The Logic of Secrecy: Digital Surveillance in Turkey and Russia

Article · September 2018

CITATIONS
10

READS
251

1 author:

Hamid Akın Ünver
Özyeğin University
70 PUBLICATIONS **462** CITATIONS

SEE PROFILE

THE LOGIC OF SECRECY: DIGITAL SURVEILLANCE IN TURKEY AND RUSSIA

Turkey and Russia have been developing comparable approaches to digital surveillance. The advent of Internet Communication Technologies (ICTs) and social media platforms have enabled significantly increased systematic state surveillance. From the state's perspective, data-centric digital surveillance is required for two reasons. First, the extent and depth at which terrorist organizations and criminal groups use these platforms for recruitment, logistics and planning. Second, this trend is driven by a variant of "security dilemma" in which one state's intelligence advantage in digital space renders other states relatively less secure, generating a never-ending momentum of digital surveillance capability investment. Turkish and Russian surveillance regimes have grown as two particularly problematic cases in the wider surveillance literature.

Akın Ünver*

TURKISH POLICY QUARTERLY
Summer 2018

* Dr. Akın Ünver is an Assistant Professor of International Relations at Kadir Has University in Istanbul, Turkey and a Visiting Fellow at the Center for Technology and Global Affairs at Oxford University, UK.

Turkey's digital surveillance policy has been shaped by five events: the 2013 Gezi protests, the leakage of wiretapped government conversations (the "17-25 December incident"), the country's growing involvement in the Syrian Civil War and the subsequent refugee influx, successive terrorist attacks through 2015-16, and the failed coup attempt in July 2016.

Turkey's digital surveillance legal framework can be traced back to the beginning of its accession negotiations with the European Union in 2003, when the Accession Partnership Document first emphasized data protection as a prerequisite for membership. Although Turkey adopted this criterion into the EU Accession National Programme, the country did not pursue the matter and draft legislation. The issue reemerged in 2014, largely out of the need to cooperate with EU legal and police institutions EUROJUST and EUROPOL, following the intensification of the Syrian refugee crisis. In addition, the EU 2013 Progress Report had criticized the lack of a dedicated data protection law in Turkey that would enable better cooperation between Brussels and Ankara.[1] A specific source of criticism was that Turkey had adopted a Cyber Security Council and a National Cyber Security Strategy and Action Plan, yet had taken no steps towards the protection of personal data and e-commerce regulations.

It was only in December 2014 that the "Draft Law on the Protection of Personal Data" was finally crafted and was submitted to related EU organs and domestic civil society groups for legal commentary. The resultant amendments were reflected into the revised Draft Law, which was submitted to the Parliament on 18 January 2016.[2] However, the state of emergency declared after the 2016 failed coup attempt put many of the external views and recommendations on the back-burner. In addition, emergency rule gave the government the constitutional authority to rule through statutory decrees, without parliamentary approval.

In this context, Decree Laws 670, 671, and 680[3] allowed for the digital communication interception of individuals whowere actively involved in the coup attempt—or were believed to have taken part (an obscure definition)—and their families. The decrees also granted full authority to Turkey's Information and Communication Technologies Authority (Bilgi Teknolojileri ve İletişim Kurumu, BTK) to take over any service telecommunications service provider believed to be a threat to national

[1] The full version of the 2013 Progress Report can be accessed at: https://www.ab.gov.tr/files/2013%20ilerleme%20raporu/tr_rapport_2013_en.pdf

[2] The 2016 version of the Draft Law on the Protection of Personal Data can be accessed at: https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf

[3] Full versions can be accessed at: Statutory Decree 670 (http://www.resmigazete.gov.tr/eskiler/2016/08/20160817-17.htm), Statutory Decree 671 (http://www.resmigazete.gov.tr/eskiler/2016/08/20160817-18..htm), Statutory Decree 680 (http://www.resmigazete.gov.tr/eskiler/2017/01/20170106M1-2.htm)

security, health and morals of the public (another obscure definition) and finally, to allow the State Cyber Crimes Division to intercept any Internet data traffic without a court order or supervision. CitizenLab—a major Canadian digital rights platform—has identified multiple additional problems with this legal framework, mainly related to political intrusions into the parameters set by the law.[4] For example, the use of spyware application in Turkey skyrocketed after 2015, including deep pocket inspection and mass digital surveillance platforms such as the Phorm, PackageShaper, Remote Control Systems, Hacking Team, FinFisher, and Procera Networks.

"Turkey adopted a Cyber Security Council and a National Cyber Security Strategy and Action Plan, yet has taken no steps towards the protection of personal data and e-commerce regulations."

In Russia, on the other hand, System Operational Investigatory Measures (SORM) has long been the basis of lawful surveillance of digital communications and telecommunication networks. A set of legal and technical requirements that define the legal limits of surveillance, SORM has been updated three times so far, with SORM1 implemented in 1995 (obligatory installment of Federal Security Service hardware to all telecom operators), SORM-2 in 1998 (additional Federal Security Service hardware to be installed on Internet Service Providers' servers) and SORM-3 in 2014 (a more detailed wiretapping system for targeted digital surveillance, with separate specifications for IPv4-IPv6 networks, IMSI-IMEI (International Mobile Subscriber Identity-International Mobile Equipment Identifier) data and Post Office Protocol, Simple Mail Transfer Protocol and Internet Message Access Protocol 4 addresses. Legally, SORM enables surveillance agencies to track and store metadata without a warrant, but a warrant is still required for content. Even when agencies have a warrant, they do not have any responsibility to display the warrant to the target ISP or company, but only for intra-agency audit purposes. The 2016 "Yarovaya Law" (named after Irina Yarovaya, a senior member of the ruling United Russia party) eased these restrictions further, ordering all Internet Service Providers and communication companies to automatically transfer all metadata on agency request without a warrant.[5]

More specifically—and similar to Turkey—Russia's digital surveillance evolution owed much to the 2011-12 mass protests against Vladimir Putin's reascent to the

[4] Bill Marczak, Jakub Dalek, Sarah McKune, Adam Senft, John Scott-Railton, and Ron Deibert. "Bad Traffic: Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?," *The Citizen Lab*, 9 March 2018, https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/

[5] A review of the law in English can be accessed at: https://analytica.digital.report/wp-content/uploads/2017/07/The-Yarovaya-Law.pdf

Presidency in May 2012. Multiple "social media laws" passed after May 2012 have strengthened state monopoly on the media environment, both traditional and digital. By 2014, these laws introduced specific restrictions on news related to Ukraine and most importantly, Crimea. It is also after 2014 that state surveillance and censorship expanded beyond the limits of regime and government criticism. By May 2014, online criticism of any regime component, from the military to the Russian Orthodox Church was considered "extremist speech." This trend grew exponentially more problematic after Russia's entry into the Syrian Civil War in the summer of 2015. Russian think-tank SOVA Center data was quoted in the Human Rights Watch as saying:

> The number of social media users convicted of extremism offences in 2015 was 216, in comparison with 30 in 2010. Between 2014 and 2016, approximately 85 percent of convictions for "extremist expression" dealt with online expression, with punishments ranging from fines or community service to prison time. In the period between September 2015 and February 2017, the number of people who went to prison for extremist speech spiked from 54 to 94.[6]

However, Western democracies too have a mixed record on surveillance. Although Canada, Belgium, Croatia, Norway, Sweden and the Netherlands have made significant progress in creating expert, civilian-led oversight bodies that exist alongside national, formal security committees to restrain their intelligence agencies, the same cannot be said for the United States, United Kingdom, or France. The United States has long been at the forefront of mass surveillance practices. Post-9/11 surveillance operations like Stellarwind[7] have enabled American intelligence agencies (mostly the National Security Agency) to conduct global-scale mass surveillance on digital platforms, Internet Exchange Points (IXPs), and underwater fiber-optic Internet cables. Although much of these draconian surveillance practices were exposed with the "Snowden revelations," the central role of the United States in spearheading some of the most advanced spying technologies is unchanged. It is also mainly the US that drives the global "secrecy dilemma," a concept that I will introduce in the next section, for European countries. Indeed, most major European countries follow the American mass surveillance examples, with varying levels of oversight.

In November 2017, Britain passed the Investigatory Powers Act (IPA), which allowed the Government Communications Headquarters (GCHQ) to conduct mass collection, cataloguing, and interception of "overseas-related" digital activities.[8]

---

[6] "Russia: Assault on Freedom of Expression," *Human Rights Watch*, 18 July 2017, https://www.hrw.org/news/2017/07/18/russia-assault-freedom-expression)

[7] Charlie Savage, "Surveillance and Privacy Debate Reaches Pivotal Moment in Congress," *The New York Times*, 10 January 2018, https://www.nytimes.com/2018/01/10/us/politics/nsa-surveillance-privacy-section-702-amendment.html

[8] The full text of the Investigatory Powers Act 2016 can be accessed at: https://www.legislation.gov.uk/ukpga/2016/25/contents

"Multiple 'social media laws' passed after May 2012 in Russia have strengthened state monopoly on both traditional and digital media environment."

This Act provided a legal basis for "bulk data acquisition" through a warrant, which authorizes the collection of large amounts of transmission, metadata and equipment (hardware data), along with mass-hacking of digital networks throughout the globe. In Germany, on the other hand, an October 2017 "Communications Intelligence Gathering Act"[9] has authorized the Federal Intelligence Service (BND) for bulk collection overseas, as well as large numbers of Germany-based Internet Exchange Points, the latter making the country a unique player in worldwide Internet traffic, as well as surveillance activities of other intelligence organizations around the world. Despite the law's seemingly "domestic" concern, the physical location of IXPs in Germany renders the law truly global, and BND a major player within the systemic surveillance debate. France passed the International Electronic Communications Law[10] following the November 2015 attacks in Paris, enabling Directorate General for External Security (DGSE) to tap, catalog, and store digital data from and to foreign countries, similar to the powers given to GCHQ and BND. Unlike UK and Germany, in the French case it is not the head of DGSE that directly requests bulk collection, but rather it has to originate from the Minister of Defense, Interior, or Finance, who then issues a request to the Prime Minister's Office. Once issued, the storage period of communication content is up to one year, and communication metadata, up to six years.

Rational Actor Model Explanations of Digital Surveillance

The above-mentioned examples demonstrate how democratic, hybrid, and authoritarian countries rely on similar modes of mass surveillance. It is further possible to argue that the extent of mass surveillance and the ability to circumvent legal and parliamentary oversight is a universal policy, which is not contingent upon regime type. This is because how secrecy is produced, processed, and stored goes beyond the regular regime type debate.

Following the Weberian logic that the states are the sole legitimate bodies that can wield organized violence, the same interpretation applies to the role of secrets: States are the sole legitimate bodies that can wield organized and institutionalized

[9] The full text of the Act in English can be accessed at: https://www.loc.gov/law/help/intelligence-activities/germany.php
[10] The full text of the Law in English can be accessed at: https://www.loc.gov/law/help/foreign-intelligence-gathering/france.php

secrecy. The concept of "legitimate secrecy" however, is contingent on regime type, as different political systems understand the concept differently. The reason for this difference in interpretation is the fact that states collect secrets by spending monetary, institutional, and human costs. For a state to conduct surveillance for example, it has to maintain an intelligence bureaucracy, establish tight trust relations within this organization, and acquire and maintain technological infrastructure to process and protect these secrets. Digital surveillance for example, requires technically proficient intelligence operatives, programmers and supervisors, along with high tech computer infrastructure and/or monetary expenditure to outsource these technology items to third parties (i.e. technology surveillance companies). According to the conceptualization by Michael Colaresi, states conduct intelligence and surveillance based on their "secrecy capital."[11] The secrecy capital is structured on an understanding of "secrecy cost," which defines states' abovementioned expenditure of financial, material and institutional costs required to extract, process, and store a single unit of secret. The more a state spends on secrecy—computer infrastructure, encryption or organizational capacity—the better it is able to maximize its intelligence power vis-à-vis other agencies and gain a strategic upper hand.

However, secrecy cost is always subject to the law of diminishing returns. "Easy secrets," defined as a set of information that can be obtained by using comparatively less secrecy cost are usually more common knowledge and already stored by the majority of intelligence agencies. It is the "hard secrets" (secrets that require greater secrecy capital and thus, cannot be afforded by most agencies) that usually face the fiercest battles between agencies. These are highly classified operational information that can only be acquired and processed by a select few and thus, require exponentially larger sums of secrecy capital to be acquired. To that end, countries cannot be "secrecy maximizing" entities. They are rather "secrecy optimizing" units that accumulate secrets based on their own pareto-optimal level of secrecy. This optimal level is defined by a country's threat perception, risk assessment, and political ideology.

Countries that can afford higher sums of secrecy cost will also be able to extract and process secrets from other nations. These foreign secrets can be anything from regime solidarity, public morale, industrial production to military preparedness. Traditionally, states play this game at two levels: State versus state, and state versus society. At the state-state level, states compete to acquire strategic information from each other, as well as protect their own secrets from foreign spies. Just like regular security dilemma, "secrecy dilemma"[12] occurs when states' intelligence maximiz-

[11] Michael P. Colaresi, *Democracy Declassified: The Secrecy Dilemma in National Security* (Oxford Oxford University Press, 2014).

[12] Julian Richards, "Intelligence Dilemma? Contemporary Counter-Terrorism in a Liberal Democracy," *Intelligence and National Security* 27, No. 5, Vol. 1 (October 2012), pp. 761–80.

ing behavior creates a vicious circle, as states spend exponentially greater sums on secrecy costs, paradoxically leaving the other side at a disadvantage. At the societal-level, the state attempts to maximize the information it has on its citizens for a variety of reasons, ranging from benign (i.e. efficient distribution of goods and services, taxation, healthcare, schooling etc.) to securitizing (such as policing, regime/government stability, anti-terrorism and so on).

> *"State are the sole legitimate bodies that can wield organized and institutionalized secrecy."*

In democracies, states' ability to maximize domestic secrets is checked by audience costs—a popular term in political science, which defines the set of popularity and legitimacy penalties states suffer from in cases of overreach, abuse, and corruption. It is only in democracies that for any one unit of secrecy cost, there is another counter-force from the society, which calls for the transparency of the type of information the state tries to extract from the public and keep secret. Who will oversee the process by which leaders are discouraged to abuse secrecy power? How will civil society and the parliament exercise its essential duty to hold the decision makers accountable for their policy choices? Like secrecy is used to mislead and suppress the enemy, it can easily be used to do the same with the public, or oversight institutions. Yet it is only in democracies that these questions are mobilized through electoral, parliamentary, and legal oversight mechanisms; rarely, or never in authoritarian states. In authoritarian states, audience costs can be suppressed through a variety of brute-force tactics, such as imprisonment, censorship, or intimidation. In addition, although audience costs materialize, they cannot be communicated through political, legal, or parliamentary avenues.

Democratic versus Authoritarian Secrets

According to political scientist Michael Desch, the difference between how democracies and authoritarian countries deal with secrecy and surveillance is quite similar, although in democracies, it is the public audience costs and policy punishment that creates the biggest difference.[13] In a democracy, the constraints on how leaders process secrecy and surveillance are institutionalized through an elaborate set of interconnected layers that both insulate secrets from public (and adversarial eye), while simultaneously enable the public to pressure the government when there are

[13] Michael C. Desch, "Democracy and Victory: Why Regime Type Hardly Matters," *International Security* 27, No. 2, Vol. 1 (October 2002), pp. 5–47.

doubts about the handling of such information. From this perspective, there is also a "transparency cost" in democracies that such states have to pay to make certain secrets available for public knowledge. Transparency costs interact with secrecy costs in the sense that every single secret the government makes public for democratic purposes is also automatically shared with the enemy. To offset the transparency cost of such moves, the state then should invest even further to make new information secret, or it will lose a key comparative advantage against rival states.

Even some of the most democratic states abuse secrecy costs. In the 1970s, Canadian Security Intelligence Review Committee (SIRC) exposed how the Canadian Mounted Police had spied on and physically suppressed domestic opposition groups through systematic attacks.[14] In Norway too, a 1990s Lund Commission report identified how the Norwegian police, intelligence, and security apparatus used state resources to spy on domestic opposition initiatives with the intention to disrupt and intimidate them.[15] Yet, the distinguishing feature of democratic and authoritarian abuses of surveillance is the concept of "retrospective accountability"[16] that is a real, transparent, and binding legal punishment against such abuses and overreach. Usually, such abuses are justified by democracies and autocracies alike as "necessary" from a national security point of view—be it for counter-terrorism, or crime fighting. Yet in democracies, there is always an expiration date for such excuses, after which legal and parliamentary commissions are established to retrospectively assess the extent and content of such overreach; a feature, which autocracies do not have.

The tension between security and freedoms in digital space appears precisely at this moment. As states compete for secrets at the international level, they also compete domestically against their societies. Societies push for greater freedoms, privacy, and oversight mechanisms on their security agencies, and states push against almost all of these constraints. Any domestic societal intelligence that is not collected by the state is considered a target for foreign intelligence agencies. In order to prevent foreign intelligence agencies from gaining a comparative advantage, states seek to maximize societal intelligence that they collect and process. Online freedoms and privacy are understood by the states as an unwelcome hindrance—much like rugged terrain in counter-insurgency operations. Both civilians and criminals alike can hide in that space and state reflexes always seek to eradicate any and all similar safe zones. The society then pushes back against states' bid to get rid of this safe space and calls for checks and balances on their states' potential to abuse information collected from the society.

[14] Justin Ling, "The Story of How Canadian Police Committed Arson to Stop a Black Panther Meeting," *VICE News*, June 2017, https://news.vice.com/en_ca/article/eva8da/story-of-how-canadian-police-committed-arson-to-stop-a-black-panther-meeting

[15] Daniel Baldino, ed., *Democratic Oversight of Intelligence Services* (Sydney: Federation Press, 2010), p. 87.

[16] Colaresi (2014), p. 178.

"Even some of the most democratic states abuse secrecy costs."

The elusive middle ground is always hard to find. This is partly because it is a moving target due to the ever-changing contours of communication and information technologies, but also because this sweet spot is culturally contingent. Different electoral cultures have different understandings of secrecy excess, as well as different views on state legitimacy. In some democratic countries, increased secrecy may be viewed as a means to hide corruption and mismanagement. However, in democracies that are faced with direct security threat (cross-border or terrorist), this secrecy may be viewed as necessary. For example, French surveillance practices following the Bataclan ISIS attacks have been considered overreach by voters, and in the absence of the politicians and security chiefs to make a convincing case in favor of the program, public support gradually declined. The decline in public support had direct repercussions for the French government; voters resisted policies to prolong military service requirements or purchase heavy artillery for foreign operations. While intelligence is useful, it cannot on its own mobilize resources for a major conflict or generate favorable public opinion towards supporting allies: Governments must win public consent.

Surveillance or Privacy: Is There a Middle Ground?

Regime type notwithstanding, countries that are under an acute threat (border, or refugee-related, terrorism, crime), are militarily deployed in overseas or cross-border operations, or have recently witnessed one or a series of protests tend to follow a similar policy route in mass surveillance. A country's democratic character significantly influences how frequently it suffers from such problems. Yet, once these problems materialize, regime type has little influence over how intelligence agencies conduct mass surveillance. As dissected in this article, states view any suggestion of legal or parliamentary oversight as an unwelcome intrusion into national security affairs. Especially in political systems when such oversight mechanisms lack technological know-how or have obsolete knowledge on an essentially technology-driven topictopic like digital surveillance. This can incur a real hindrance upon intelligence agencies that need to compete with other state and non-state strategic rivals. For authoritarian states, the debate ends here. But for democracies, this logic creates a deadlock. How can citizens be certain that the decision makers are conducting surveillance purely to counter terrorist threats or criminal activities, and not to spy on political opposition groups or civil society figures? Which political institution makes the decision to securitize a particular domestic target as a threat,

and which legal and parliamentary oversight bodies check, verify, and negotiate with that political institution in cases of overreach and abuse? How will the public know that the country's secrecy capital is spent on foreign threats and not spent on masking corruption, mismanagement, and miscalculation?

> *"Although the French authorities introduced substantially increased surveillance powers following the Bataclan attacks, voters have viewed these powers as 'excessive,' leading to a gradual decrease in public support for surveillance."*

The answer to these questions is inherently cultural in that it depends on a country's political, electoral, and bureaucratic culture, and is also heavily driven by that country's past and recent security environment. The same set of broadened surveillance powers can be understood as "excessive" in a democratic country that has a lower security profile and "necessary" in another democratic country that is deployed in overseas military missions, has a border or refugee problem, and/or has recently suffered from a terrorist attack. Furthermore, states operate in a global environment plagued by the secrecy dilemma and have to compete against other states, as well as non-state and sub-state actors to optimize their intelligence policies. As mentioned above, although the French authorities introduced substantially increased surveillance powers following the Bataclan attacks, voters have viewed these powers as "excessive," leading to a gradual decrease in public support for surveillance.[17] This then spilled over into voter punishment, as the government bid to prolong military service requirements and purchasing heavy artillery equipment to use in foreign missions, were rejected in the parliament.

A likely solution for democracies is the concept of "retrospective accountability." Retrospective accountability attempts to solve the surveillance vs. privacy deadlock by requiring intelligence services to release sensitive information to the parliament gradually, once the time sensitive nature of those secrets expire. For example, although an intelligence agency can exercise its surveillance powers citing terrorism or crime, it must disclose how these powers were exercised (i.e. which institutions and people were spied on, what kind of data was extracted and stored) to a fact-finding task force later on. As a second step, retrospective accountability institutions and structures must be set in place—namely, which legal and parliamentary branches

[17] Ed Vulliamy, "Paris Attacks: Security and Surveillance Cast a Dark Shadow over France's Love of 'liberté' and 'fraternité,'" *The Observer,* 22 November 2015, https://www.theguardian.com/world/2015/nov/22/paris-attacks-security-liberte-fraternite

will oversee and evaluate intelligence disclosures, what is the specific time lag required, and what kind of retrospective legal punishment mechanisms can be exercised in case of demonstrated abuse. For both mechanisms to work, however, a country's offline democratic and legal structures must be strong and functional. Without a nationally agreed upon interpretation of what the rule of law constitutes and a non-partisan mechanism in place to monitor intelligence agencies, the middle ground between security and privacy will remain elusive.

Both Turkey and Russia are locked in a vicious cycle of relative insecurity, risky policy choices, and the resultant need for broadened surveillance powers. However, broadened surveillance powers in turn generate social instability, legal overreach problems, and mass reliance on circumvention and IP masking tools. Social insecurity intensified through draconian surveillance methods in turn render counter-terrorism and crime-fighting tasks more difficult, due to the state's broadly securitizing moves. If Turkey seeks to demonstrate that it is more democratic than Russia, it needs to establish retrospective accountability and legal oversight mechanisms that Russia cannot and will not.