Computer Standards & Interfaces 50 (2017) 76–82

Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

Mass surveillance and technological policy options: Improving security of private communications

Stefan Schuster[a,*], Melle van den Berg[b], Xabier Larrucea[a], Ton Slewe[b], Peter Ide-Kostic[c]

[a] Tecnalia, Derio, Spain
[b] Capgemini Consulting, Utrecht, Netherlands
[c] European Parliament, Brussels, Belgium

ARTICLE INFO

Keywords:
Surveillance
Policy
Encryption
Privacy

ABSTRACT

The 2013 Snowden revelations ignited a vehement debate on the legitimacy and breadth of intelligence operations that monitor the Internet and telecommunications worldwide. The ongoing invasion of the private sphere of individuals around the world by governments and companies is an issue that is handled inadequately using current technological and organizational measures.

This article[1] argues that in order to retain a vital and vibrant Internet, its basic infrastructure needs to be strengthened considerably. We propose a number of technical and political options, which would contribute to improving the security of the Internet. It focuses on the debates around end-to-end encryption and anonymization, as well as on policies addressing software and hardware vulnerabilities and weaknesses of the Internet architecture.

1. Introduction

The discussion about the legitimate balance between national security and information privacy, particularly concerning electronic – or digital – communication of all kinds, has been going on for several years. Intensified by the Snowden leaks, this discussion was also a topic of debate in various national parliaments and the European Parliament. This was the case, as the published information indicated that surveillance practices were used that infringe upon the basic civil liberties of (both US and non-US) citizens and the national sovereignty of states.

We argue that the debate on mass surveillance has highlighted the need to improve the security of the Internet, by paying attention to policies that help to i) stimulate the adoption of Privacy-Enhancing Technologies (PETs), ii) address software and hardware vulnerabilities and weaknesses of the Internet architecture/backbone and iii) devise industry incentives, in order to give consumers and organisations more choice about which products to adopt.

Recent developments and discussions, both in the US and the EU, indicate that governments are reluctant to adopt such policies, despite the recommendations of security experts and civil rights activists. This illustrates several scenarios and lists several promising technical means for providing more privacy and security to citizens.

2. The post-Snowden world has laid vulnerabilities bare

The Snowden files revealed the existence of a large-scale surveillance program carried out by the US National Security Agency (NSA) and its intelligence partners in the "Five Eyes" Network.[2] Massive amounts of data have been collected under this program, which was set up with the objective of protecting the national security of the involved countries. This data collection was achieved through the exploitation of vulnerable Internet protocols, software and hardware and the use of a plethora of highly sophisticated and cutting-edge software and hardware tools[3] available to the intelligence agencies, as well as through more traditional practices like coercion or physical wiretapping.

In a similar manner, businesses all over the world are gathering consumer-related electronic data and analysing it to find clues that help increase customer experience and profitability.

Most of the data gathered by these organisations is so-called

* Corresponding author.
E-mail addresses: Stefan.Schuster@tecnalia.com (S. Schuster), meberg@capgemini.com (M. van den Berg), Xabier.Larrucea@tecnalia.com (X. Larrucea), ton.slewe@capgemini.com (T. Slewe), peter.ide-kostic@europarl.europa.eu (P. Ide-Kostic).

[1] This article is based on research carried out at the request of the Science and Technology Option Assessment Panel (STOA) and the Committee for Civil Liberties, Justice and Home Affairs (LIBE) of the European Parliament [11,9]. Its scope is therefore primarily European, however its implications are assumed to be generally applicable.

[2] U.K., Canada, New Zealand, and Australia.

[3] Documented in the so-called ANT catalogue that has been published on WikiLeaks.

http://dx.doi.org/10.1016/j.csi.2016.09.011
Received 31 March 2016; Received in revised form 23 September 2016; Accepted 25 September 2016
Available online 28 September 2016

metadata. Metadata is “data about data” and describes the attributes of data *content* or *communication*. These attributes may, for instance, specify the author, the length or the type of data *content*. It may also specify the sender, receiver, time, date, duration and channel of data *communication*.

Despite the fact that metadata, by definition, does not contain the *content* of a message, its combination and analysis can reveal an extraordinary amount of information. The application of novel data fusion, analysis and processing techniques that work on large amounts of structured and unstructured data from different sources, commonly called Big Data Analytics, allows to identify patterns and relations, and to draw conclusions about very intimate details on people's habits and associations. Studies [1,2] show that sometimes only a few data points are needed to accurately identify individuals by applying this kind of analysis on anonymized or pseudonymized data. The larger and more diversified the underlying dataset is, the more precise big data analysis is becoming.

The ability of deriving personal details from all obtained communication metadata, not to mention snooping on the actual content of messages or private data, is raising severe concerns of privacy advocates, civil rights activists, politicians, technologists and citizens. It is considered to violate the fundamental right to privacy. Citizens lack control over what happens with their data and who has access to it and, more often than not, are not even aware that they are being observed. In light of the evolution of the Internet of Things (IoT) and the way our environment is becoming increasingly ‘smart’, privacy invasion has truly reached Orwellian dimensions. Smart home appliances, telecare, autonomous cars, and of course smartphones are already available today. These generate massive amounts of data that is related to the human beings operating or using these environments. Most of this information and associated metadata is not adequately secured against unauthorized access or modification.

Data protection laws exist in most western countries, but they are largely limited to regulating the treatment of “personal data”, which includes names, addresses, identification numbers, biometric information and any information that directly or uniquely identifies a person. The existing mechanisms for enforcing these regulations are, however, insufficient in the majority of cases [3,4]. This is because they are limited to ex-post sanctions, but do not provide means to prevent data privacy violations from the outset. For a number of online services, data privacy settings cannot be defined by end users, but are pre-set. In cases in which users can influence these settings, their default configuration is often based on an opt-out instead of an opt-in principle. Options for disallowing the transmission of personal data to third parties for commercial purposes are not available in most services that are based on business models that rely on user-data for generating revenue.

Three relevant stakeholder groups can be identified in the context of the discussion addressing online privacy and mass surveillance: i) state agencies and law enforcement authorities (LEA), ii) the businesses world (i.e. B2C), and iii) citizens. Each of these groups has different interest, can conflict with each other at times. Security agencies and LEA argue that privacy is secondary to national security. Businesses build on the prospects of developing services supported by IoT technologies and of customizing their offering to meet the individual needs of consumers in niche markets. Citizens want to enjoy the benefits of online and customized services, smart spaces, telecare, autonomous cars and other technology based advances. Some are willing to sacrifice part of their privacy, while others defend the preservation of their privacy vehemently. This is a generational phenomenon, with the digitally native generation apparently being more inclined to surrender some of their privacy than older generations [5]. Even when users are concerned about their privacy, they value it very low in monetary terms. Many users are willing to give away personal data for a small price and would pay even less for increased protection of their privacy. This underlines the need for regulations and policies that make the value of private data more explicit and transparent to the users. This way, users will be able to make better informed and qualified decisions with respect to ceding part of their privacy in online transactions [6–8].

From a societal perspective it is important to maintain an adequate balance between security interests and citizens' privacy and basic civil rights. The International Covenant on Civil and Political Rights (ICCPR) – as part of the Universal Declaration of Human Rights (UDHR) and ratified by all democratic states – establishes the right to democratic governance, the right to intellectual freedom, and the right to moral equality. These human rights, together with the principle of separation of executive, legislative and judiciary powers, form the basic pillars of democratic societies. The imbalance between security and privacy that has been created by the described mass surveillance practices and the intrusion of the privacy sphere by means of data analysis, clearly compromises the right to intellectual freedom and, as such, compromises one of the pillars of democratic societies.

For this reason adequate levels of privacy must be guaranteed both in real life, as well as in the digital world. The means to achieve this balance need to be established on both the political and on the technical level.

2.1. Research approach

In 2014, the Science and Technology Option Assessment Panel (STOA) and the Committee for Civil Liberties, Justice and Home Affairs (LIBE) of the European Parliament requested the elaboration of a two-part study [9] aiming to verify and confirm published evidence and information on the practice of mass surveillance by nation state agencies. Due to the delicate and sensitive nature of the general topic and the specific questions at hand, the methodology used was desktop research for comparing the coherence and consistence of the information from various sources. This information was then reflected on, adapted and in some cases extended through a number of interviews with and reviews by a panel of thirty-five internationally renowned subject matter experts. This article summarizes these findings in a concise way, focusing on elaborating the different policy options available, while elaborating on developments in law-enforcements in the past few years.

3. Possible scenarios to counter mass surveillance

Based on the findings of the study described in Section 2.1, this study recommends a number of short-to-mid-term technical and mid-to-long-term policy options for protecting the privacy and confidentiality of data and communications of (European) citizens. In structuring these options, two dimensions were deemed the most exclusive, in the sense that there was no direct, apparent correlation between the two: level of innovation and level of public intervention. The options in the level of innovation range from promoting the use of existing technologies (or making them more user-friendly) to constructing a complete new technological world and many things in between. In IT terms, the options are either to patch the current world in order to optimize what is already there or to deliver an entirely new update, substantially mitigating risks. With regards to the level of public intervention, the options range from promoting good practices and financing worthwhile initiative, to regulating industries and/or instituting new institutions. When these dimensions are plotted opposite one another, four scenarios emerge. The quadrants depicted in Fig. 1 cover these scenarios, which have been termed i) ‘Promote adoption’ ii) ‘Build confidence’ iii) ‘Disrupt’ and iv) ‘Innovate’.

The scenario calling for ‘*promote adoption*’ of readily available technologies, methods, concepts and models covers the most easily implementable measures for generating short-term impact. The wide scale adoption of the ‘security-by-design’ principle in software and hardware development and network administration is one of the

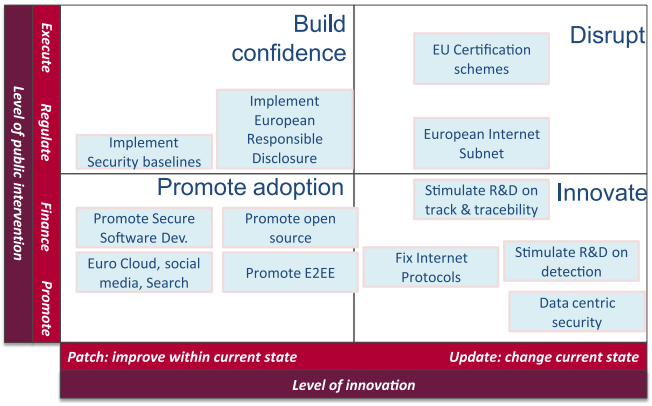

Fig. 1. Quadrant of policy option scenarios recommended in study on mass surveillance [9].

recommendations in this context. Together with the demand for a reinforced regionalised IT service industry, this is capable of competing with today's major ISPs and Cloud service providers, of which the headquarters are mostly based in the US.

The motivation behind the policy recommendation of "*promoting open protocols, open implementations [and] open systems*" is the idea of enabling public scrutiny that allows for validation and verification of software and service functionality by analysing their design and implementation. This recommendation does not imply Open Source Software (OSS) and systems to be less error prone or even more secure than proprietary software and systems, but is based on the public accessibility of its sources. The related recommendation to "*initiate a European 'OSS Bug Bounty Program' or finance existing programs*", is a measure that would directly contribute to and foster the idea of community-driven code inspections.

The foremost short-term *technical* option recommended for ensuring data security and privacy is encryption. A consistent and sufficiently strong encryption of both, the transmitted data (content) and the transmission channel guarantees a secure data exchange between two endpoints, also called end-to-end encryption (E2EE). Regulations that require applications to adopt E2EE and maximum privacy settings as default would help in stimulating a widespread adoption of cryptographic technologies. Although most service providers nowadays do encrypt messages during transfer, some encrypt them on their servers, through which they are owners of the encryption keys. This cannot be considered E2EE, since the very provider could act as a 'man in the middle' and decrypt data without the consent of its owner [10].

Secondly, the '*build confidence*' approach includes measures to improve trust between countries without the use of disruptive changes in technology. This mainly implies regulating existing technologies. Deploying security baseline regulations in order to ensure a minimum level of security measures for critical information infrastructure elements would facilitate the establishment of liability schemes and according sanctions for companies whose products or services do not comply with such baselines. Another way in which building confidence can be done is by implementing in a more widespread manner so-called coordinated vulnerability disclosure, i.e. the decriminalization and incorporation into corporate workflows of responsibly discovering and disclosing security flaws.

The '*disrupt*" scenario explores protectionist approaches, such as isolating a European Internet subnet or establishing territorially limited certification schemes. Both endanger and ignore the global character of the Internet. The scenario proposes a number of further-reaching measures, including certification schemes on an international level, and the option of instituting different subdomains – sometimes negatively referred to as the 'Balkanization' of the internet. However, this option in itself is questionable due to its limitative nature and the costs and expertise involved.

The options laid out in the '*innovate*' quadrant cover the advancement of vulnerability detection, tracking and tracing technologies, the improvement of protocols and so-called data-centric security concepts[4] through further development, fostered by an increased research and development funding. These possible developments are concerned with stimulating research and development into reduced traceability of data and devices and detection of surveillance. This would imply developing technology explicitly aimed at making large-scale tracking of users impossible. Another possible innovation is aimed at improving (current) insecure protocols and insecure architecture elements, or alternatively depreciating inherently insecure protocols. The final option is aimed at focusing on data-centric security, especially on implementation concepts and more specifically those for individual users.

The discussions in the past years have focused on three main areas for improving privacy and security for end-users. These are related to i) stimulating the widespread adoption of Privacy-Enhancing Technologies (PETs), ii) addressing hardware and software vulnerabilities and broken Internet protocols, and iii) strengthening the capacity of the IT security industry.

4. Policies stimulating adoption of PETs, including E2EE and anonymization tools (Tor, Funding of OS)

A field of research that has received a considerably increased amount of attention since the Snowden revelations is the field of the so-called Privacy-Enhancing Technologies (PETs). This grab-bag term refers to technologies that allow users to protect their data privacy while using (online) services or applications. One of the proposed short-term options considered is the widespread adoption of end-to-end encryption (E2EE).

E2EE is the technical option that has been identified in a number of studies and reports [11], as well as by experts on the subject, as the principal and most secure technical manner of protecting privacy and security of electronic information and communication. Obviously, this only refers to encryption that is implemented correctly: when there is no legal restriction regarding the power of the encryption used, endpoints are secured and communications are not subject to any 'man-in-the-middle' attacks. Legislation should forbid the use of generic backdoors for LEA purposes and the trading of zero-day exploits.

When E2EE messages are encrypted on the sender's device and decrypted on the recipient's device, telecom providers, ISPs and service providers such as Google, Facebook, Tencent or Microsoft only see encrypted information. Thus, these companies cannot disclose (readable) copies to government agencies, even with a court order. E2EE makes potential interceptions of communications detectable. In this way, E2EE offers an improved level of confidentiality of information and, thus, of privacy by protecting users from censorship, repression and unwarranted interceptions by law enforcement and intelligence agencies. However, as no guarantees on the safety of encryption exist, a clearer definition of what companies can promise under the guise of encryption and what can be expected of them is necessary. Some forms of regulation regarding this, such as official labelling agreements, can be expected in the coming years.

Encryption has taken centre stage in discussions on what law enforcement should be able to see. Information on financial transactions is clearly crucial in identifying financial streams, and therefore LEA would hardly be able to obtain any investigation data from vendors or service providers that apply E2EE. Another way in which encryption hinders legitimate concerns is the fact that companies have a right (within reasonable bounds) to monitor employees' behaviour. Overall however, opportunities for monitoring individuals and larger

[4] Data-centric security, sometimes also referred to as de-perimeterisation [31,32], enables location independent data security through a combination of context-based access control, encryption and the usage of secure protocols.

groups abound, so the fear of LEA 'going dark' and not being able to see what happens in the world seems to be slightly oversold to the public [12]. Strong cryptographic software is available to those who want to use it, as E2EE software has existed since the 1980s. Such software includes PGP (e-mail encryption software released in 1991), OTR ('Off the Record', for secure instant messaging), Internet telephony apps like SilentPhone, Signal, or DIME (aka Dark Mail) and specific plug-ins for Chrome, Firefox and other browsers. Newer E2EE tools do not only encrypt data, but also encrypt metadata (e.g. DIME and ProtonMail) [13,14].

The integration of encryption with existing functionalities, such as web browsing, creates new applications every day. The introduction of Let's Encrypt in 2015 [15], marks the first time that the certificates used in encryption protocols were available for free. The proclaimed aim of Let's Encrypt was to make encryption the default for all web connections.

For various reasons (technical, social, psychological, political), adoption of E2EE is not obvious for most users. The lack of user-friendliness is certainly not the only reason why users do not implement E2EE. Increasing the adoption of E2EE can follow two roads: stimulating individual users and stimulating collective solutions. Considering the many barriers that individuals face, it is advisable to raise awareness, improve knowledge, carry out testing and provide other help with finding the right tools.

On the other hand, collective options are much more promising in terms of reaching economies of scale. The public reaction to mass surveillance practices revealed by Snowden has already led to market dynamics that forced a number of service providers (such as Google, Apple, Amazon, Facebook, Twitter and LinkedIn) to deploy E2EE services. Such default settings could, however, impact the business models of these companies. In order to sustain and foster these market dynamics, regulation that mandates default security and privacy features and settings in hardware and software solutions should be considered. In order to guarantee users access and consent to information on which of their data is being used, some additional forms of regulation could also be developed.

Besides encryption, other promising manners of providing improved privacy are anonymizing services, like the Tor, i2p or GNUnet networks and secure services for logging in remotely, for example virtual private networks (VPN) and similar services. These are able to hide some of the most sensitive metadata elements such as time, duration, or endpoint addresses.

Anonymizing services act as a 'man in the middle'[5] while browsing the Web. They handle communications between the device and the website that is being visited anonymously. If everything is configured well and works correctly, the target website only sees information from the anonymizing service, so it cannot identify the user's IP address or other personal information [16]. This prevents third parties from identifying the endpoints of such communications and enables access to otherwise blocked or censored websites. Generally, anonymizing services make it possible for users to surf the Internet anonymously and without being observed. Without anonymization, the website that is visited, the Internet service provider (ISP), or any eavesdropper on the Internet connection can determine which websites the user of a specific device visits. Moreover, other personal data can also be accessed likewise [17].

Most anonymizing technologies still have considerable issues with usability, in the sense that they require effort on the users' part (separate installation and some amount of knowledge) and produce noticeable delay. In the case of Tor, this issue has been addressed by developing the Tor Browser to a certain extent.

Furthermore, a number of possible attack strategies against the Tor network have demonstrated the possibility of identifying the IP addresses of Tor users, as documented on the Tor project's blog [18]. Although such attacks are highly complex and require a fair amount of technical and financial capability not readily available to everyone, they demonstrate the impossibility of establishing absolute levels of anonymity. Some of the documents revealed by Snowden also confirm the technical ability of state agencies in compromising seemingly secure VPNs.

Encouraging the development of fast, high-quality TOR-like network(s) with many entry points and exit points on a national or regional level appears to be a desirable development. Some regulation could stimulate research and development, as well the commercialization of such services. For instance, Facebook in the US has already facilitated the integration of TOR as a way to access its services in a privacy-friendly way [19].

A lot of work on PETs remains to be done. The industry is in its infancy in relation to patenting and standardization. Moreover usability remains a challenge. Nevertheless, PETs are currently the most promising short-term approach for protecting privacy.

5. Policies addressing software and hardware vulnerabilities and the Internet architecture/backbone

Vulnerabilities in hardware and software have always been the Achilles' heel of information systems. Preventing these vulnerabilities would considerably contribute to an increased level of security. Despite efforts in the field of quality assurance, most hardware and software products and services still include many vulnerabilities that can be exploited. Mostly, security measures are added later, instead of including security in the design from the very start, as is promoted by the "security-by-design" paradigm [20]. Taking malicious practices into account during the design phase can not only prevent vulnerabilities, but can also reduce their impact. Supporting certification schemes, coordinated disclosure policies and funding of development and implementation of open source software are the leading ways forward in designing policies for addressing hardware and software vulnerabilities. These fall mainly within the '*Promote Adoption*' and '*Build Confidence*' scenarios mentioned earlier: these are relatively low-hanging fruit and are, in fact, already starting to be implemented within Europe.

Secure design relies on secure open standards and protocols. However, many protocols in use today should be considered insecure (e.g. DNS, BGP) [21,22] and are in dire need of repair. Implementing fixes will take a lot of time. In the meantime, consumers are left vulnerable to attacks by states and criminals. Additionally, insecure protocols remain in use while secure variants are available.

The verification and certification of the design and implementation of open standards, protocols and hardware and software solutions by globally trusted (independent) organizations is a prerequisite for addressing the problems mentioned above. Setting up regional certification bodies around the world could remedy the potential lack of trust in organizations that have acquired a bad reputation for conspiring with intelligence agencies to weaken PETs. The call for openness of systems is not to be confused with licensing schemes or intellectual property rights. It is based on the idea that open systems can be scrutinized by the community, whereas closed proprietary systems require the user to blindly trust in them without being able to validate and verify their trustworthiness. This does not imply that open source code is automatically better than proprietary code. Evidently, bad code is bad code. Initiatives to standardize the review and verification of coding are expected to take off in coming years and could receive more governmental funding. Using open source applications in publicly-funded institutions seems like an obvious way to expand their use and acceptability. Regulations that enable the coordinated disclosure[6] of

[5] This obviously implies a level of trust of the user in the company offering the service.

[6] Sometimes also called responsible disclosure.

vulnerabilities are considered another important instrument that would help reporting and fixing flaws in a timely and controlled manner. Actually, in many countries and organizations the disclosure of vulnerabilities is still regarded to be an offense, either against the national security or trade secrets. In such cases, the reporting party may be sued. This situation contributes to sustaining a black market for vulnerabilities and developing new attack vectors. A well-designed coordinated-disclosure policy stimulates those who report to disclose vulnerabilities. Rewarding and recognizing reporters for their work enables organizations to fix vulnerabilities and reduces the workload of law enforcement. The rewards for reporters have enabled the development of a new business model, connecting reporters and organizations.

Secure design and implementation is essential for open source software. Most users use open source software in daily life, but too little effort and funding is spent on the security of this software. More funds could be provided for this, as well as for independent evaluation. A good example of a provision of such funds is the 2015 initiative by the Dutch government to grant €500.000 to OpenSSL, an open-source encryption software library that is used around the world [23]. Since it is nearly impossible to guarantee the security of the whole supply chain, some academics have argued that a possible alternative could be to stimulate research to design resilient software architecture, offering secure products and services on top of potentially insecure hardware components.

6. Industry incentives to improve security

In the past few years, several countries began setting up separate Internet infrastructure services in order to provide a higher level of security. Russia has professed a desire to be able to 'draw up the bridge' and is providing localized services. There are several reasons for larger countries or regions (such as the EU) to pursue an amount of independence. First of all, increasing independence helps to improve adherence to a country/region's own security standards and, most importantly, legislation. Furthermore, regionalization makes sense, as it can promote the development of nationalized IT capabilities. In recent years, the idea of security as a business enabler has become fashionable, although its effects remain to be seen more clearly, especially on the consumer side.

Technologically, there are no great impediments to developing nationalized or regionalized services. In fact, in earlier decades, many examples of nationally-oriented social media, search engines, operating systems and other services abounded. Due to market concentration, a few giant (US) corporations – such as Google, Facebook and Apple – now control most of this landscape. Yet, these services were never developed with the security of their users in mind. They also do not have any specific legislation attached to protect users against spying. Such services mainly comply with US law, but hardly take local legislation into account. Therefore, the market for software is still mainly focused on the US and the market for hardware is centralized in Southeast Asia. As it is nearly impossible to guarantee the security of the whole supply chain, more hardware components could be designed and manufactured on a regional level, under a stricter legislation.

Taking the example of the European Union: despite the sustained growth of the IT sector worldwide, the overall IT market revenue of Europe in comparison with the rest of the world has been steadily declining since 2005. This situation is expected to continue as a recent IT market report of IDC/EITO3 [24] predicts a growth rate of 2,7% for the US ICT market in 2016, while it estimates the European IT market to grow only between 0,8% and 0,9% in the same period.

The idea of developing IT capabilities that are regionally oriented and focussed on enabling businesses received a boost after the 2015 European Court decision that invalidated the free exchange of data between the EU and the US.[7] It is becoming increasingly clear for businesses that in order to do business in regional markets, they need to adhere to the playing field there.

The effects of the knowledge of mass surveillance on consumer behaviour are also still unclear. Although a lot of industry initiatives have been developed, few 'safe' alternatives do exist. The 2014 launch of the Signal app, as an alternative to Facebook-owned Whatsapp, has seen significant use and is used as an encrypted SMS-like service.

In order to strengthen regionalized initiatives, investment by governments is necessary. Structural differentiators in this field are usually described in terms of the availability of qualified professionals and regulatory flexibility. Up to this point, a demand for secure products does not rank highly within industry development and customer demand.

7. Big brother strengthens the law: governments increase mass surveillance instead of making laws to strengthen security

As a consequence of the Snowden revelations, some expected governments to restore (part of) the privacy of individual users. However, the reverse seems to be the case. While parliaments in the EU and in the US have held hearings to learn more about the practices of intelligence agencies and have many options to improve privacy, little progress has been made in imposing privacy controls. Despite this, governments in a number of European countries have even strengthened laws to increase mass surveillance. This increase in surveillance entail a commensurate threat to the security, privacy and user's trust levels.

After the invalidation of the Data Retention Directive (2006/24/EC) by the European Court of Justice in 2014 and the European Commission's statement that it is "*neither opposing, nor advocating the introduction of national data retention laws*", many European countries have and practice data retention laws that establish retention periods ranging between 6 and 24 months for connection and metadata [25]. Some of the most criticised national regulations, which were brought to the table in the aftermath of the 2015 terrorist attacks in Paris and capitalized on the then reigning climate of scare and fear in the population, are those of the UK, France, the Netherlands and Germany. In the case of the UK, the draft communications bill known as "snoopers charter", required telecom and Internet service providers to keep records of customers' browsing activity, social media use, emails, voice calls, online gaming and text messages for 12 months. The French Council – in spite of warnings from the UN Committee for Human Rights about the excessively broad and very intrusive surveillance it would enable – approved a law that allows intelligence agencies to monitor phone calls and emails without prior judicial authorisation in July 2015. This law requires Internet service providers to filter all Internet traffic and enables metadata analysis for identifying suspicious behaviour.

Advocates of mass surveillance have often used the terrorist threat as an excuse for mass surveillance. Although mass surveillance has been in use for many years now, it has not been able to stop recent terrorist attacks in Tunisia, Egypt and Paris. The NSA has published figures on how many attacks have been thwarted [26] and US officials claim that "*the information gathered from these programs provided the U.S. government with critical leads to help prevent over 50 potential terrorist events in more than 20 countries around the world*."[8] However, it is not possible to verify the accuracy of these figures [27].

One of the ways to solve the problem of providing lawful interception capabilities evolves around the idea of public (controlled) agents

(*footnote continued*)

[7] Schrems vs. Data Protection officer, C-362/14.

[8] Gen. Keith B. Alexander, former Director of the NSA, in a hearing before the U.S. House of Representatives Permanent Select Committee on Intelligence.

that escrow master- or partial keys that would allow deciphering encrypted data. Key escrow and recovery agents are two conceptual implementations of this idea which have recently started being re-introduced in the discussion by different government and LEA representatives. While key escrow refers to the case in which a trustee holds a key for each user, a recovery agent will hold a master key that could decipher data of all users of a specific encryption algorithm.

The US government pushed for a key escrow system in the 1990s in order to allow LEA to have the ability to decrypt encrypted information, provided they had the necessary court order. However, the tech community and companies were not comfortable with the government having this ability, since they were not convinced of its trustworthiness for administering such universal pass-keys and because there were technical problems with the proposed mechanism at the time [28].

In the eyes of many security professionals, the use of key-recovery-based encryption infrastructures to meet law enforcement's stated specifications, undermines the security of encryption as a whole and increases costs to the end-user. Building a secure governance infrastructure for such an approach would be extremely complex. Even if it could be built, its risks and costs would eventually render it unacceptable. In addition, these infrastructures would generally require extraordinary levels of trust that cannot be easily transferred. Both backward and forward security could not be guaranteed by key escrow or key recovery mechanisms, since the possession of master keys, be they restricted to individuals or of generic purpose, enables the decryption of all past and future messages that have been encrypted with the corresponding public keys. Even if a current government would comply with the required trust-level, a subsequent government could shamelessly violate this trustworthiness.

For these reasons neither key escrow, nor key recovery agents can be considered valid and feasible solutions to the problem of guaranteeing LEA access to encrypted evidence.

Governments seem to hold on to the now ancient adage *get what you can lay your hands on*. The reasoning seems to follow classic tragedy-of-the-commons thinking: the incentive for monitoring, retaining metadata and indiscriminate mass surveillance is supposed to be a higher level of (national) security, but at the same time these practices are eroding the security (and privacy) of electronic communications. The attempts of some governments to introduce backdoors in encryption standards are the most prominent and obvious examples of this dilemma. Legislators and security agencies must understand that weakening the security of electronic communications will have a major negative impact on the digital economy, since all online transactions rely on adequate security (i.e. encryption) mechanisms.

8. Conclusions

This article has presented several ways to improve security in electronic communications. The years since 2013 have shown an increasing willingness on the part of companies to implement more secure encryption. However, governments seem reluctant to give up their acquired data sources to re-establish the state of law.

In a general sense, the Internet represents a classic 'tragedy of the commons'. Commons are goods that benefit all, regardless of how they are governed or created. They differ from public goods in the sense that they are a social system [29]. The idea of 'knowledge commons' has been increasingly in vogue. The concept of the tragedy of the commons is based on the idea that rationally acting individuals will deplete a common resource. This idea seems inspiring with regards to the Internet in its current form: the idea of securing the Internet by building back doors will inevitably lead to the demise of the Internet as a place for a secure and private exchange of ideas with peers.

Improving security on the Internet is done in the interplay between several parties: governments, industry and the public. *Governments* can take positions by implementing regulation on security. The implementation of baselines with regards to the security and privacy are still in their infancy. They can also stimulate better understanding by the general public by investing in education. Perhaps most importantly, they can nudge markets towards desired behaviour by defining a basic security level and using secure devices and applications themselves, as well as financing essential non-profit, open-source applications that benefit all users.

The *industry* has already been working on implementing more security, by increasing the use of encryption in commonly used applications. However, a lot can still be achieved by improving the user-friendliness of secure technology. The costs for integrating security-by -design principles can be steep at first, but they pay dividends when implementing. Patching afterwards can be minimized, as can the damage done to the image of the companies involved in potential breaches. The growth of privacy as a business enabler is beginning to take up speed.

The public has the obvious role of demanding security and privacy enhancing technology to be implemented. Secure e-mail, secure messaging and secure phone calls should be the current basic demand of consumers of electronic products. In the future this demand should extend to secure communications with IoT devices that will invade all aspects of human life.

Finally, the deployment of PETs and encryption more specifically should not prevent LEA from conducting targeted investigations pending the delivery of proper warrants by judicial authorities. LEA should have the skills and technical means for targeted interception of data at the end-point level before/after it is encrypted/decrypted (as opposed to indiscriminate bulk data collection for the purpose of signals intelligence), if necessary by conducting physical interventions on the devices of the data subject under investigation [30]. If major security vulnerabilities are identified and exploited by LEA during targeted investigations, LEA should report them to the vendors/service providers concerned as soon as a possible, without compromising the results of on-going investigations.

Acknowledgements

This work has been partially funded by the European Parliament, under the following contract number: 03210-02-00/5127/98400.

References

[1] Y.-A. de Montjoye, C.A. Hidalgo, M. Verleysen, V.D. Blondel, Unique in the crowd: the privacy bounds of human mobility, Nat. Sci. Rep. 3 (1376) (2013).
[2] M. Barbaro, T. Zeller, The New York Times. [Online], Available: ⟨http://www.nytimes.com/2006/08/09/technology/09aol.html⟩, 09.08.2006 (accessed 23.09.15).
[3] A. Arnbak, Securing Private Communications: Protecting Private Communications Security in EU Law: Fundamental Rights, Functional Value Chains and Market Incentives, Amsterdam, 2015.
[4] Organisation for Economic Co-operation and Development (OECD), Report on the Cross Border Enforcement of Privay Laws. [Online], Available: ⟨http://www.oecd.org/sti/ieconomy/37558845.pdf⟩, 2006 (accessed 27.01.16).
[5] University of Southern California, Is online privacy over? Findings from the USC Annenberg Center for the Digital Future show Millennials Embrace a New Online Reality. [Online], Available: ⟨http://annenberg.usc.edu/news/around-usc-annenberg/online-privacy-over-findings-usc-annenberg-center-digital-future-show⟩, (accessed 08.02.16).
[6] J. Tsai, S. Egelman, L. Cranor , A. Acquisti, The effect of online privacy information on purchasing behavior: an experimental study, in: Proceedings of the 6th Workshop on the Economics of Information Security, WEIS, Pittsburgh, PA, USA, 2007.
[7] E. Rose, Data users versus data subjects: are consumers willing to pay for property rights to personal information? in: Proceedings of the 38th Hawaii International Conference on System Sciences, 2005.
[8] A. Acquisti, L.K. John, G. Loewenstein, What is privacy worth?, J. Leg. Stud. 42 (2) (2013) 249–274.
[9] M. van den Berg, P. de Graaf (Eds.), P.O. Kwant, T. Slewe, Mass surveillance - Part 2: Technology Foresight, Options for Longer Term Security and Privacy Improvements, EPRS/European Parliamentary Research Service, Brussels, 2015.
[10] Electronic Frontier Foundation (EFF), EFF Secure Messaging Scorecard. [Online], Available: ⟨https://www.eff.org/secure-messaging-scorecard⟩, (accessed 27.01.16).
[11] A. Gamino Garcia, C. Cortes Velasco, E. Iturbe Zamaolla, E. Rios Velasco, I. Eguía Elejabarrieta, J. Herrera Lotero, J. Mansell, Linguistic review, in: J.J. Larrañeta

Ibañez, S. Schuster (Eds.), Mass Surveillance - Part 1: Risks and Opportunities Raised by the Current Generation of Network Services and Applications, EPRS/European Parliamentary Research Service, Brussels, 2015.
[12] B. S. a. J. Z. Matt Olsen, Don't Panic: Making Progress on the 'Going Dark' Debate. [Online], Available: ⟨https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf⟩, 2016 (accessed 08.02.16).
[13] R. Gallagher, Future Tense. [Online], Available: ⟨http://www.slate.com/blogs/future_tense/2013/10/30/dark_mail_alliance_lavabit_silent_circle_team_up_to_create_surveillance.html⟩, (accessed 17.12.15).
[14] L. Levison, Kickstarter. [Online], Available: ⟨https://www.kickstarter.com/projects/ladar/lavabits-dark-mail-initiative/posts⟩, (accessed 17.12.15).
[15] Internet Security Research Group (ISRG), Let's Encrypt. [Online], Available: ⟨https://letsencrypt.org/⟩, (accessed 17.12.15).
[16] PC World. [Online], Available: ⟨http://www.pcworld.com/article/2013534/how-and-why-to-surf-the-web-in-secret.html⟩, 2012 (accessed 17.12.15).
[17] JAP Anonymity & Privacy. [Online], Available: ⟨http://jap.inf.tu-dresden.de/index_en.html⟩, (accessed 17.12.15).
[18] TOR Project blog. [Online], Available: ⟨https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack/⟩, (accessed 17.12.15).
[19] Facebook, Making Connections to Facebook more Secure. [Online], Available: ⟨https://www.facebook.com/notes/protect-the-graph/making-connections-to-facebook-more-secure/1526085754298237⟩, 2014 (accessed 17.12.15).
[20] A. C. a. M. Chanliau, Privacy and Security by Design: A Convergence of Paradigms. [Online], Available: ⟨https://www.ipc.on.ca/site_documents/PbDBook-From-Rhetoric-to-Reality-ch8.pdf⟩, January 2013 (accessed 7.01.16).
[21] Dyn Research, The New Threat: Targeted Internet Traffic Misdirection. [Online], Available: ⟨http://research.dyn.com/2013/11/mitm-internet-hijacking/⟩, (accessed 08.02.16).
[22] Google, DNS Security Threats and mitigations. [Online], Available: ⟨https://developers.google.com/speed/public-dns/docs/security⟩, (accessed 08.02.16).
[23] K. McCarthy, Dutch Govt Says no to Backdoors, Slides $540k into OpenSSL Without Breaking Eye Contact. [Online], Available: ⟨http://www.theregister.co.uk/2016/01/04/dutch_government_says_no_to_backdoors/⟩, 4.01.2016 (accessed 20.01.16).
[24] E. I. Observatory, ICT Market Report 2015/16. [Online], Available: ⟨www.eito.com⟩.
[25] L. O'Donnell, Electronic Frontiers Australia. [Online], Available: ⟨https://www.efa.org.au/2015/07/29/european-data-retention-laws-update/⟩, (accessed 27.01.16).
[26] ProPublica. [Online], Available: ⟨http://www.propublica.org/documents/item/802269-untitled0001.html⟩, (accessed 17.12.15).
[27] T. Meyer ,J. Elliott, ProPublica. [Online], Available: ⟨http://www.propublica.org/article/claim-on-attacks-thwarted-by-nsa-spreads-despite-lack-of-evidence⟩, (accessed 17.12.15).
[28] J. Kilian, y F. T. Leighton, «Fair cryptosystems, revisited: a rigorous approach to key-escrow», in: de crypto '95 Proceedings of the 15th Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, California, 1995.
[29] S. B, D. Hammerstein, The EU and the Commons: A Commons Approach to European Knowledge Policy. [Online], Available: ⟨http://commonsnetwork.eu/wp-content/uploads/2015/06/A-Commons-Approach-to-European-Knowledge-Policy.pdf⟩, July 2015 (accessed 25.01.16).
[30] S. M. a. Bellovin, Going Bright: Wiretapping without Weakening Communications Infrastructure. [Online], Available: ⟨https://www.cs.columbia.edu/~smb/papers/GoingBright.pdf⟩, January/February 2013 (accessed 20.01.16).
[31] G. Palmer, De-Perimeterisation: Benefits and Limitations, Elsevier, Oxford, UK, 2005.
[32] Z. Hayat, J. Reeve, C. Boutle, Ubiquitous Security for Ubiquitous Computing, Elsevier, Oxford, UK, 2007.

Stefan Schuster received an M.Sc. degree in Software and Systems Engineering and a B.Sc. degree in Industrial Psychology from the Technical University of Berlin, Germany. He accumulates over 25 years of professional experience and broad knowledge in different ICT areas. During his work for European Software Institute and Tecnalia he occupied positions as Project-, Business Unit- and Strategy-Director. His areas of expertise cover Process Quality Management, Enterprise Interoperability, SOA, Cloud, Cybersecurity and online Privacy. He chaired three international conferences on Composition Based Software Systems (ICCBSS2008) and Process Quality (EuromedSPI-2011, SEPG-LA 2014) and is author and co-author of various scientific publications.

Melle van den Berg is a political scientist. He has been working at Capgemini Consulting in the fields of crisis management and cyber security. He has previously published on the topics of security and privacy and the security of the Internet of Things. He is a co-author of the study "Mass Surveillance - Part 2: Technology foresight, options for longer term security and privacy improvements".

Xabier Larrucea is a senior project leader and research scientist at Tecnalia and a part-time lecturer at the University of the Basque Country. He is IEEE Software constituency ambassador for Spain and Latin America. His research focuses on areas such as safety-critical software systems, software quality assurance, software process improvement, empirical software engineering, and metamodeling technology strategy. He contributed to the Scientific & Technological Strategic Plans in Colombia in 2013 and to several Object Management Group standardization initiatives, such as SPEM 2.0 and UPMS. Larrucea has received a Ph.D. in software engineering, an executive MBA, and Project Management Professional certification.

Ton Slewe is an experienced consultant in cybersecurity, with almost 30 years of knowledge of security and architecture. He has advised on and implemented new information system in large organizations. Mr Slewe has also been a leading author for multiple national Cyber Security Assessments, analyzing and writing on a broad range of (mostly technical) cybersecurity topics, including cryptology, Internet protocols, malware and exploits, cyber espionage and vulnerabilities. Mr Slewe is a Certified Information System Security Professional (CISSP), visiting lecturer at the Technical University of Twente and University of Amsterdam.

Peter Ide-Kostic is an administrator and policy analyst within the Secretariat of the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament. He is also the former administrator of the European Parliament's Science and Technology Options Assessment unit (STOA). He specializes in parliamentary research, security Management, Information Security, Technical security and IT security.