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