A whistle blowin' in the wind? Why indifference towards mass surveillance will make a difference

Evin Dalkilic

04.11.2013 doi: 10.17176/20170930-161031

"One of the most disturbing aspects of the public response to Edward Snowden's revelations about the scale of governmental surveillance is how little public disquiet there appears to be about it." But why should we care when most likely the majority of us will never even notice that their data are being stored and can easily be accessed by State authorities? To put it simply: because it is against the law. Despite the calls for an international agreement on the protection of data and Brazil's and Germany's circulation of a draft General Assembly Resolution to demand the cessation of the current spying activities, we should be aware that an international agreement to protect citizens' privacy and correspondence already exists. That is the International Covenant on Civil and Political Rights (ICCPR) with 167 State parties and 74 signatories, among them the United States and the United Kingdom who also ratified the treaty.

What? Who? Where? - The www of human rights

There are a number of politicians and scholars who consider the disclosed spying practices to constitute a breach of international law in general and of the ICCPR in particular. But little has been said or written about the actual legal requirements to find such a violation in light of the recent revelations. The first questions that need answering are: What is protected by the ICCPR, who is protected and where must the violation occur?

Article 17 (1) ICCPR provides that:

> *No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence [...].*

Even though the ICCPR was drafted in the 1960s, it is generally acknowledged that also modern forms of correspondence are covered[1]. Frank La Rue, the current Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, even considers metadata – which can form an integral part of one's private sphere – to fall within the scope of the Covenant.

The ordinary meaning of the term 'interference' covers all actions that are not necessary and impede the exercise of the right. In its General Comment No. 16, the Human Rights Committee stated that "'arbitrary interference' can also extend to interference provided for under the law" if it runs counter to the object and purpose of the Covenant (para. 4). Arbitrariness "contains elements of injustice, unpredictability and unreasonableness".[2]

The collection and storing of estimated "850bn 'call events' [...] and close to 150bn internet records" in NSA databases with 1-2bn records being added every day qualifies for both arbitrariness and interference, even though they might be permissible under US law. The collection and storing of that much data from that many people without any preceding examination of potential relevance amounts to a massive level of capriciousness.

Additionally, the Human Rights Committee (General Comment no. 16) found that "every individual should have the right to ascertain in an intelligible form whether, and if so, what personal data is stored in automatic data files, and for what purposes"(para. 10). Such information is not disclosed by the NSA, though.

Article 2 (1) ICCPR contains the general obligation of States to respect the Covenant's rights. It states:

> *Each State Party to the present Covenant undertakes to respect and to ensure to all individuals*

> *within its territory and subject to its jurisdiction the rights recognized in the present Covenant […].*

Because the territory is seen as the primary connection, applying the 1966 Covenant to the exercise of human rights on the internet poses some problems.

A territorial link undoubtedly exists when data "transit or terminate" in the respective State and are intercepted from servers located within that State. The fact that merely their data and not the individual itself is on the territory is sufficient to trigger human rights protection.

If, however, the data are intercepted from a server located on the territory of another State, a traditional and narrow understanding of 'jurisdiction' would assume that human rights do not apply, because no physical control is exercised over the protected individuals. In light of present-day's realities, when the vast majority of data and correspondence is stored on servers all over the globe, data protection would thus only depend on the technical capabilities of States to repel interception. That result, however, would be incompatible with the object and purpose of human rights obligations. In order to give effect to human rights obligations, 'jurisdiction' has to cover the exercise of control over the protected good, ie data.

In support of an argument for greater human rights protection, mention must be made of the general acknowledgement of the need to protect and apply human rights to activities on the internet. Often, such calls refer to the freedom of expression as in the case of the Freedom Online Coalition (currently encompassing 19 member States, among them, again, the United States and the United Kingdom). These efforts are mostly related to concerns about censorship through public authorities and the persecution of dissidents who are active online. The problem of the scope of territorial application usually does not arise in those cases, as the measures are typically directed against individuals within those States.

But at the same time, one cannot ignore the inextricable link between the right to privacy and the freedom of expression as was also pointed out by Frank La Rue.

Consequently, States that genuinely aim to protect the freedom of expression on the internet will equally have to respect the privacy of online data as a necessary prerequisite.

Consequently, though by no means undisputed, the data and correspondence of citizens are protected against interference from States other than the home State.

Permissible limitation? It's the proportionality, stupid!

Although Article 17 ICCPR itself does not expressly allow for limiting the right to privacy and correspondence, it is recognized that such a limitation is permissible due to other provisions of the Covenant. Limitations are for example possible for reasons of national security as provided in Articles 12 (3) or 19 (3). Undeniably, potential terrorist attacks pose a severe threat to human lives and national security. Equally undeniable is the need for secret intelligence services to covertly collect intelligence in order to prevent attacks. However, it is understood that any limitation will have to satisfy requirements that are established in the Human Rights Committee's General Comment No. 27 (paras. 11-15). These are, inter alia, the necessity and proportionality of the restrictions and also "the relation between right and restriction, between norm and exception, must not be reversed".

In his advanced 2009 report, Martin Scheinin, former Special Rapporteur on human rights and counter-terrorism, made clear that "countering terrorism is not a trump card which automatically legitimates any interference with the right to privacy". But in his earlier report he also stressed the legitimacy of "covert surveillance or the interception and monitoring of communications" if they occur on a case-by-case basis, rely on a suspicion which is based on facts, and are approved by a judge. This, indeed, is "a desirable, reasonable and proportionate method to identify risks or to find out more about suspicions against a terrorist suspect."

What actually happens can be seen on one of the disclosed pages of the power point presentation explaining the functioning of the XKeyscore program. Conducting e-mail searches, for example, NSA person-

nel (and apparently contractors working for the NSA like Edward Snowden did) just need to enter a justification for their query in order to gain access to an individual's e-mails. This practice does not satisfy the requirements outlined above – neither is a judge involved nor does surveillance occur on a 'case-by-case' basis. Indeed, the secret services' practices reverse the relation between norm and exception, when the norm is surveillance with the need of prior judicial approval. Accordingly, the applied surveillance practice is not a permissible limitation of the rights deriving from Article 17 (1) ICCPR as it is disproportionate.

Another possibility to derogate from the Covenant's obligations is laid down in Article 4 ICCPR which provides for the implementation of measures in time of public emergency. Such state of emergency must be officially proclaimed and the respective State must inform the other parties of the provisions from which it has derogated and of the reasons for the derogation.

In its latest available Periodic Report (Art. 40 ICCPR) to the Human Rights Committee, the US stated not to have declared a state of emergency within the meaning of Article 4 ICCPR. It is not apparent that the United Kingdom has, either.

So what difference does it make?

The above considerations should illustrate the (presumably) ongoing human rights violations affecting a large part of the world's population. Those rights reflect values agreed upon by a significant number of States and as such they reflect our understanding and conception of the societies we belong to. I am very well aware that those standards are not at all implemented in every State that is party to Covenant. But I have always thought of them as standards to be strived for.

Should this massive violation simply be ignored by our societies, we would have to reconsider that understanding and conception. This would mean that unwarranted access to and interference with our privacy and correspondence becomes the rule and not the exception. It would also mean our consent to private conversations and browsing history possibly triggering some algorithms or to being held accountable for anything we may have said or written and which in retrospect can add up to a twisted image of ourselves. And, ultimately, it would mean restraint when voicing our opinions as well as restraint when browsing through the internet. Even though all of that is already happening, living at peace with it will make a difference because it will be a self-imposed restriction of our freedoms.

This article was previously posted on JuWissBlog and is re-posted here with kind permission.

ABOUT THE AUTHOR

Evin Dalkilic
Evin Dalkilic is the head of publishing at Verfassungsblog.

SUGGESTED CITATION

Dalkilic, Evin: A whistle blowin' in the wind? Why indifference towards mass surveillance will make a difference, Verfassungsblog, 04.11.2013, doi: 10.17176/20170930-161031.

Licensed under CC BY-SA 4.0.

Langzeitarchiviert bei IntRechtDok unter: doi.org/10.17176/20170930-161031.