Big Brother’s Democratic Debate: Mass Surveillance versus the Right to Privacy

Eleanor Mount

Professor Rachel Cichowski

LSJ 490, Winter 2017

10 March 2017

Introduction

In 2013, Edward Snowden made international news headlines when he released top-secret activities of the United States’ National Security Administration. The NSA’s surveillance program, codenamed PRISM, had captured emails, text messages, photographs and documents of suspected individuals on an unprecedented scale and was unbeknownst to the public or most members of Congress (Ni Loiedian 5). Since this global revelation about the way by which the US and other Western powers intercept communications on a massive scale, there has been no question mass surveillance exists. Even if people dislike the idea they are being spied on, the public generally accepts that mass surveillance happens. Any individual using the Internet is one of many millions of people—and if an individual isn’t engaging in any suspect behavior, such as acts of terrorism, they have nothing to hide (“UnfollowMe”). In a global age marked by terrorist threats and rapid increases in technology, the right to privacy is often portrayed as the loser in tensions between privacy and security.

This paper analyzes the emerging field of mass surveillance case law of the European Court of Human Rights (ECHR) to understand the role of individuals, Non-governmental organizations (NGOs), states, and courts in shaping this area of law. I start by outlining the justice problem from the perspective of state and non-state actors to demonstrate how mass surveillance struggles to balance the state’s interest in security with the public right to privacy. I then analyze data from the ECHR’s rulings as well as participation data from NGOs to demonstrate how these arguments take effect in case law, using the 2015 case *Roman Zakharov v. Russia* as an example. Finally, I present and critique three alternatives to resolving this justice issue relating to accountability: modern and traditional forms of democratic participation, preventing violations of privacy in legislation, and implementing greater checks on state power. In an area of case law growing rapidly with advances in technology, this area of law has important implications for future relationships between privacy and state security.

The Justice Problem

Before delving into the ECHR’s interpretation of the right to privacy, it is important to understand the justice issues surrounding mass surveillance and how both state and non-state actors’ arguments relate to accountability. Mass surveillance is typically understood as the “indiscriminate, pervasive surveillance of an entire population,” or a substantial amount of it by permitting state access to all digital communications traffic (Zalneiriute 2). While mass surveillance has been used throughout history in some degree to collect detailed information about citizens, legal concerns have increased greatly with expansions in technology. More recent expansions within mass surveillance focus heavily on monitoring phone and Internet communications (“Mass Surveillance.”). This technology has become more prevalent, but law has struggled to keep up. Very few legal guidelines exist curtailing what governments can do with broad access to surveillance. A crucial feature of representative democracy is “those who govern are held accountable to the governed,” (Grant Keohne 3), but without any specific legal mechanisms, the state has more discretion to exercise power than the citizen. Accountability typically “functions to expose and sanction” the unauthorized or illegitimate exercise of power and decisions perceived to be unjust (Grant Keohne 3). Mass surveillance’s secretive and omniscient nature poses challenges to accountability because it is no longer clear what states are doing and how much information they collect on citizens.

Given the absence of any laws outlining government use of technology, this area has undergone substantial consideration by the ECHR to determine what is lawful. All complaints brought to the Court about mass surveillance are lodged under Article 8 of the European Convention, the “Right to respect for private and family life.” This right asserts “Everyone has the right to respect for his private and family life, his home and his correspondence.” Part two of Article 8 outlines what constitutes an illegal interference on the right to respect for private life, stating “There shall be no interference” with this right “except such as in accordance with the law and is necessary in a democratic society.” “Such as in accordance” provides a causal link to ensure these interferences are only acceptable if they fit reasons provided under several categories: “national security, public safety, prevention of disorder or crime, the protection of health or morals, or for the protection of the rights and freedoms of others” (Convention for the Protection of Human Rights and Fundamental Freedoms Art. 8). In balancing these rights, the ECHR examines whether interferences to the right to privacy were made “in accordance with the law, pursued a legitimate aim or aims, and was proportionate to the aim(s) pursued” (Factsheet: Mass Surveillance). Even when mass surveillance can be shown to have a legitimate aim, it is unlikely meet tests of proportionality and necessity. When personal information is stored in the interests of national security and adequate and effective guarantees against abuse by the State exist, the Court will not necessarily find a violation of Article 8 (“Internet: case-law of the European Court of Human Rights” 10).

From the state’s perspective, developments in technology have unquestionably made monitoring citizen’s data an important tool for national security and law enforcement (Ni Loiedian 3). To use surveillance legally states pass laws outlining the use of surveillance technology. In defending these laws, states argue without the ability to monitor “enemy phone calls and Internet communications,” there would be no effective way to prevent threats to security, such as terrorist attacks. States have only three options in obtaining information to prevent terrorist attacks: interrogating suspects, infiltrating agents into enemy ranks, and intelligence, or monitoring enemy phone calls and Internet communications. Interrogation has proven ineffective and infiltration is extremely difficult, so this leaves only intelligence as the state’s principal source of intelligence to stop terrorist plots (Thiessen). In collecting this data, states are only targeting a few select individuals marked as “terrorists,” but in order to “connect the dots and stop the next attack,” the state has to have “all of the dots.” For example, if a terrorist’s cellphone is found in a raid information from the phone can be plugged in to systems of mass surveillance to figure out who has communicated with this terrorist, but the state has to have all of this information in order to unravel networks connected to that particular terrorist. The collection of this data itself in order to form these networks is a benign measure that does not offend privacy rights; if people aren’t communicating with terrorists, they will likely not ever be suspects. Additionally, most states only collect and aggregate “metadata” which concerns the context of communication rather than the content. The context, such as location data, user data, and information about the cellular phone network or Internet service provider is already public information, as opposed to the content of communication, which is private and generally cannot be obtained without a warrant (Ni Loiedian 4).

Significant public concern about mass surveillance remains even for those who are not engaging in any suspect activity. Metadata certainly does not sound revealing, but distinct advancements in digitization have created smartphones, which converge both mobile and Internet communications. Through location services, online activities, and Internet and phone communications, the constant trail of metadata smartphones leave makes metadata just as valuable as the content of communications for law enforcement purposes. Access to the content of communications is no longer necessary to infer what people are doing. This data could be used to target journalists, persecute activists, profile and discriminate against minorities, and to crack down on free speech (Ni Loiedian 3). Amnesty International, a NGO dedicated to human rights argues “when governments spy on [people], they abandon long-standing legal principles” by treating every detail of an individual’s personal life as suspicious (“UnfollowMe”). By surveilling everyone without any suspicion of wrongdoing, mass surveillance programs undermine the principle of “presumption of innocence” before one is proven to be guilty and therefore, the very effectiveness of the legal process (Newell 32). Bulk collection of communications data also has been shown to have a “chilling effect” on free speech (Newell 32), thought, and association—all fundamental human rights protected by the European Convention (Convention for the Protection of Human Rights and Fundamental Freedoms Art. 9; Art. 11). When people are thinking, reading, and communicating with others to make up their mind about political and social issues, if individuals know they are being watched, they are unlikely to experiment with new or deviant ideas (Richards 35). This undermines the very nature of the right to free speech and expression.

The Evidence

In this section, I will provide an overview of the development of mass surveillance case law in the ECHR. In particular, I draw attention to how this policy area has been shaped by both state expansions of mass surveillance and political activism of NGOs. The data utilized in this section includes all cases in the “Mass Surveillance” factsheet area published by the ECHR. The first case was lodged in 1978 and concerned German monitoring of telecommunications. Cases were at a complete standstill until 2008, and since then law has steadily increased and the Court has seen an average of at least one case surrounding mass surveillance per year. This increase can be attributed to the far-reaching impact of the September 11th attacks on the United States in Europe, and terrorist bombings in Madrid and London in 2004 and 2005 (Ni Loiedian 4), which both led to states monitoring communications data to prevent future attacks. The United Kingdom and Germany experience the majority of litigation in this area, with 40% of cases coming from the UK and 20% from Germany. A violation is found in half of cases, which demonstrates tensions between individuals filing claims and the states are prevalent in this area of case law and even the Court is not strictly decisive in this area. At a further glance when breaking the data down by country, it is important to note the Court has always found a violation in countries with one case brought against them, but has yet to find a violation with the United Kingdom or Germany, who make up the bulk of this dataset (Factsheet: Mass Surveillance).

NGOs also have a strong presence in ECHR cases in this area; 40% of cases were lodged by NGOs instead of individuals (Factsheet: Mass Surveillance). NGOs have to prove they are directly harmed by legislation in order to lodge complaints to the ECHR, which is unusual and speaks to NGO activism monitoring civil liberties in the realm of mass surveillance. Privacy International and Amnesty International, two leading NGOs fighting against mass surveillance globally currently have a pending case with the ECHR, where they partnered with eight other NGOs to challenge the United Kingdom’s surveillance regime (10 Human Rights Organisations v. the United Kingdom). Big Brother Watch, a United Kingdom NGO focused on opposing mass surveillance, also recently filed a case against the UK. Edward Snowden triggered their concerns following his revelations about the prevalence of mass surveillance in Western governments (Big Brother Watch and Others v. the United Kingdom).

To understand more precisely how the court balances the right to privacy with state interests in security, I will provide an analysis of the Court’s decision-making process through the Grand Chamber’s ruling in *Roman Zakharov v. Russia*. In 2015, the Court’s ruling in *Zakharov* brought international attention of many of these NGOs, states, and the public in Europe. Roman Zakharov, the Editor-in-chief of a publishing company and the chairperson of an NGO monitoring the state of media freedom in Russia, brought judicial proceedings against three mobile networks operators claiming a violation of his right to the privacy of his communications. Zakharov specifically challenged the “Operational-Search Activities Act” legislation in Russia, an ongoing system of secret interception of telephone and Internet communications. The law required mobile network operators in Russia to install equipment enabling law-enforcement agencies to carry out operational-search activities, which include the interception of postal, telegraphic, telephone, and other forms of communication (6-7). A warrant is only required for government offices to view communications content, but metadata can be viewed without a warrant. The law, according to Russia, had aims of “detection and prevention” of criminal offences, tracing fugitives and missing persons, and “obtaining information about events or activities endangering the … security of the Russian Federation” (6). Russian courts rejected Zakharov’s claims because he had no concrete evidence he was being a target; he could only show mobile networks officers were technically capable to intercept all of his telephone communications without obtaining prior judicial authorization (37).

In the Grand Chamber ruling, the ECHR found there had been a violation of Article 8 even though Zakharov was unable to allege he had been the subject of a concrete measure of surveillance. Given the secret nature of surveillance measures, the fact these measures affected all users of mobile telephones, and no domestic remedy existed for people who suspected they were subject to secret surveillance, the very existence of the contested legislation amounted in itself to an interference with Zakharov’s rights under Article 8 (83). The Court does note the interception of communications pursued “legitimate aims” of protection of national security and public safety, prevention of crime, and protection of Russia’s economic well-being (58). However, given the risk a system of secret mass surveillance could undermine or even destroy democracy, the Court had to find adequate and effective guarantees against abuse existed. The Court also noted the risk of abuse is inherent in any system of secret surveillance and is particularly high in Russia. In the Court’s conclusion, they quote Edward Snowden, stating “Facts are more convincing than fear” and “the value of the right [to privacy] is not in what it hides, but in what it protects” (89). This highlights the court’s belief the protection of the right to privacy is far from sufficient across Europe in its present manner.

*Zakharov* drew a great amount of public attention, but it had little domestic impact in the ECHR’s member states. The same day of the ECHR ruling, Russia passed legislation allowing it to overrule international court orders to “protect the interests of Russia” (“Russia Passes Law to Overrule European Human Rights Court”). Around the same time *Zakharov* was issued in late 2015, the United Kingdom published the “Investigatory Powers Bill” in Parliament. This Bill aimed to greatly expand powers available to the police, security and intelligence agencies to gather and access electronic communications (Griffin). In particular, it greatly expanded the government’s use of bulk personal datasets, including rules that require Internet providers to complete records of every website all of their customers visit, communications data and records, data retention, and makes it easier to obtain warrants to search this data. Despite public concern over their right to privacy amid recent concerns raised regarding mass surveillance from *Zakharov,* the Bill passed in late 2016 (“Investigatory Powers Act – Big Brother Watch”).

The Alternatives

This section will discuss and evaluate the various remedies available for individuals to protect rights to privacy and for member states to comply with Article 8 of the European Convention. The ECHR notes while the primary object of Article 8 is to protect the individual against arbitrary interference by public authorities, there may be “positive obligationsinherent in an effective respect for private” life (“Internet: case-law of the European Court of Human Rights” 9). While personal information is stored in the interests of national security, there should be adequate and effective guarantees against abuse by the state (“Internet: case-law of the European Court of Human Rights” 8). This section will proceed by outlining the advantages and drawbacks to democratic participation, legislative safeguards, and implementing greater checks on government power, and by explaining situations in which each solution may be appropriate. These solutions revolve around balancing the right to privacy with the state’s interests in protecting security, and ensure the public can hold the state accountable if mass surveillance is not conducted in a proportional, necessary, and legitimate way. Grant and Keohne allude to solving these issues, writing “accountability requires establishing institutions that provide information to those people trying to hold [the state] accountable” (3). If individuals and NGOs hope to avoid potential invasions of privacy, they have no alternative but to be more active partners with the state in developing legislation.

Using channels of democratic participation available to the public in any democratic society allows individuals and NGOs to effectuate their own interests in privacy. These channels include “political participation, litigation, exercising free speech rights, or documenting government conduct in various ways” (Newell 34). Exercising the right to free speech is a simple yet effective way to curtail mass surveillance and show dissatisfaction with a representative government. Traditional mechanisms such as political participation and litigation remain popular, as demonstrated by NGOs and the increase in mass surveillance case law in the ECHR since 2008. A more contemporary way to document government conduct is through “sousveillence,” which roughly translates to “watching from under.” Sousveillance is a form of “reflectionism” that seeks to increase the equality between the surveiller and the one being surveilled (Mann 333). Examples include civilians photographing or filming government officials and residents beaming satellite shots of occupying troops onto the Internet (Mann 334). Sousveillance provides an outlet for public sharing of information and has been effective in raising public support and awareness. However, states continue to expand mass surveillance laws amidst public protest and legal action in examples such as the Investigatory Powers Bill in the United Kingdom.

If traditional reactionary mechanisms like litigation and sousveillance cannot effectively counter and change the law, providing safeguards against violations of privacy in the legislation itself provides legal avenues to simultaneously allow states to engage in mass surveillance legally and prevent abuses against privacy. Clearly defined technical, legal, and privacy safeguards should be written when a government passes legislation to collect data (Big Brother Watch) to prevent against arbitrary use. Individuals could also be notified when their data is accessed, shared, or retained by the state. For example, states could implement greater checks on the exercise of government surveillance powers by sending annual audits of requests, actions, and shares of personal data to every individual. This requires states to remain transparent about how they use surveillance, but sending annual individualized audits could be costly and requires a large allocation of resources.

Finally, states can implement Freedom of Information laws, which serve as a powerful and effective means to empower oversight by ordinary to citizens. Freedoms of Information laws provide a legal mechanism for citizen-initiated surveillance and grant citizens greater power to check government abuse and force even greater transparency. These laws must capture more information about surveillance programs to ensure “adequate and effective guarantees against abuse” exist (Newell 34). These laws are similar to annual audits in that they both require government transparency, but Freedom of Information require citizens to ask for information rather than having it automatically sent to them, therefore being less costly. Information facilitates power (Newell 34), and this form of reciprocal surveillance grants citizens greater power to hold their governments accountable. Providing ways to prevent against the abuse of mass surveillance is both necessary and possible through democratic participation, encouraging government transparency, and enacting safeguards in legislation.

Conclusion

Mass surveillance undoubtedly exists and as access to technology expands, it has become a popular form of citizen oversight used by states. States argue mass surveillance is the most efficient way to protect public safety, but this has clashed with citizen’s interests in privacy, free speech, and the presumption of innocence. The ECHR has ruled mass surveillance technologies have a high risk for abuse and they must be strictly necessary for safeguarding democratic institutions if implemented. As this area of law continues to develop, NGOs have been active in preventing threats to civil liberties and bringing litigation to the ECHR. To balance individual interests in the right to privacy with the state’s interest in security, I suggest individuals continue engaging in democratic participation, states provide safeguards to prevent against abuse of surveillance in legislation, and both individuals and states cooperate to create and use Freedom of Information laws. Mass surveillance has certainly provided a useful tool for intelligence agencies, but it has the potential to make serious erosions on democratic ideals of free speech and privacy if it remains unchecked.

Works Cited

*10 Human Rights Organisations v. the United Kingdom* (App no. 58170/13). 9 January 2014.

*Big Brother Watch and Others v. the United Kingdom* (App no. 58170/13). 9 January 2014.

Convention for the Protection of Human Rights and Fundamental Freedoms (European Human Rights Convention) (Rome, 4 November 1950; T.S. 71(1953)); Cmd. 8969.

Factsheet: Mass Surveillance. European Court of Human Rights, 2016.

Grant, Ruth W., and Robert O. Keohane. “Accountability and Abuses of Power in World Politics.” *American Political Science Review* 99.1 (2005): 29–43.

Griffin, Andrew. “The British Government Just Officially Got the Most Extreme Spying Powers Ever Seen.” *The Independent*. Indepdendent.co.uk 29 Nov. 2016.

“Internet: case-law of the European Court of Human Rights.” European Court of Human Rights, June 2015.

“Investigatory Powers Act – Big Brother Watch.” *Big Brother Watch*, n.d.

Mann, Steve et al. “Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments.” *Surveillance & Society,* 2003.

“Mass Surveillance.” *Privacy International.* N.d.

Newell, Bryce Clayton. “Mass Surveillance, Privacy, and Freedom: A Case for Public Access to Information About Mass Government Surveillance Programs.” (2015): n. pag.

Ni Loideain, Nora. “EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era.” (2015): n. pag.

Richards, Neil. The Dangers of Surveillance, 126 Harvard L. Rev. 1934, 1934-35 (2013).

“Russia Passes Law to Overrule European Human Rights Court.” *BBC News* 4 Dec. 2015. *www.bbc.com*.

Thiessen, Marc A. “Big Brother Isn’t Watching You.” Washington Post. N.p., 10 June 2013.

*Roman Zakharov v. Russia*. (App no. [47143/06](http://hudoc.echr.coe.int/eng" \l "{\"appno\":[\"47143/06\"]}" \t "_blank)). ECHR 4 December 2015.

“UnfollowMe.” Amnesty International, *Amnesty International* N.d.

Zalnieriute, Monika. “An International Constitutional Moment for Data Privacy in the Times of Mass-Surveillance.” *International Journal of Law and Information Technology* 23.2 (2015): 99–133.