EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 8/2015

Dissemination and use of intrusive surveillance technologies

15 December 2015

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 41.2 of Regulation 45/2001 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies', and '…for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data'. He was appointed in December 2014 together with Assistant Supervisor with the specific remit of being more constructive and proactive. The EDPS published in March 2015 a five-year strategy setting out how he intends to implement this remit, and to be accountable for doing so.

This Opinion follows on from the EDPS's previous Opinion on the General Data Protection Regulation which aimed to assist the main institutions of the EU in reaching the right consensus on workable, future-oriented set of rules which bolsters the rights and freedoms of the individual. Like the Opinion on Mobile Health in early 2015, it addresses the challenge of data protection to 'go digital' - the third objective of the EDPS Strategy – 'customising existing data protection principles to fit the global digital arena', also in the light of the EU's plans for the Digital Single Market. It is consistent with the approach of the Article 29 Working Party on data protection aspects of the use of new technologies, such as the ´Internet of Things´, to which the EDPS contributed as a full member of the group.

This Opinion addresses the data protection and privacy issues raised by the dissemination and use of intrusive surveillance technologies.

Executive Summary

The EDPS addresses in this Opinion the data protection and privacy issues raised by the dissemination and use of intrusive surveillance technologies. The use of these tools implies by default the processing of personal data and a possible intrusion of privacy: the main goal of intrusive surveillance tools is to remotely infiltrate IT systems (usually over the Internet) in order to covertly monitor the activities of those IT systems and over time, send data back to the user of the surveillance tools.

While such tools can be instruments for legitimate (and regulated) use by law enforcement bodies or intelligence agencies, they can be also used as "Trojan horses" to circumvent security measures in electronic communications and data processing.

The tension between the positive use of ICT tools and the negative impact that the misuse of technology can have on human rights, and especially on the protection of personal data and privacy, has to be addressed by national and EU policies, and by all actors involved in the ICT sector (developers, service providers, sellers, brokers, distributors, and users).

In this Opinion, the EDPS proposes to address the threat constituted by the use of intrusive surveillance technologies with the following actions:

- An assessment of the existing EU standards for ICTs should be performed, with the purpose to increase the protection of human rights, especially in case of exportation of surveillance or interception technology and related services;
- The use and dissemination (including inside the EU) of surveillance and interception tools, and related services, should be subject to appropriate regulation, taking into account the potential risk for the violation of fundamental rights, in particular the rights of privacy and data protection;
- Consistent and more effective policies should be developed by the Council of the EU, the European Parliament, the European Commission and the EEAS regarding the export of intrusive surveillance tools in the context of dual-use technologies, at EU and international level;
- Up-to-date policies should regulate “0-day” exploits and vulnerabilities in order to avoid their use for fundamental rights violations;
- EU policies on cybersecurity should take into account the dissemination of interception and surveillance technologies and address specifically this issue within the appropriate legislation;
- Investments in security on the Internet and initiatives to embed privacy by design in new technological solutions should be fostered;
- A consistent approach should be put into place to grant international protection to whistle-blowers who contribute to revealing violations of human rights through the use of interception and surveillance technologies.

TABLE OF CONTENTS

1 The context

In the beginning of July 2015[1], an Italian company was the victim of a major data breach. The attackers stole a large amount of data (reportedly more than 400 Gigabytes) and published it on the Internet. The published data contained internal documents, audio recordings, e-mail correspondence, employee passwords, client lists and, more importantly for the purpose of this Opinion, technical information and source code of an advanced piece of software designed for intrusive surveillance.

According to the media[2], this intrusive surveillance software would allow its user to bypass encryption, collect data out of any device and monitor a target covertly and remotely[3]. In addition, law enforcement bodies and intelligence agencies would be the potential customers, at the same time limiting the offer to governments or countries not blacklisted by the U.S., E.U., U.N., NATO or ASEAN[4]. However, the media[5] has reported that the software might have been sold to "governments and security services of Azerbaijan, Kazakhstan, Uzbekistan, Russia, Bahrain, Saudi Arabia and the UAE, many of whom have been criticised by international human rights organisations for their aggressive surveillance of citizens, activists and journalists both domestically and overseas".

Several companies are actors in this part of the cybersecurity field and provide related services[6]. Evolving in the same sphere of activities, other companies[7] operate in the cybersecurity business by trading in so-called "exploits" (chapter 2.2) which allow intrusive surveillance tools to be used to their full potential. The business model of such companies consists of providing customers with the technical capabilities necessary to perform attacks on IT systems.

This Opinion is focused on the specific case of intrusive surveillance tools which are designed, marketed and sold for (mass)surveillance, intrusion and exfiltration. These tools are used to attack systems of defined targets. It does not address the broader political debate about possible regulation of network and information security technologies, such as limiting encryption[8] and the mandatory weakening of security systems by using backdoors[9].

2 Concepts and technical implications

The main goal of intrusive surveillance tools is to remotely infiltrate IT systems (i.e. over the Internet) in order to covertly monitor the activities of those IT systems and, over time, send data back to the user of the surveillance tools. In order to understand how this purpose is achieved, the explanation of the intrusive surveillance tools can be divided in two parts: the management part (chapter 2.1) and the exploits (chapter 2.2). We will then look at some key technical consequences related to the use of this type of software (chapter 2.3).

2.1 Management part of intrusion and surveillance tools

In essence, the management part of intrusive surveillance tools can be defined as an advanced software to manage infiltration of targets and to deliver users exploits (see also chapter 2.2) concerning targets of their interest in a user-friendly way.

Typically, the user has a graphical interface that allows him/her to:

- Input the IP (Internet Protocol) address of an IT system connected to the Internet (target) in order to collect basic data on that target such as the type of Operating System

(OS) running, the services running (e.g. web server, email server, etc.), geolocation information, etc.. This first step is useful in order to determine how best to attack that target.

- Manage and launch attacks on targets in an effort to infiltrate them and collect data from those targets. Attacks may take many forms but are typically performed by using exploits (discussed in chapter 2.2).

- Once a target is infiltrated, further compromise the target (i.e. try to bypass local security measures active on the target by using other exploits in order to be able to perform more operations, gain privileges, or access more data processed by the target) and install a small piece of software that would collect data and send it to the user of the surveillance tools (akin to a Trojan Horse[10]).

- Use a compromised target in order to launch an attack against another interconnected target.

- Keep track of targets already infiltrated and of the data received/exfiltrated from those targets. These data are the prime reason for using intrusive surveillance tools and may contain any data processed by the target such as browsing data from any browser used on that target, e-mails sent and received, files residing on the hard drives accessible to the target (files located either on the target itself or on other IT systems to which the target has access), all logs recorded, all keys pressed on the keyboard (this would allow collecting passwords), screenshots of what the user of the target sees, capture the video and audio feeds of webcams and microphones connected to the target, etc.

This list of functionalities is of course non-exhaustive. It should however be sufficient to analyse the consequences of the use of such tools in the context of this Opinion.

2.2 Exploits

Exploits are small pieces of software, sequences of commands or pieces of data that are designed to take advantage of a flaw/vulnerability in the software of the targeted IT system in order to cause an unintended and unanticipated reaction of that software. Often the objective is to craft the exploit in such a way that the automatic reaction of the attacked software leads to the attacker gaining some kind of control over or access to the target.

An exploit can only exist if there is a flaw/vulnerability in a piece of software. Flaws/vulnerabilities are discovered over time by researchers, software vendors, the public and may occur in any software such as MS Windows, Linux, MAC OS X, Android, Apple iOS, Blackberry OS or any other OS, and also software used with and through the Internet such as Adobe Flash (used on a big number of websites including Youtube, Google, etc.), Firefox, Safari, Internet Explorer etc.

Usually, once a software vendor is informed of a flaw/vulnerability in his product, he can fix the issue and provide a new version of the software to the public. Once the updated software is installed on an IT system, that IT system can no longer be affected by the corresponding exploit.

"0-day" exploits is a term used to designate exploits using a flaw/vulnerability unknown to the vendor of the software and for which there is no existing fix. These types of exploits are

valuable since they are very likely usable to successfully attack a system running the corresponding flawed software. The prices for exploits can go beyond 100.000 euros, depending on numerous technical factors[11].

In the case of HT, an exploit that was widely reported by the media related to the Adobe Flash software[12]. This exploit affected the latest version of the Adobe Flash software at the time running on a variety of platforms and browsers. It allowed the attacker to execute any program of his/her choice on the target. A credible scenario for an attack would have been:

- a user surfs the web using a vulnerable version of Adobe Flash on his computer. The user accesses a website containing Adobe Flash content (such as a video) that contains the exploit;
- the user's computer plays the Adobe Flash content and at the same time runs the exploit, with no visible sign for the user;
- the attacker (the one who has prepared the Adobe Flash content with the exploit) now has access to the user's computer with the same rights as the user;
- the attacker can now run additional exploits to gain more access to the user's computer and/or he/she can install a piece of software that would communicate data back to him/her.

A large market exists[13] for exploits such as the one just mentioned, because they are extremely useful in the context of surveillance tools. Furthermore, without these exploits, infiltrating an IT system would be much more difficult and would require a more active participation by a user that has already access to the target. The companies concerned have a strong interest in keeping the knowledge of these flaws/vulnerabilities closely guarded.

2.3 Technical implications

Given the data breaches that have been widely publicised on the Internet[14], intrusive surveillance software is now available to the public at large. According to the press, "*sufficient code was released to permit anyone to deploy the software against any target of their choice"; "…ability to control who uses the technology has been lost.", "We believe this is an extremely dangerous situation"*[15].

It should be noted that once an exploit (and associated flaws/vulnerabilities) has been disclosed, software vendors issue patches or new versions of their software that are not prone to the same attacks. Provided the user base has installed these new versions or patches, the users will be safe from these particular issues. This demonstrates the importance for any entity (private companies, public organisations or individuals) to keep track of which software it uses and quickly update its IT systems.

Nevertheless, in their own interest, providers and users of these surveillance tools would not normally disclose information related to existing flaws/vulnerabilities: providers will do this to ensure that their intrusion software remains effective for as long as possible (and by extension ensure their business success), and users of these surveillance tools want to keep their cyber-capabilities intact at the expense of the security and privacy of hundreds of thousands, if not millions of Internet users. Less reputable groups (organised crime, malicious

hackers etc.) may very well know and exploit the same flaws/vulnerabilities for their own gains.

Furthermore, intrusive surveillance tools do not discriminate between multiple users on one specific target: once a target is compromised, all data requested by the surveillance tools will be collected, regardless of the individual using the target.

Moreover, depending on how the attacks on targets are carried out, there may be unintended victims using altogether different IT systems along the way.

- Reusing the example presented in section 2.2, a user browsing the Internet may unknowingly stumble upon the Adobe Flash content incorporating exploits and find himself the victim of an unwarranted attack compromising his security and privacy.

- In order to successfully compromise a specific target, it might be necessary for the user of the intrusive surveillance tools to compromise another IT system which is known to be accessed by that target (*e.g.* in order to gain access to a user´s online banking account, an attacker might first target the video-on-demand website visited by the same user or the Facebook account of one of his friends). This would again mean compromising the security and privacy of individuals who have no connection to the investigation apart from being the unlucky users of an IT system interconnected with the target.

Depending on technical specifications and the specific context, intrusive surveillance tools can in some circumstances be instruments for a legitimate (and regulated) use by law enforcement bodies or intelligence agencies. They can be also used as "Trojan horses" to circumvent security measures in electronic communications (e.g. network encryption): once the attack on the target is successful, the surveillance tools will access the target's data even before the transmission of these data on the Internet, thus before network encryption would be applied to the data. That would of course leave useless any encryption used by the target.

3 The role of the EDPS and other Data Protection Authorities

Regulation 45/2001 grants the EDPS the duty to advise all EU institutions and bodies on all matters concerning the processing of personal data[16]. Pursuant to the same Regulation, the EDPS may also adopt Opinions, on its own initiative, in order to signal risks affecting the citizens' rights to privacy and data protection. In this Opinion the EDPS addresses the data protection and privacy issues raised by the dissemination of surveillance devices and software, since the use of these tools implies by default the processing of personal data and a possible interference with the right to privacy.

In parallel, Directive 95/46 also applies "*to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system*"[17].

The use of intrusive surveillance tools certainly involves the processing of personal data. Indeed, the notion of personal data encompasses, among others, any information, communication, metadata, activities, and movements relating to an identified, or identifiable, natural person. This is the type of information that is obviously processed by any surveillance

system. Moreover, the act of collecting, storing or intercepting data is considered as processing of such data. Therefore, as soon as the processing of these data are automatically performed by surveillance tools and remain within the scope of the Directive 95/46/EC, its rules and principles are applicable (as implemented by national laws and by Regulation 45/2001).

This means, in particular, that even if other regulatory or administrative provisions (for example, on the dissemination, export and use of the technology) are complied with, data protection law principles are still to be respected. In other terms, if a technology or device is cleared for sale to the public and use, this authorisation by no means affects the impact that such technology may have on individuals´ private sphere and the fact that any use has to be in compliance with privacy and data protection rules.

The EDPS and other data protection authorities at EU level, therefore, may intervene to signal specific risks that may arise for citizens´ right in connection with the use of intrusive surveillance technology, in addition to their advisory role in relation to any administrative or regulatory measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

In this respect, it must be pointed out that the interception of communications, the storage of personal information and the analysis of sets of data obviously have a serious impact on everyone's privacy and on protection of personal data.

4 Evaluation of the policies concerned

The following chapter will briefly present:

1. *the challenges, arising in connection with the use of surveillance and interception technologies, that should be addressed;*
2. *the existing policies that as concerns intrusive surveillance technologies;*
3. *possible outcomes and a forward-looking approach to further regulation.*

4.1 Challenges

Some technological systems can be used for human rights violations, such as censorship, surveillance, unauthorised access to devices, jamming, interception, or tracking of individuals. These violations can be performed by private organisations or public bodies (including law enforcement entities and governments). Cyberattacks, illegal interception, mass surveillance by governmental bodies, and attacks on computer systems are all examples of activities which can be perpetrated by using specific ICT devices, tools, or even information (e.g. knowledge of vulnerabilities in software).

On the other hand, ICT instruments can also be tools helping to disseminate ideas and information, organising social movements, especially in regions with authoritative regimes. The Internet is also a forum providing individuals with a multitude of possibilities to exchange data, information and knowledge. Therefore, ICT can have a very positive impact on the improvement of human rights. For example, encryption can be used by human rights advocates to avoid any intrusion, interception or surveillance by their governmental bodies.

Furthermore, some technologies can be used by journalists to circumvent the censorship in dictatorial regimes. Therefore, it must be recognised that the use of ICT can help protecting human rights and facilitate digital rights and freedom, including the protection of confidentiality, privacy and personal data.

The tension between the positive use of ICT tools and the negative impact that the misuse of technology can have on fundamental rights, and especially on the protection of personal data and privacy, has to be addressed by national and EU policies, and by all actors involved in the ICT sector (developers, service providers, sellers, brokers, distributors and users).

In a situation of enhanced security concerns, intelligence services and police may opt for the use of technology (including intrusive surveillance technology), in order to make their investigations better targeted and more effective. We cannot exclude, in this context, the use of big data as an investigative tool, as it is effective in connecting information and evidence from various sources. In this respect, we note that current data protection legislation, even in a newly reformed version, might not be sufficiently specific to address all the issues raised by the use of privacy-affecting technologies in the context of investigation and law enforcement.

With today's global interconnectedness, cybersecurity has an international dimension which goes beyond the EU borders. This international dimension makes effective cybersecurity a significant challenge, but it is a challenge that must be met as cybersecurity is a crucial element of data protection. The rights to privacy and data protection and cybersecurity share the same objective: ensuring a high level of cybersecurity will indeed help improve the security of all the information processed, including personal data.

However, cybersecurity must not become an excuse for disproportionate processing of personal data such as in the case of intrusive surveillance tools. Data protection principles such as necessity and proportionality help guide the lawful use of intrusion and surveillance technologies. In addition, privacy-by-design encourages the embedding of data protection safeguards in the technology in the design phase. Similarly, privacy-by-default ensures that the default settings of technology are compliant with data protection, in the absence of specific users´ choices.

Security of data, systems and networks is also crucial, in terms of trust, integrity of transactions and development of the Digital Single Market, Smart Grids and the Internet of Things. Weakened data security for the sake of allowing more pervasive surveillance would destroy trust and undermine the EU single market and the EU Digital Agenda. It is understandable that surveillance and law enforcement bodies require the appropriate means to fight crime, including on the Internet. But for any new measure, there is a need to assess beforehand the necessity and proportionality of the measure envisaged and to provide in advance substantiated evidence of the necessity of those measures.

Privacy and data protection are not in antithesis with economic growth and international trade, nor with cybersecurity or better services and products. Rather, they are part of a high-quality solution.

4.2 Assessment of policies concerned by the surveillance and interception technologies

The processing of personal data within the scope of EU law by the competent authorities for law enforcement purposes should also respect the standards and safeguards laid down in the EU Charter of Fundament Rights. Article 7 of the Charter enshrines the **right of privacy**, a

right for which the protection of personal data can be of fundamental importance. Thus the intrusion into the virtual domicile through spyware, exploits, or similar devices, should be considered a violation of one's privacy. In this context, the "virtual domicile" should be protected with the same respect as the physical domicile[18]. The **right to protection of personal data** is enshrined in Article 8 of the Charter, which entitles individuals to the protection of certain safeguards whenever their personal data are processed. Thus the use of surveillance tools should be addressed by specific legislation framing the acceptable limits of the dissemination and use of such technologies and laying down the necessary safeguards for such use.

Therefore, surveillance tools and software used in the EU will have an impact on these two fundamental rights of individuals. On the other hand, the EU should measure the impact of its policies on the fundamental rights of individuals in third countries. A consistent approach should be clearly encouraged to avoid any double standards when it comes to assessing the consequences of EU policies within and outside the EU.

Member States' legislation provides for the unlawfulness of the use of ICT tools under certain circumstances. Article 6 of the **Budapest Convention on cybercrime,** for example, already addresses the issue of the production, sale, procurement for use, import, distribution or otherwise making available of device, software or computer password, or access code, or similar data primarily for the purpose of committing an offence. However, the scope of this provision might not be adapted to address all surveillance and interception technologies. Moreover, this provision does not prohibit legitimate surveillance or interception acts (*e.g.* by law enforcement bodies authorised by law). It remains therefore uncertain, in some respects, whether the effective application of this provision can fully and properly address the issue of surveillance and interception tools capable of violating human rights in a way that can also affect individuals in the EU.

The **export of surveillance and interception technologies** may also be subject to the so called "dual-use" Regulation 428/2009[19]. Under this Regulation, the export of harmful technologies to third countries can be controlled. The EDPS welcomes the fact that, in December 2013, the states parties to the Wassenaar Arrangement agreed to implement export controls related to "Intrusion Software" and "IP Network Surveillance Systems".

However, the EU dual use regime fails to fully address the issue of export of all ICT technologies[20] to a country where all appropriate safeguards regarding the use of this technology are not provided. Therefore, the current revision of the "dual-use" regulation should be seen as an opportunity to limit the export of potentially harmful devices, services and information to third countries presenting a risk for human rights.

In the context of dual-use, standards should be developed in order to assess how the ICT or the information at stake might be used and the potential impact on fundamental rights in the EU[21]. An analysis of the situation in the third country regarding the actual protection of human rights or the respect of people's freedoms should be performed in order to evaluate whether an export authorisation should be delivered and under which conditions. In addition, an assessment of the context within which technologies are used is essential to evaluate their impact on human rights.

However, the EU's dual use Regulation cannot address all the questions concerning the dissemination and use of surveillance technologies. Another instrument that should set up a

frame for the actions of the law enforcement sector is the **future data protection Directive** applying to the law enforcement sector[22]. The use of ICT technologies by law enforcement bodies will have to respect the limits of the provisions of this Directive and its national implementation.

In consequence the effective protection of ICT systems from any attacks or illicit interception is essential to protect the fundamental rights to privacy and to data protection of individuals in the EU. The **EU digital agenda** already includes a set of measures aimed at improving cybersecurity, and should provide for a better resilience of ICT systems to any incidents that could breach the security of ICT systems.

In this context, the EU proposed a **cybersecurity strategy**[23], which should better involve ENISA (European Union Agency for Network and Information Security), setting up Computer Emergency Response Teams (CERTs) and propose new legislation[24] and actions[25] to counter security threats and incidents. The cybersecurity strategy of the EU should take into account the possible use of ICT technologies to harm fundamental rights both in the EU and in third countries. A consistent approach towards the dissemination of ICT surveillance and interception technologies should therefore be adopted within the context of the cybersecurity strategy.

Finally, the **data protection framework** is also a helpful instrument that might be used to address the security and violation of fundamental rights. Since the interception and surveillance of personal data will trigger, in response, the application of the data protection legal framework, the mere compliance of an ICT technology with export, security, commercial, or safety legislation will not exonerate the user from complying with the data protection principles as enacted in the national data protection legislation or in Regulation 45/2001.

The **obligation to secure the processing of personal data** is already enshrined in Directive 95/46/EC [26]. The future legal framework under the General Data Protection Regulation also provide for new principles which may serve to address the security and the protection of personal data. For example, the principles of *privacy by design* and *privacy by default* should encourage the companies to design the use of their ICT technologies in a way that allows to better serve the legitimate purposes of an organisation, by restricting the collection of data to what is necessary, or by targeting appropriately the persons and communications to be intercepted. The obligatory reporting of data breaches is another tool that might help identifying the weaknesses of an ICT system of the insufficient security that exists regarding a certain processing of personal data.

4.3 The Way Forward

With respect to the objectives stated above specific legislation should regulate as appropriate the application of data protection safeguards to investigative and enforcement activities that rely on technology. Although law making and technology development proceed at different speeds, such legislation should be as forward-looking as possible. In particular, it should be based on an assessment of, and take into account, technologies that, although not yet used in intelligence and police investigations, are already tested and available on the market. At the same time, legislation should remain technologically neutral and focus on the effect technology may have on data protection in order to mandate the application of certain

safeguards. Such policies should not inhibit legitimate research[27], nor unnecessarily limit access and communication of information.

The recourse to surveillance tools will affect the interests of multiple stakeholders: software designers and vendors, law enforcement bodies and the Internet community as a whole. It is crucial, therefore, that the debate on legislative measures to be adopted allows for a broad consultation of such stakeholders. In particular, principles such as *privacy by design* and *privacy by default* should be part of the discussion, as the former allows incorporating data protection safeguards in technology (thus attenuating its impact on the life of citizens) and the latter ensures that even individuals who are less concerned about their privacy receive an adequate level of protection. If we understand that companies need more legal certainty, they also have a moral responsability when engaging in this type of activities.

In the above respect, a crucial challenge consists of ensuring effective investigation tools based on technology while, at the same time, preserving the role of the Internet as a forum for free expression and democratic interaction between citizens. Citizens will increasingly demand to be protected by external threats (*e.g.* criminality and terrorism). At the same time, however, they will have a legitimate expectation that increased security does not take place at the expenses of their fundamental freedoms. The implementation of principles such as necessity and proportionality shall ensure that investigations and police activities are targeted and have a limited impact on citizens´ private sphere.

There is a need for all actors in the cybersecurity field (researchers, law enforcement bodies, CERTs (Computer Emergency Response Teams), private and public organisations etc.) to share information related to software flaws/vulnerabilities as well as information on security incident and breaches in order to ensure the most efficient, effective and widest adoption of proper software and security measures. In this interconnected world, the security of each entity is dependent on the security of the whole. It is by acting together in a coordinated manner that we are most effective in ensuring cybersecurity for all.

In addition, the revelations concerning the mass surveillance led to significant concerns regarding the respect of the protection of EU data subjects. National security cannot be a justification for untargeted, indiscriminate, and secret surveillance. Therefore, the EU should adopt a consistent global approach: since the surveillance practices revealed by Edward Snowden in the USA raise concern regarding their compatibility with the fundamental rights of the data subjects in European, the Member States should provide for the possibility of granting international protection to the whistle-blowers, including the right to seek asylum.

5 Conclusions

On the basis of the above, the EDPS is of the opinion that the threat raised by the use of intrusive surveillance technologies could be addressed through the following actions:

- An assessment of the existing EU standards for ICTs should be performed, with the purpose to increase the protection of human rights, especially in case of exportation of surveillance or interception technology and related services;
- The use and dissemination (including inside the EU) of surveillance and interception tools, and related services, should be subject to appropriate regulation, taking into account the potential risk for the violation of fundamental rights, in particular the rights of privacy and data protection;
- Consistent and more effective policies should be developed by the Council of the EU, the European Parliament, the European Commission and the EEAS regarding the export of intrusive surveillance tools in the context of dual-use technologies, at EU and international level;
- Up-to-date policies should regulate "0-day" exploits and vulnerabilities in order to avoid their use for fundamental rights violations;
- EU policies on cybersecurity should take into account the dissemination of interception and surveillance technologies and address specifically this issue within the appropriate legislation;
- Investments in security on the Internet and initiatives to embed privacy by design in new technological solutions should be fostered;
- A consistent approach should be put into place to grant international protection to whistle-blowers who contribute to revealing violations of human rights through the use of interception and surveillance technologies.

Done in Brussels, 15 December 2015

(**signed**)

Giovanni BUTTARELLI

European Data Protection Supervisor

Notes

[1] http://www.engadget.com/2015/07/09/how-spyware-peddler-hacking-team-was-publicly-dismantled/.

[2] http://www.engadget.com/2015/07/09/how-spyware-peddler-hacking-team-was-publicly-dismantled/.

[3] https://www.hackingteam.com/images/stories/galileo.pdf.

[4] https://www.hackingteam.com/index.php/customer-policy.

[5] http://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim.

[6] https://www.finfisher.com/FinFisher/company.html.
https://www.finfisher.com/FinFisher/products_and_services.html.
http://www.zdnet.com/article/top-govt-spyware-company-hacked-gammas-finfisher-leaked.

[7] https://www.zerodium.com/about.html.

[8] http://www.theverge.com/2015/11/10/9703526/tim-cook-encryption-uk-investigatory-powers-bill.

[9] https://en.wikipedia.org/wiki/Backdoor_%28computing%29.

[10] http://malware.wikia.com/wiki/Trojan.

[11] http://www.wired.com/2015/11/heres-a-spy-firms-price-list-for-secret-hacker-techniques/.

[12] http://arstechnica.com/security/2015/07/hacking-team-leak-releases-potent-flash-0day-into-the-wild/.

[13] http://arstechnica.com/security/2015/07/hacking-team-leak-releases-potent-flash-0day-into-the-wild/.

[14] http://www.engadget.com/2015/07/09/how-spyware-peddler-hacking-team-was-publicly-dismantled/, http://www.zdnet.com/article/top-govt-spyware-company-hacked-gammas-finfisher-leaked

[15] Hacking Team news releases of 08/06/2015, 14/06/2015 and 22/06/2015 (http://www.hackingteam.it/index.php/about-us).

[16] Article 43 of the Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 december2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data

[17] Article 3 (1) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[18] See for example decision of the German Constitutional Court of 29 February 2009, BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 267), http://www.bverfg.de/e/rs20080227_1bvr037007en.html.

[19] Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items

[20] Technologies, information, exploits, software and devices having a potential effect on human rights should all be subject to the dual-use regime, to avoid any shortcoming and loophole of this regime.

[21] For example, see Action 6 as proposed by M. SCHAAKE, Member of the European Parliament, suggesting applying EU 'know your customers' guidelines on exports: http://www.marietjeschaake.eu/2015/10/marietje-schaake-proposes-12-actions-to-remedy-human-rights-shortcomings-in-the-eus-dual-use-regulation/.

[22] Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.

[23] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667.

[24] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union - COM(2013) 48 final - 7/2/2013 - EN. The Commission, the Council and the Parliament reached an agreement on this text on the 8th of December: see http://europa.eu/rapid/press-release_IP-15-6270_en.htm.

[25] http://ec.europa.eu/digital-agenda/en/our-goals/pillar-iii-trust-security%23Our%20Actions

[26] Article 17.

[27] Including bug-bounty programs meant to incentivise invidividuals to provide information related to vulnerabilities to software companies.