UDK 351.817
https://doi.org/10.18485/fb_ic4hs.2018.6

MASS SURVEILLANCE THROUGH RETAINED METADATA: AN OVERVIEW

Bojan PERKOV[*], Danilo KRIVOKAPIĆ[**], Andrej PETROVSKI[***]

Abstract: Data retention, i.e. collecting bulk data and analysing patterns and anomalies for the entire population under the pretext of national security and fighting crime has been in place for a while in most countries in the world, including Serbia. The research focuses on the mechanisms and practices of accessing retained data by police and government agencies, which brings some transparency and can help understand different aspects and implications of surveillance. Mass surveillance through metadata is one of the most severe threats to privacy. This paper revolves around the issue of accessing retained data through mechanisms that are based on a law, but also on the practices that are in place that do not have a legal basis, i.e. do not include a court order, which is a requirement according to Serbian law. The research methodology has two aspects. The first aspect is the infrastructure, and focuses on the architecture of the ICT network in Serbia. The second aspect is the analytical aspect; it includes an analysis of data regarding the statistics and mechanisms of access to retained data. Data from previous years have shown that state agencies access retained data over 200,000 times every year directly on the servers of one ICT company. Additionally, the difference between the number of requests for retained data that include a court order and independent accesses without one is extremely big. Even though a legal framework exists and the rules of accessing retained data are quite clear, some practices are not in line with the law. Some countries in Europe have set a trend in abolishing data retention altogether as it has proven to be an ineffective manner of fighting crime. This is a positive development and something that should be looked into in the future.

Keywords: data retention, surveillance, privacy, personal data, metadata

[*] MA, SHARE Foundation, Policy Researcher, bojanperkov@sharedefense.org
[**] LL.B., SHARE Foundation, Director, danilo@sharedefense.org
[***] MSc, SHARE Foundation, Director of Tech, a.petrovski@sharedefense.org

1. DATA RETENTION - "COLLECT IT ALL NOW, ACCESS LATER"

In the past 20 years, many aspects of law enforcement have been shifting towards data collection and analysis, not just because of the rise of cybercrime, but also because data are a reliable proof in investigations for all types of criminal activity. Increasing challenges for national security, such as international terrorism, have influenced the introduction of measures such as the mass collection and retention of data on electronic communications of citizens – their emails, phone calls, instant messages, text messages and so on. This so-called "metadata", i.e. data describing communication data, includes information such as the date and time when the communication took place, the duration of this communication, data on the sender, data on the recipient, location data, IP addresses, phone numbers, email addresses and other personal data. In the digital era, you do not need the content of communication to investigate a person's activities, map their daily movement and routines or their social circles and connections. When collected, processed and analysed on a mass scale, these data sets represent a treasure for anyone aiming for uncontrolled mass surveillance of the population. Having all this in mind, "the future-orientation increasingly severs surveillance from history and memory and the quest for pattern-discovery is used to justify unprecedented access to data" (Lyon, 2014: 1).

The first decade of the 21st century was marked by terrorist acts which shook the foundations of Western democracies and instigated governments to rethink their approach to surveillance and communications interception. The United States of America, targeted in September 2001, passed the USA PATRIOT Act ("Patriot Act") soon after the attacks on the World Trade Center in New York City. It gave government agencies and law enforcement unprecedented surveillance powers which significantly reduced the U.S. citizens' right to privacy. Even after the sweeping surveillance revelations by former National Security Agency (NSA) contractor Edward Snowden in 2013, USA FREEDOM Act reforms and many other controversies over the years (Tummarello, 2016), the Patriot Act still stands strong and will almost certainly reach "adulthood" in 2019.

The European Union (EU) took a similar path as the U.S., and after terrorist attacks in Madrid and London in 2004 and 2005 respectively, the EU Data Retention Directive 2006/24/EC was adopted. As early as 2006, the Directive imposed a mandatory communications data retention regime for operators of electronic communications, such as internet service providers or telecommunication services providers, with the duration for keeping the data between six months and two years, depending on how a Member State implemented the Directive. However, in 2014, the Court of Justice of the European Union (CJEU) ruled that the Data Retention Directive was invalid since it seriously undermined the right to privacy and the right to personal data protection of EU citizens in its landmark judgement in joined cases *Digital Rights Ireland* and *Seitlinger and Others* (Back to the Drawing Board: Data Retention Directive Declared Invalid, SHARE Foundation, 2014). This was an important first step towards better protection of citizens' privacy in the EU, but more challenges for the complete abolishment of data retention remained.

After the ruling, it was not exactly clear what this invalidation meant from a legal perspective, or how it would be implemented on the Member State level and what the next steps regarding data retention in the EU were. The CJEU therefore had to issue another,

more detailed judgement in late 2016. The joined cases were *Tele2 Sverige AB v. Swedish Post and Telecom Authority* and *Secretary of State for the Home Department v. Tom Watson and Others,* and the Court's opinion was that EU Member States cannot impose a general regime of communications data retention on providers of electronic communications services (The Member States may not impose a general obligation to retain data on providers of electronic communications services, Court of Justice of the European Union, 2016). The CJEU reasoning was that the "legislation prescribing general and indiscriminate retention of data does not require there to be any relationship between the data which must be retained and a threat to public security" (The Member States may not impose a general obligation to retain data on providers of electronic communications services, Court of Justice of the European Union, 2016: 2) and it "therefore exceeds the limits of what is strictly necessary and cannot be considered to be justified within a democratic society" (The Member States may not impose a general obligation to retain data on providers of electronic communications services, Court of Justice of the European Union, 2016: 2).

However, even in spite of the second landmark CJEU judgement on practically the same matter, data retention still haunts EU citizens. In June 2018, a group of more than sixty NGOs, community networks, academics and activists sent an open letter to the European Commission, explaining that blanket data retention, still in practice in 17 EU Member States, is not in accordance with EU law and asking for change (Massive claims against unlawful data retention, Stop Data Retention, 2018). Since the EU has adopted a new set of data protection rules, i.e. the General Data Protection Regulation (GDPR) and the Law Enforcement Directive, they are expected to bring important changes to the way EU citizens enjoy their rights to privacy and personal data protection and how their data are used for law enforcement purposes.

2. CURRENT STATE OF DATA RETENTION IN SERBIA

In 2017, 68 per cent of households in Serbia had an internet connection (Usage of Information and Communication Technologies in the Republic of Serbia in 2017, Statistical Office of the Republic of Serbia, 2017: 14), whereas 53 per cent of households had access to the Internet via mobile phones or tablets using the 3G network – a large increase from 18 per cent in 2015 (Usage of Information and Communication Technologies in the Republic of Serbia in 2017, Statistical Office of the Republic of Serbia, 2017: 17). Also, it is estimated that almost five million people in Serbia use a mobile phone (Usage of Information and Communication Technologies in the Republic of Serbia in 2017, Statistical Office of the Republic of Serbia, 2017: 22). Tablets, smartphones and other devices that keep us constantly connected have become an essential part of our everyday lives, but have also caused us to produce more data about ourselves and our habits than ever before.

In the Republic of Serbia, mandatory data retention for all electronic communications for the duration of 12 months from the date of communication is prescribed in the Law on Electronic Communications, which was adopted in 2010 and most recently amended in 2014. However, the legal framework was not harmonized, since laws on security services

had loopholes which enabled access to citizens' data and communications without a court order. In 2012, provisions of the law regulating the work of Serbia's military agencies, which granted the Military Security Agency (MSA) (Vojnobezbednosna agencija, VBA) powers to access citizens' data from telecom operators, were declared unconstitutional. A year later, three provisions of the Law on Security Information Agency (SIA) (Bezbednosno-informativna agencija, BIA), the Serbian secret service focused on civilian matters, were also struck down by the Constitutional Court of Serbia (Ustavni sud RS). Finally, in June 2013, provisions of the Law on Electronic Communications which ignored the constitutional guarantees of communications secrecy by enabling access to retained data without a court order were deemed unconstitutional, forcing the adoption of amendments to the Law (Communications Data Retention in Serbia: How much are we being surveilled? (2014-2016), SHARE Foundation, 2017).

As a mechanism of transparency and control of access to citizens' retained communications data, Article 130a of the Law on Electronic Communications prescribes that all operators of electronic communications in Serbia and state bodies authorised to access retained data submit annual *records on access to retained data* to the Commissioner for Information of Public Importance and Personal Data Protection of the Republic of Serbia (Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti RS) (Law on Electronic Communications, 2014). These records are a foundation for researching the data retention practices of operators and access to the data by state authorities. SHARE Foundation, an expert think-tank from Serbia focused on advocacy and research at the intersection of human rights, technology and law, obtained these records using a freedom of information request for four consecutive years, from 2014 to 2017, and will continue with this yearly practice.

It is important to note that these records only contain statistical data (number of received requests for access to data, number of granted requests, dates, authority which submitted the request etc.), the publication of which cannot endanger the national security of Serbia or criminal investigations. Also, publishing these statistics is important for the public oversight, transparency and accountability of state authorities carrying out surveillance and is therefore in the public interest. The European Court of Human Rights (ECtHR) affirmed the public's right to know when it comes to statistical data on surveillance, i.e. the number of people in Serbia placed under electronic surveillance by the Security Information Agency during one year (Youth Initiative for Human Rights v. Serbia, European Court of Human Rights, 2013).

On a practical level, state authorities access retained communications data in two ways: through submitting requests to the operators (by email, fax, phone or in person) and by directly accessing the operators' information systems through dedicated applications. While the first way has a legal basis and offers more protection to citizens' rights to privacy and protection of their personal data, independent (direct) access is a highly controversial measure of very dubious legality, which makes arbitrary access to citizens' data possible.

Analysis of mobile network data surveillance by SHARE Foundation (Invisible Infrastructures: Surveillance Architecture, SHARE Foundation, 2015), based on the

documents obtained from the Commissioner for Information of Public Importance and Personal Data Protection, has shown that between March 2011 and March 2012, i.e. during one year, the Ministry of Interior, VBA[1] and BIA[2] independently accessed Telenor's database more than 270,000 times (Proceedings of oversight of implementation of the Law on Personal Data Protection by Telenor, Commissioner for Information of Public Importance and Personal Data Protection, 2012: 16). Data on Telenor from more recent years show that this practice has continued, showing that retained data were accessed independently slightly more than 200,000 times, almost exclusively by the Ministry of Interior. In 2015 and 2016, the numbers were even higher – around 300,000 for each year. Telenor, the second largest mobile operator in Serbia, is the only one which registers instances of direct access to retained data made by the competent authorities in addition to the requests received through the regular procedure – or is the only one reporting the statistics on direct access. Given the scope of direct access, it seems logical to assume that the practice of direct access by competent authorities exists with other operators, but that they either do not record these approaches or do not want to report them to the Commissioner. We confirmed this conclusion in the report of the Military Security Agency, which states that "access to retained electronic communications data is obtained through VIP, Telenor, MTS and Telekom's access applications" (Communications Data Retention in Serbia: How much are we being surveilled? (2014-2016), SHARE Foundation, 2017). According to data obtained from the Commissioner for 2017, Telenor remains the only operator which provides information about independent access in their report, recording 381,758 instances of direct access to retained communications data.

When we take into account the market share of mobile operators in Serbia for the second quarter of 2018, Telekom Serbia as the largest operator covered 45.4% of users, Telenor 31.3%, VIP 23.2% and virtual mobile operators had 0.1% of the market share (An overview of the electronic communications market in the Republic of Serbia - the second quarter of 2018, Regulatory Agency for Electronic Communications and Postal Services, 2018: 8). If we make a realistic assumption that there was a similar number of direct access instances in the cases of Telekom Serbia and VIP to those of Telenor, the total number of direct access instances in Serbia could be estimated at one million.

3. FUTURE OF DATA RETENTION IN SERBIA

For some time now, there are intentions to adopt a new Law on Electronic Communications and in late 2016 the Ministry of Trade, Tourism and Telecommunications presented a draft of the new law. The draft practically confirmed that the provisions of the current Law on Electronic Communications related to the secrecy of electronic communications, legal interception of communications and retention of metadata will continue to apply even after the adoption of a new law until there is a separate law regulating these issues. This means that the lawmakers have decided not to change the legal framework at this time, but a completely new law opens the possibility

[1] Military Security Agency

[2] Security Information Agency

for better adjustment to EU standards on the one hand, and carries the risk of further reducing citizens' right to privacy on the other. The draft law envisaged the mandatory registration of electronic communications subscribers, which is a highly controversial measure as it could also include user registration of prepaid SIM cards, which the current law does not prescribe (Communications Data Retention in Serbia: How much are we being surveilled? (2014-2016), SHARE Foundation, 2017).

As the new Law on Electronic Communications is expected, data retention in its current form needs to be considered, especially in the wake of new developments in the EU, where some Member States are still quite reluctant to completely give up on their data retention policies. The "collect and store all data by default" approach to data retention will certainly need to be changed, since it is a very intrusive measure for the privacy and secrecy of citizens' communications, employed without adequate transparency and safeguards.

4. REFERENCES

Commissioner for Information of Public Importance and Personal Data Protection. (2012). Proceedings of oversight of implementation of the Law on Personal Data Protection by Telenor. Retrieved July 2, 2018, from https://labs.rs/Documents/ZapisnikTelenor.pdf

Court of Justice of the European Union. (2016). The Member States may not impose a general obligation to retain data on providers of electronic communications services. Retrieved June 25, 2018, from https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-12/cp160145en.pdf

European Court of Human Rights. (2013). Youth Initiative for Human Rights v. Serbia, App. no. 48135/06. Retrieved June 28, 2018, from http://hudoc.echr.coe.int/eng?i=001-120955

Law on Electronic Communications. (2014). Official Gazzette of the Republic of Serbia, 44/2010, 60/2013 - Constitutional Court judgement and 62/2014. Retrieved June 28, 2018, from https://www.paragraf.rs/propisi/zakon_o_elektronskim_komunikacijama.html

Lyon, D., (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. Big

Data & Society, 1(2), 1-13. https://doi.org/10.1177/2053951714541861

Regulatory Agency for Electronic Communications and Postal Services. (2018). An overview of the electronic communications market in the Republic of Serbia - the second quarter of 2018. Retrieved September 21, 2018, from https://www.ratel.rs/uploads/documents/empire_plugin/Q2%202018%20ENG.pdf

SHARE Foundation. (2017). Communications Data Retention in Serbia: How much are we being surveilled? (2014-2016). Retrieved June 28, 2018, from https://labs.rs/sr/zadrzavanje-podataka-o-komunikaciji-u-srbiji/

SHARE Foundation. (2015). Invisible Infrastructures: Surveillance Architecture. Retrieved July 2, 2018, from https://labs.rs/en/invisible-infrastructures-surveillance-achitecture/

SHARE Foundation. (2014). Back to the Drawing Board: Data Retention Directive declared invalid. Retrieved June 25, 2018, from http://www.shareconference.net/sh/defense/back-drawing-board-direktiva-o-zadrzavanju-podataka-nevazeca

Statistical Office of the Republic of Serbia. (2017). Usage of Information and Communication Technologies in Republic of Serbia in 2017. Retrieved September 20, 2018, from http://publikacije.stat.gov.rs/G2017/PdfE/G20176006.pdf

Stop Data Retention. (2018). Massive claims against unlawful data retention. Retrieved June 27, 2018, from http://stopdataretention.eu/

Tummarello, K., (2016). Debunking the Patriot Act as It Turns 15. Retrieved June 25, 2018, from https://www.eff.org/deeplinks/2016/10/debunking-patriot-act-it-turns-15