The collision of national Security and Privacy in the age of information technologies

Ilin Savov
Associate Professor
University of Security and Economics, Plovdiv, Bulgaria

Abstract
Potential transatlantic privacy standards for surveillance in the context of national security are analysed in this article. Dynamic EU-US relations concerning the opportunity for data exchange are scrutinised. A review has been made regarding the key features of a human rights compliant legal framework, and producing a joint set of principles.

Keywords:
national security, privacy and protection of personal information, data exchange, surveillance, tapping

Introduction

The boom of technologies and communications radically changed the world we live in. Information technologies completely redesigned the nature of interpersonal interactions. Social media allow every individual to share information anywhere around the globe within seconds, and the global network offers us digital storage in which everyone can store personal or professional information at a low price or for free. Apart from the effects on trading and international relations, these changes had an unprecedented influence on human rights.

On the one hand, communication technology innovations created possibilities for protecting fundamental human rights and freedoms by giving activists a louder voice, as they were given new means of documenting abuses and new ways of promoting their ideas. Just like experience from previous events shows us — events like the uprising of the 'Arab Spring'; the attacks that took place on European territory in Bulgaria (Burgas) in 2012, in France (Paris, Nice) and in Belgium in 2014, 2015 and 2016; the latest events in Turkey (the acts of terrorism

in Istanbul and the military coup attempt on 15 July); the armed uprising in Armenia and the events in Kazakhstan (the attempted mutiny ([1])) in 2016 — smartphones and social media improved access to information for all members of society; they provided greater freedom of expression and encouraged citizen participation in political processes. On the other hand, however, digital revolution also brought up great new challenges in the area of human rights protection. The internet assists and facilitates terrorist networks like those of Al-Qaeda and ISIS ([2]) in spreading their beliefs and planning destruction of life and property.

Discussion

In the context of fighting against terrorism, the advance of telecommunications and the rise of digital technologies brought up unprecedented challenges concerning privacy and protection of personal information. After the terroristic attacks on 11 September 2001 in the United States, in Spain in 2004, and in the United Kingdom in 2005, governmental institutions considerably extended their abilities for the surveillance and monitoring of individuals in order to enhance national security and to prevent potential threats of terrorism. These are obtained in two ways — in a direct way, by giving their own security and law enforcement agencies the ability to monitor and tap electronic communications, or by delegation of these tasks to the private sector (e.g. obliging internet and telephone services providers to retain electronic communications traffic data for long periods of time and to supply law enforcement and special agencies with these data when needed). Governments of different countries greatly enhanced their abilities to find and monitor individuals by tapping their communications. Despite the reasonable concerns about national security, and state and supranational institutions' duty to provide security for their citizens and protection from terrorism, the implementation of this all-embracing surveillance method raised concerns about privacy.

Privacy and protection of personal information are deeply rooted in national constitutions, as well as in many international agreements concerning human rights. Article 12 of the Universal Declaration of Human Rights of 1948, Article 8 of the European Convention on Human Rights of 1950, and Article 17 of the International Covenant on Civil and Political Rights of 1966 are all such examples. In the case of justice in countries with older constitutions, recognition of privacy is a result of decisions made by supreme and constitutional courts in particular legal cases. Such an example is the decision of the Supreme Court of the United States, which recognises the right to privacy with the Fourth Amendment to the United

([1]) Mutiny is a criminal conspiracy among a group of people (typically members of the military or the crew of any ship, even if they are civilians) to openly oppose, change, or overthrow a lawful authority to which they are subject. The term is commonly used for a rebellion among members of the military against their superior officer(s), but can also occasionally refer to any type of rebellion against an authoritative figure.

([2]) The Islamic State of Iraq and the Levant (ISIL), also known as the Islamic State of Iraq and Syria (ISIS), Islamic State (IS), and by its Arabic language acronym Daesh, is a Salafi jihadist militant group that follows a fundamentalist, Wahhabi doctrine of Sunni Islam.

States Constitution ([3]) that prohibits unreasonable searches and seizures. It is necessary to observe that Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ([4]) include the right to respect for private and family life and protection of personal data concerning the individual. Despite the disputes and debate between international law experts, there is a consensus on the idea that privacy should at least protect the area of intimate relationships from state bodies' interference.

The recent disclosures about state bodies of the United States and some EU Member States' regular practice of phone calls, emails and text messages bulk data collection prove that the right to privacy is under considerable pressure for the sake of fighting against terrorism. Restrictions on personal rights in relation to national security are further complicated by some factors. For example, there is no existing possibility for adequate and objective monitoring over some of the surveillance programmes that have been created and are being practiced in top secret conditions. Because of the extremely great abilities of modern digital communications through which data transfer anywhere in the world is achieved within seconds, surveillance programmes provide national security agencies with the opportunity to monitor people's actions worldwide.

Developed countries that have highly developed technological intelligence services are capable of practicing mass surveillance and tapping their own borders. As a result of the increasing collaboration between intelligence and law enforcement agencies both at local and at international level, the information collected through surveillance programmes becomes their basic exchange value.

Despite the various levels of protection of personal data that most legal systems provide to their citizens, the reality of the transnational collaboration practically allows governments to circumvent constitutional protections of citizens' privacy, while foreign bodies are relied on for embarking on illegal surveillance of the local citizens. It should be observed that disclosures (that is, data leaked by Edward Snowden, former National Security Agency agent) about governments' existing massive programmes for surveillance, in combination with increasing awareness about the negative impact that these measures have on privacy rights, started an international debate about whether there is a balance between privacy and security in the age of information technology. Following a proposal by Brazil and some of the EU Member States, in December 2013 the United Nations General Assembly adopted a resolution restricting the execution of programmes for control over citizens. It should be observed that a great number of the US government members were occupied

([3]) The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

([4]) The Charter of Fundamental Rights recognises the range of personal, civil, political, economic and social rights of the citizens and residents of the EU, by combining them in EU law.

with reconsideration of legality and efficiency concerning data collection and tapping by security agencies that use surveillance technologies.

In turn, the US Congress took measures for amending the legislation in that direction. The European Parliament responded with a resolution in March 2014, which strictly criticised the US programmes for surveillance and tapping of EU members. Following this, with a resolution of 8 April 2014 the Court of Justice, in extended composition, invalidated Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006. The Court of Justice's decision was motivated by the lack of plain and precise rules in the directive for setting the scope of and minimum requirements for interference in fundamental rights, and the lack of sufficient measures that would provide efficient protection of retained data, guaranteeing that there would be no abuses, no illegal access and use of traffic data. These flaws have motivated the Court to invalidate the directive concerned despite the existing legitimate aim, namely, enhancing public security and international peace and security by providing efficiency in fighting against grave offences and acts of international terrorism.

The Court stated the following:

> *'… data … are particularly important and therefore a valuable tool in the prevention of offences and the fight against crime, in particular organised crime. It must therefore be held that the retention of data for the purpose of allowing the competent national authorities to have possible access to those data, as required by Directive 2006/24/EC, genuinely satisfies an objective of general interest.'*

New threats and challenges in relation to the protection of national security on the one hand and protection of personal correspondence on the other hand compelled the governments on both sides of the ocean to work on developing privacy standards. A significant step in that direction would be to guarantee efficient control of surveillance and tapping activities of national security agencies. There are several EU-US agreements allowing bulk data sharing of air passenger and financial transaction records, and a Mutual Legal Assistance Treaty ([5]) (MLAT) allowing a case-by-case sharing of law enforcement information. The two parties have been attempting to negotiate an overarching data protection agreement, as urged by the European Parliament, but have so far found their differences insurmountable. The EU-US Mutual Legal Assistance Treaty (Agreement on mutual legal assistance between the European Union and the United States of America, OJ L 181, 19.7.2003, pp. 34-42) was agreed in 2003, but not concluded until November 2009. It allows the use of shared data for the purpose of criminal investigations and proceedings, and for preventing an 'immediate and serious threat to ... public security'. Both non-governmental organisations (NGO) and industry have called for all future US foreign data collection to take place through such MLATs, and that the Unites States 'desist from any and all data collection measures which

([5]) A mutual legal assistance treaty (MLAT) is an agreement between two or more countries for the purpose of gathering and exchanging information in an effort to enforce public laws or criminal laws.

are not targeted and not based on concrete suspicions' (Reform Government Surveillance campaign principles).

In response to the final report from the High-Level Contact Group, the European Data Protection Supervisor ([6]) (EDPS) suggested a number of principles that should guide an EU-US sharing agreement. Most are at least partially included in the European Commission negotiating mandate, but some remain controversial with the US government ([7]):

- Clarification as to the nature of the instrument, which should be legally binding in order to provide sufficient legal certainty.
- A thorough adequacy finding, based on essential requirements addressing the substance, specificity and oversight aspects of the scheme. The EDPS considers that the adequacy of the general instrument could only be acknowledged if combined with adequate specific agreements on a case-by-case basis.
- A circumscribed scope of application, with a clear and common definition of law enforcement purposes at stake.
- Precisions as to the modalities according to which private entities might be involved in data transfer schemes.
- Compliance with the proportionality principle, implying exchange of data on a case-by-case basis where there is a concrete need.
- Strong oversight mechanisms and redress mechanisms available to data subjects, including administrative and judicial remedies.
- Effective measures guaranteeing the exercise of their rights to all data subjects, irrespective of their nationality.
- Involvement of independent data protection authorities, especially in relation to oversight and assistance to data subjects.

Internationally, not only governments, but also civil society groups have identified some key features of the human rights compliant legal framework, and produced a joint set of principles that have been endorsed by over 200 organisations. These include the following:

([6]) The EDPS is an independent supervisory authority whose primary objective is to ensure that European institutions and bodies respect the right to privacy and data protection when they process personal data and develop new policies.

([7]) Opinion of the EDPS on the final report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection, 8 November 2011.

- Intelligence agencies should only have targeted, limited access to data. The Electronic Frontier Foundation (EFF) ([8]) suggests 'a specific person or specific identifier (like a phone number or email address), or a reasonable, small and well-cabined category (like a group on the terrorist list or member of a foreign spy service)' (Cohn and Timm, 2013), 'What Should, and Should Not Be in NSA Surveillance Reform Legislation'). European Digital Rights (EDRi) ([9]) suggests a ban on 'all data collection measures which are not targeted and not based on concrete suspicions.'
- Agency access should be to specific records and communications. They should not be authorised to undertake bulk, pervasive or systematic monitoring, which has the capacity to reveal private information far in excess of its constituent parts. Any data access should trigger legal protections — this should not come only when data are picked out of a large data stream already collected by an agency.
- Data collected using special national security powers should be completely blocked from use for other government purposes, including law enforcement. They should be retained for limited periods and deleted once no longer required.
- Metadata (communications data) can be extremely revealing about individuals' lives, and currently receives very low levels of legal protection. This was highlighted by the Court of Justice in its judgment invalidating Directive 2006/24/EC, which required the retention of such data for a period of up to 2 years (Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others (C-293/12), and Karntner Landesregierung, Michael Seitlinger, Christof Tschohl and others (C-594/12)). The EFF has called for the requirement of a probable cause warrant for agencies to access previously non-public information, e.g. revealing identity, websites and info accessed, 'who with/where/when' people communicate.
- The incorporation of privacy-protective technologies and limitations within surveillance systems.
- Illegal surveillance should be criminalised, with effective remedies when individuals' rights are breached. Illegally gathered material should be inadmissible as evidence, while whistle-blowers should be protected for revealing illegal behaviour. EDRi has demanded 'that any foreign data collection measures include provisions giving all affected individuals, at the very least, equal rights to US citizens at all stages of an investigation, rights that are not significantly lower than any democratically approved safeguards in

([8]) The EFF is an international non-profit digital rights group based in San Francisco, California. The EFF provides funds for legal defense in court; presents amicus curiae briefs; defends individuals and new technologies from what it considers abusive legal threats; works to expose government malfeasance; provides guidance to the government and courts; organises political action and mass mailings; and supports some new technologies which it believes preserve personal freedoms and online civil liberties.

([9]) EDRi is an international advocacy group headquartered in Brussels, Belgium. EDRi was founded in June 2002 in Berlin by 10 NGOs from seven countries. In March 2015, the European Council adopted a proposal that may compromise net neutrality, a major concern of EDRi.

their country of residence.' The European Commission is also pushing for this in their negotiations with the United States over a data sharing privacy agreement.

The referendum conducted on 25 September 2016 in the Swiss Confederation should be observed as an indisputable argument in favour of enhancing the competences of intelligence agencies concerning protection of national security through restriction of personal freedom and privacy.

During this referendum nearly 60 % of Swiss citizens responded positively to the proposal for providing the Swiss intelligence agency with legal rights so that the agency can enhance the monitoring of phone calls and internet correspondence, and use tapping devices for the fight against terrorism and grave offences, which would restrict personal freedom.

Here a conclusion could be reached that the content of the collision of national security stability and state system protection, in the context of implementing temporary restrictions on particular individuals' privacy, is too variable in today's circumstances. Competent state agencies are to enhance their abilities for preliminary surveillance and monitoring of events, occurrences and processes that could be a potential threat to national security, while minimising the impact on privacy.

A non-secret treaty basis for exchanging information, approved by the US Congress and EU Parliament and which meets European Convention on Human Rights standards is the best long-term enabler of bringing intelligence data collection and sharing within a transparent and genuinely human rights compatible framework.

The greatest area of EU-US disagreement is over the remedies available to non-US citizens and permanent residents when their privacy rights are breached. As a matter of policy the US Department of Homeland Security applies the protections in the US Privacy Act of 1974 to both citizens/permanent residents and visitors, giving everyone the right to access and correct their own personal data (US Department of Homeland Security, Privacy Policy Guidance Memorandum 2007-1). However, because the privacy act's definition of 'individual' applies only to the former, the latter has no right of judicial review. Obtaining this is a key goal of the EU and has been promised by the US administration.

Conclusion

As a conclusion, it should be pointed out that a range of potential transatlantic privacy standards for surveillance have been developed by civil society groups, courts and watchdogs such as the European Data Protection Supervisor. These cover data sharing, surveillance activities and oversight of intelligence agencies. The principal opportunities for implementing them are in EU-US negotiations over a data sharing privacy agreement. The Council of Europe and state-state negotiations over intelligence sharing are also possible venues.

References

- Cohn, C. and Timm, T. (2013), What Should, and Should Not Be in NSA Surveillance Reform Legislation. Retrieved from https://www.eff.org/de/deeplinks/2013/08/what-should-and-should-not-be-nsa-surveillance-reform-legislation
- Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, OJ L 195, 27.07.2010, pp. 5-14.
- European Commission, Report on the second joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program (TFTP), SWD(2012) 454 final, 14 December 2012.
- Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others (C-293/12), and Karntner Landesregierung, Michael Seitlinger, Christof Tschohl and others (C-594/12).
- US Department of Homeland Security, Privacy Policy Guidance Memorandum 2007-1.