the data subject are allowed, e.g. when it is necessary to meet national security, public interest, or law enforcement requirements. The Data Protection Directive and the Safe Harbour agreement are currently under revision, addressing among other issues the national security exemption in the current data protection regime.

As illustrated, the right to privacy and data protection are extensively regulated within Europe; thus, several instruments exist for enforcing data protection standards within and among European states. The ECHR is binding for Council of Europe states and may be claimed via

national courts and as a last resort via the European Court of Human Rights. The EU Data Protection Directive is binding on EU states and transposed into national data protection law with attached data protection agencies. However, neither the ECHR nor the EU Data Protection Directive cover privacy violations that occur outside Europe. EU states may try to negotiate stricter agreements for data exchange with third countries and/or adopt EU legislation that enforces certain data protection standards on internet companies targeting the EU market, as is currently proposed as part of the revision of the EU data protection regime. Yet in practice, EU states have limited means of enforcing European privacy standards towards the US.

The PRISM case to a large extent involves direct US access to Europeans' (and others') personal data that is stored and processed in the US due to the technical infrastructure of the internet and because many major internet services (Google, Facebook, Yahoo, Microsoft, etc.) are US-based. Turning to international human rights law, the question remains, however, whether the PRISM programme violates US obligations under the ICCPR.

PRISM AND HUMAN RIGHTS LAW

On July 4, 2013, the European Parliament adopted a resolution on the US National Security Agency surveillance programme expressing concern over PRISM and other such programmes, specifically on how these programmes affect Europeans' fundamental rights and freedoms[11]. In the resolution, the European Parliament instructed the Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) to conduct an inquiry into the matter, which has, up until January 2014, resulted in 15 hearings of experts as well as several studies on the issue[12].

As part of the LIBE inquiries, former UN-rapporteur on the protection of human rights while countering terrorism, Martin Scheinin, addressed the lawfulness of the NSA surveillance programmes *vis-à-vis* US obligations under the ICCPR (Scheinin, October 14, 2013). On the basis of Article 17 of the ICCPR, a General Comment on Article 17 from 1988, as well as other practices by the Human Rights Committee, Scheinin presented an analytical test for permissible limitations upon the right to privacy. The test includes the following cumulative conditions for deciding whether an interference with the right to privacy is justified (Ibid: 3)[13]:

(a) Any restrictions must be provided by the law;

(b) The essence of a human right is not subject to restrictions;

(c) Restrictions must be necessary in a democratic society;

(d) Any discretion exercised when implementing the restrictions must not be unfettered;

(e) For a restriction to be permissible, it is not enough that it serves one of the enumerated legitimate aims; it must be necessary for reaching the legitimate aim;

(f) Restrictive measures must conform to the principle of proportionality; and

(g) Any restrictions must be consistent with the other rights guaranteed in the Covenant.

Based on the application of the above test, Sheinin argued that the surveillance architecture of the NSA violates the legal obligations of the US under the ICCPR. Firstly, the surveillance has been based on vague and broad provisions of the Foreign Intelligence Surveillance Act (FISA),

thereby lacking a legal basis. The requirement of a legal basis for restrictions cannot be extended to a situation where neither the publicly available law - in this case FISA - nor the secret case law by a secret court provide to individuals precise information about the situations where their privacy and correspondence might be subject to surveillance (Ibid: 4). In line with the principles from the ECtHR mentioned above, accessibility and foreseeability of the legal basis are fundamental elements of the requirement of a proper legal basis so that individuals are able to adjust their conduct to the requirements of the law.

Second, the sophistication of the PRISM programme suggests that the degree of intrusion through the mass collection of metadata has affected the inviolable core of privacy. Equally important, the surveillance was not limited to metadata, but instead metadata analysis was used to identify persons whose content data would also then be accessed (Ibid).

Third, it has not been justified that the degree of intrusion employed under the PRISM programme is necessary for preventing terrorism or other serious crime in a democratic society. The failures to provide any privacy protection to non-citizens as well as the large numbers of innocent people being targeted, support the conclusion that the programme fails under the proportionality requirement. Moreover, the absence of a legitimate aim is highlighted as FISA authorises surveillance not only for the prevention of terrorism, but also for the purpose of serving the 'conduct of the foreign affairs' of the US. "This is a legitimate national interest to be pursued by lawful means that do not interfere with human rights but not a pressing social need that would justify interference with the privacy of ordinary people." (Ibid:4-5)

Fourth, there has been a lack of both judicial and parliamentary mechanisms of oversight that could prevent abuses. Moreover, since the operation was based on broad and vague laws, it was open for discriminatory application resulting in interference with other human rights such as the right to non-discrimination, freedom of expression, and freedom of association without proper justification.

As a final issue, the question of extraterritoriality was addressed, since the territorial scope of the state's obligation under ICCPR is crucial in the current context. ICCPR Article 2, paragraph 1, establishes the general obligation of a state party "to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognised in the present Covenant." According to the practice of the Human Rights Committee, this formulation entails an extraterritorial effect, implying that the state has a duty to protect not only individuals within its territory but also individuals that are subject to its control irrespective of the territory[14]. The committee has codified this practice in the General Comment on Article 2, in 2004. "10. States Parties are required by article 2, paragraph 1, to respect and to ensure the Covenant rights to all persons who may be within their territory and to all persons subject to their jurisdiction. This means that a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party"[15]. In Scheinin's intervention, these examples are used to argue a U.S violation of Article 17 for both US citizens and foreigners, since the US government de facto has had control over - and thus means to violate – the privacy rights of individuals outside the US territory. As stressed in Burgos[see footnote 13], the key issue is not the place where the violation occurs, but rather the relationship between the individual and the state in relation to a violation of any of the rights set forth in the Covenant, wherever they occurred. The question of extraterritorial effect, however, is legally complex and Scheinin's interpretation is largely contested, not least by the US government[16].

USING HUMAN RIGHTS LAW TO DEFEND THE RIGHT TO PRIVACY

In response to the inquiries within the European Parliament, a draft report is currently being prepared by LIBE rapporteur Claude Moraes[17]. The report proposes a European digital habeas corpus for protecting privacy based on 7 actions, including the adoption of the EU data protection reform in 2014, and to ensure proper redress mechanisms for EU citizens in case of data transfers from the EU to the US for law-enforcement purposes. All of the proposed actions focus on strengthening existing EU instruments and EU-US agreements and do not address the lawfulness of the PRISM programme with regard to international human rights law. Yet, some options remain open in this regard.

First, any European state can, in principle, raise an inter-state complaint under Article 41 of the ICCPR. Up until now, the inter-state complaint procedure has never been used, and for political reasons it seems unlikely that European states will resort to this option.

Second, the UN Human Rights Committee examines state parties to the ICCPR and will look at the United States record in March 2014[18], including on the question of NSA surveillance. The examination and concluding report will most likely provide specific recommendations to the US government on the PRISM programme and may be useful in further determining the US compliance with Article 17 of the ICCPR, including possible follow-up action on the European side.

Third, the UN Human Rights Council will follow up on the issue as part of the newly adopted consensus resolution on Privacy in the Digital Age (United Nations General Assembly, December 18, 2013). The resolution calls upon member states to review their practices and legislation on the interception and collection of personal data, including mass surveillance, in order to ensure the full and effective implementation of their obligations under international human rights law. It also mandates that the UN High Commissioner for Human Rights, Navi Pillay, submit a report on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance to the Geneva-based Human Rights Council at its 27th session and to the General Assembly at its 69th session taking place in September 2014.

Finally, further analysis and clarifications are needed in order to substantiate precisely how the human rights principle of extraterritorial effect applies to global data flows. Such analysis and elaboration could inform a long overdue revision of the General Comment on Article 17 from 1988, taking into account the technological developments and current challenges to the right to privacy[19].

CONCLUSION

The PRISM case is illustrative of the vulnerability of the right to privacy in the digital age. The means and measures for interference with personal data are unprecedented, and occur in a global digital domain, outside the reach of national or regional privacy protection. As such, there is a pressing need for legal analysis and recommendations concerning extraterritorial privacy violations *vis-à-vis* states' obligations under international human rights law. If the many policy commitments to a free and open internet are to be taken seriously, an authoritative human

rights-based response to the protection of privacy in the age of global data flows is urgently needed.

FOOTNOTES

1. NSA stands for the US National Security Agency

2. The revelations also addressed other programmes e.g., the UK TEMPORA programme.

3. See Bowden (2013) for further elaboration on the PRISM components.

4. According to the Council of Europe Convention of 1981 for the protection of individuals with regard to automatic processing of personal data, 'personal data' is defined as any information relating to an identified or identifiable individual (Council of Europe 1981).

5. Klass and Others, no 5029/71 §§ 30-38; Malone v. the United Kingdom no 8691/79§ 64; and Weber and Saravia v. Germany no. 54934/00, §§ 78 and 79.

6. Klass and Others, no 5029/71 §§ 49-50.

7. The following principles are a shortened version of the principles outlined in the Council of Europe's draft Explanatory Report on a Guide on Human Rights for Internet Users (Council of Europe December 6, 2013).

8. On October 3, 2013, a complaint was filed with the European Court of Human Rights by three non-governmental organisations from the UK, as well as a German internet activist against the UK. The complaint argues for a violation of Article 8 the ECHR through UK's involvement in digital mass surveillance, specifically the PRISM and TEMPORA programmes. The legal challenge is available at: https://www.privacynotprism.org.uk/news/2013/10/03/legal-challenge-to-uk-internet-surveillance/, retrieved January 14, 2013.

9. Framework decision 2008/977/JHA provides the data protection rules for the law enforcement sector when exchanging data within the EU.

10. Commission Decision 2000/520/EC of July 26, 2000, available at: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm, retrieved January 14, 2014.

11. European Parliament resolution of July 4, 2013 on the US National Security Agency surveillance programme, surveillance bodies in various member states and their impact on EU citizens' privacy, available at: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2013-322, retrieved January 14, 2014.

12. Material from the LIBE inquiries is available at: http://www.europarl.europa.eu/committees/en/libe/events.html, retrieved January 14, 2014.

13. The test is outlined in Scheinins thematic report to the UN Human Rights Council in 2009 (Scheinin 2009: para. 17)

14. As outlined in Sergio Euben Lopez Burgos v. Uruguay, HRC Communication No. R.12/52 "12.1 The Human Rights Committee further observes that although the arrest and initial detention and mistreatment of Lopez Burgos allegedly took place on foreign territory, the

Committee is not barred either by virtue of article 1 of the Optional Protocol ("... individuals subject to its jurisdiction ...") or by virtue of article 2 (1) of the Covenant ("... individual~ within its territory and subject to its jurisdiction ...") from considering these allegations, together with the claim of subsequent abduction into Uruguayan territory, inasmuch as these acts were perpetrated by Uruguayan agents acting on foreign soil. 12.2 The reference in article 1 of the Optional Protocol to 'individuals subject to its jurisdiction' does not affect the above conclusion because the reference in that article is not to the place where the violation occurred, but rather to the relationship between the individual and the State in relation to a violation of any of the rights set forth in the Covenant, wherever they occurred".

15. General Comment No. 31, adopted by the Human Rights Committee in 2004, available at: http://www.unhchr.ch/tbs/doc.nsf/0/58f5d4646e861359c1256ff600533f5f , retrieved January 14, 2014.

16. The extraterritorial implications of human rights law is covered by e.g., Milanovic (Milanovic, 2011). For an account of this debate in relation to the current case and Article 17 of the CCPR see e.g.,: http://www.lawfareblog.com/2013/11/does-the-iccpr-establish-an-extraterritorial-right-to-privacy/, retrieved January 14, 2014.

17. The report is available at: http://www.europarl.europa.eu/RegistreWeb/search/simple.htm?reference=LIBE/7/13778, retrieved January 14, 2014.

18. The US was originally up for review in October 2013, however the review has been postponed to March 2014 due to the US government shutdown in October, cf: http://www.ohchr.org/EN/HRBodies/CCPR/Pages/ReviewUSA.aspx, retrieved October 30, 2013.

19. A revised General Comment on Article 17 has been proposed several times, e.g., when the right to privacy in the fight against terrorism was considered by the UN Human Rights Council in March 2010 (Scheinin, 2009). On that occasion, it was also proposed that the Human Rights Council should initiate a global declaration on data protection as a soft law complement to the ICCPR.

BIBLIOGRAPHY

Casper Bowden for the LIBE Committee (2013). The US surveillance programmes and their impact on EU citizens' fundamental rights. Brussels, European Parliament.

Council of Europe (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Council of Europe. Strasbourg

Council of Europe (December 6, 2013). Draft explanatory memorandum to the draft recommendation CM/Rec (_____) __ of the Committee of Ministers to member states on a guide on human rights for Internet users. Strasbourg, Council of Europe.

European Commission (1995). EU Directive on Data Protection (95/46 EC). Brussels, EC.

Milanovic, M. (2011). Extraterritorial application of human rights treaties : law, principles, and policy. Oxford; New York, Oxford University Press.

Moraes, C. (December 12, 2013). Working Document 3 on the relation between the surveillance practices in the EU and the US and EU data protection provisions. Brussels, European Parliament.

OECD (2013). The OECD Privacy Framework. Paris, OECD.

Pillay, N. (December 10, 2013). "Mass surveillance violates human rights ". Retrieved from http://www.unric.org/en/latest-un-buzz/28900-pillay-mass-surveillance-violates-human-rights

Scheinin, M. (2009). Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, United Nations General Assembly, Human Rights Council,.

Scheinin, M. (October 14, 2013). Statement by Professor Martin Scheinin. LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens. Brussels.

The European Parliament, the European Council, et al. (2007). Charter of Fundamental Rights of the European Union. Brussels, EC.

United Nations (1948). The Universal Declaration of Human Rights. New York, United Nations.

United Nations (1966). International Covenant on Civil and Political Rights. New York, United Nations.

United Nations General Assembly (December 18, 2013). Resolution adopted by the General Assembly. The right to privacy in the digital age. New York, United Nations.

Westin, A. F. (1967). Privacy and freedom. New York, Atheneum.