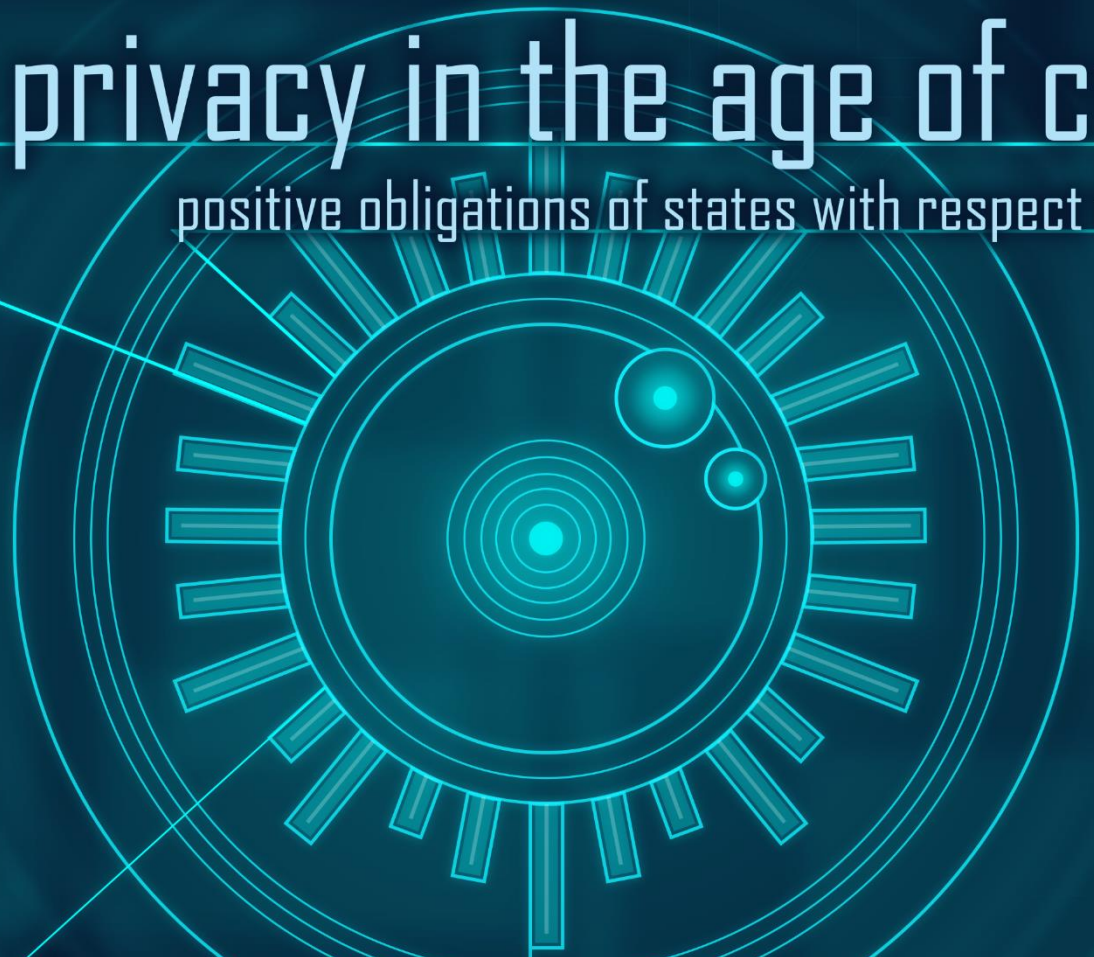
Right to privacy in the age of cyber:

positive obligations of states with respect to mass surveillance



P. Kurakina

2020

Setting the scene: acceptability of mass surveillance

The Court has expressly recognised that the national authorities enjoy a wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security (see *Weber and Saravia*). Furthermore, in *Weber and Saravia* and *Liberty and Others* the Court accepted that bulk interception regimes did not *per se* fall outside this margin.

…In view of the current threats facing many Contracting States (including the scourge of global terrorism and other serious crime, such as drug trafficking, human trafficking, the sexual exploitation of children and cybercrime), advancements in technology which have made it easier for terrorists and criminals to evade detection on the Internet, and the unpredictability of the routes via which electronic communications are transmitted, the Court considers that the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within States' margin of appreciation. (*Para 314 Big Brother Watch)*

Positive obligations in the surveillance context: outline

In IHRL, there types of obligations or duties when safeguarding human rights: to respect, protect, and fulfil.

The duty to **respect** a right bestows a negative obligation of conduct, the positive obligation to **protect** is one of the conducts that extend to third-party violations, and the obligation to **fulfil** entails a positive obligation of result.

In the surveillance context this obligation would have two main components.

- First, states would need to regulate private companies operating in areas under control that collect, store, process, or have access to personal data. This would include, but not necessarily be limited to, basic standards on data protection.
- Second, states would need to exercise due diligence and undertake all effective measures reasonably available to them to prevent interferences with privacy by third parties.

Positive obligations in the surveillance context: outline

Overall, as the Human Rights Committee has noted that states parties to the ICCPR have a positive obligation to “adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right [privacy].

Res. no. 68/167 on The Right to Privacy in the Digital Age

"The General Assembly,

...

4. *Calls upon* all States:

...

(*c*) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;

(*d*) To establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data ..."

Jurisdiction with respect to positive obligations

"Jurisdiction" would primarily mean effective overall control over areas, and the overarching positive obligation would be dependent on a state having such control over an area, as the state actually needs such control in order to be able to comply with this obligation.

The negative obligation to respect human rights would be territorially unlimited and not subject to any jurisdictional threshold, because any such threshold that was non-arbitrary would collapse anyway. Textually, this would flow from Article 1 of the ECHR only referring to the obligation to secure, while Article 2(1) of the ICCPR could reasonably be read as attaching the jurisdiction threshold only to the obligation to ensure, but not the obligation to respect.

Marco Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2014) HILJ
Peter Margulies, 'The NSA in Global Perspective: Surveillance, Human Rights and International Counterterrorism' (2014) 82 Fordham Law Review

ECHR Big Brother Watch

In its case-law on the interception of communications in criminal investigations, the the following minimum **requirements that should be set out in law** in order to avoid abuses of power:

- the nature of offences which may give rise to an interception order;
- a definition of the categories of people liable to have their communications intercepted;
- a limit on the duration of interception;
- the procedure to be followed for examining, using and storing the data;
- the precautions to be taken when communicating the data to other parties;
- the circumstances in which intercepted data may or must be erased.
- In *Roman Zakharov* the Court confirmed that the same six minimum requirements also applied in cases where the interception was for reasons of national security;

- **no** objective evidence of reasonable suspicion in relation to the persons for whom data is being sought
- **no** mandatory judicial authorization

ECHR Big Brother Watch

The Court examines the justification for any interference in the present case by reference to the six minimum requirements, adapting them where necessary to reflect the operation of a bulk interception regime. (para. 320 Big Brother Watch)

The scope of application of secret surveillance measures

The first two minimum requirements have traditionally been referred to as the nature of the offences which might give rise to an interception order and a definition of the categories of people liable to have their telephones tapped. In *Roman Zakharov* the Court made clear that pursuant to these two requirements "the national law must define the scope of application of secret surveillance measures by giving citizens an adequate indication as to the circumstances in which public authorities are empowered to resort to such measures".

In addressing the first two minimum requirements, the Court examines whether the grounds upon which a warrant can be issued are sufficiently clear; secondly, whether domestic law gives citizens an adequate indication of the circumstances in which their communications might be intercepted; and thirdly, whether domestic law gives citizens an adequate indication of the circumstances in which their communications might be selected for examination.

Review and supervision

- Review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated.
- the first two stages should be effected without the individual's knowledge.
- since the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights (see *Roman Zakharov*).
- As regards the third stage, after the surveillance has been terminated, the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers.

Lack of clarity, “below the waterline” arrangements

The applicants challenge the accessibility of domestic law on the grounds that it is too complex to be accessible to the public, and it relies on “below the waterline” arrangements. It is true that most of the reports into the United Kingdom’s secret surveillance regimes have criticised the piecemeal development – and subsequent lack of clarity – of the legal framework

Digital tracking as a response to COVID-19

Region	Digital Tracking	Censorship	Surveillance
Europe	8	0	3
Asia	8	6	2
MENA	2	3	0
SSA	1	2	0
N. America	1	0	2
S. America	2	0	0
Australasia	0	0	1

Regional breakdown of measures implemented in response to COVID-19

- In Thailand, people travelling from high-risk areas must download an app so that authorities can monitor their movements during their 14 days of quarantine.
- In Hong Kong, the government are using electronic wristbands, QR codes and an app to enforce quarantine.
- Poland has released a "home quarantine" app, where users send a geolocated picture to the police to prove that they are not violating quarantine. The app is connected to a database of phone numbers of people who are under mandatory quarantine.

QR concerns

- encryption

- data storage

- type of data gathered

- open keys and identifiers

The Yarovaya amendments

The Yarovaya amendments require telecom providers to store the content of voice calls, data, images and text messages for 6 months, and the metadata on them (e.g. time, location, and sender and recipients of messages) for 3 years. Online services such as messaging services, email and social networks that use encrypted data are required to permit the Federal Security Service (FSB) to access and read their encrypted communications.

Internet and telecom companies are required to disclose these communications and metadata, as well as "all other information necessary" to authorities on request and without a court order