EUROPEAN PARLIAMENT

Science and Technology Options Assessment (STOA)

Mass Surveillance

Part 1 - Risks and opportunities raised by the current generation of network services and applications

STUDY

EPRS | European Parliamentary Research Service

Scientific Foresight (STOA) Unit

PE 527.409

EN

Mass Surveillance

What are the risks for the citizens and the opportunities for the European Information Society? What are the possible mitigation strategies?

Part 1 - Risks and opportunities raised by the current generation of network services and applications

Study

IP/G/STOA/FWC-2013-1/LOT 9/C5/SC1

December 2014

PE 527.409

The STOA project "Mass Surveillance – Risks, Opportunities and Mitigation Strategies Part 1" was carried out by TECNALIA Research and Investigation in Spain.

AUTHORS

Arkaitz Gamino Garcia
Concepción Cortes Velasco
Eider Iturbe Zamalloa
Erkuden Rios Velasco
Iñaki Eguía Elejabarrieta
Javier Herrera Lotero
Jason Mansell (Linguistic Review)
José Javier Larrañeta Ibañez
Stefan Schuster (Editor)

The authors acknowledge and would like to thank the following experts for their contributions to this report: *Prof. Nigel Smart, University of Bristol; Matteo E. Bonfanti PhD, Research Fellow in International Law and Security, Scuola Superiore Sant'Anna Pisa; Prof. Fred Piper, University of London; Caspar Bowden, independent privacy researcher; Maria Pilar Torres Bruna, Head of Cybersecurity, Everis Aerospace, Defense and Security; Prof. Kenny Paterson, University of London; Agustín Martin and Luis Hernández Encinas, Tenured Scientists, Department of Information Processing and Cryptography (Cryptology and Information Security Group), CSIC; Alessandro Zanasi, Zanasi & Partners; Fernando Acero, Expert on Open Source Software; Luigi Coppolino,Università degli Studi di Napoli; Marcello Antonucci, EZNESS srl; Rachel Oldroyd, Managing Editor of The Bureau of Investigative Journalism; Peter Kruse, Founder of CSIS Security Group A/S; Ryan Gallagher, investigative Reporter of The Intercept; Capitán Alberto Redondo, Guardia Civil; Prof. Bart Preneel, KU Leuven; Raoul Chiesa, Security Brokers SCpA, CyberDefcon Ltd.; Prof. Hugo Scolnik, Departamento de Computación, Universidad Buenos Aires*

STOA RESEARCH ADMINISTRATOR

Peter Ide-Kostic
Scientific Foresight (STOA) Unit
Directorate for Impact Assessment and European Added Value
Directorate-General for Parliamentary Research Services
European Parliament, Rue Wiertz 60, B-1047 Brussels
E-mail: peter.ide-kostic@europarl.europa.eu

LINGUISTIC VERSION

Original: EN

ABOUT THE PUBLISHER

To contact STOA or to subscribe to its newsletter please write to: STOA@ep.europa.eu
This document is available on the Internet at: http://www.ep.europa.eu/stoa/

Manuscript completed in December 2014

PE 527.409
ISBN: 978-92-823-5535-0
DOI: 10.2861/269619
CAT: QA-05-14-155-EN-N

Abstract

This document identifies the risks of data breaches for users of publicly available Internet services such as email, social networks and cloud computing, and the possible impacts for them and the European Information Society. It presents the latest technology advances allowing the analysis of user data and their meta-data on a mass scale for surveillance reasons. It identifies technological and organisational measures and the key stakeholders for reducing the risks identified. Finally the study proposes possible policy options, in support of the risk reduction measures identified by the study.

This study covers the analysis of the existing generation of network services and applications at the time of the study (2014) and the short to mid-term technical measures and policy options suitable for counteracting mass surveillance practices and guaranteeing privacy and security of electronic communication channels.

Future long-term technological and policy options addressing privacy and security in information and communication technologies are outlined in part two of this study, published by STOA.

This study is accompanied by an Annex, which provides detailed answers to the thirty five questions posed in the original tender for this study. The annex is published as a separate document.

Table of contents

EXECUTIVE SUMMARY

The disclosure of controversial mass surveillance programmes by intelligence and national security agencies has evoked an international debate on the right of citizens to be protected from illegitimate or warrantless collection and analysis of their data and meta-data. This report aims at identifying what are the risks of data breaches for users of publicly available Internet services such as web browsing, email, social networks, cloud computing, or voice communications, via personal computers or mobile devices, and what are the possible impacts for the citizens and the European Information Society.

In this context a clear distinction has to be made between data and meta-data. Also it must be differentiated between mass unwarranted and indiscriminate interception, and targeted lawful interception of Internet and telephony data for the purpose of law enforcement and crime investigation. While targeted lawful interception constitutes a necessary and legitimate instrument of intelligence and law enforcement agencies, mass surveillance is considered a threat to civil liberties such as the right to freedom of opinion and expression. These civil liberties are essential human rights in democratic societies and of particular importance for safeguarding independent journalism and political opposition.

Meta-data is data that is produced when electronic communication channels, like Internet or telephony are used and that provides information about the time, the origin the destination, the location, the duration and the frequency of communications carried out. Meta-data does, however, not contain the content of communications. Two types of meta-data exist, meta-data that provides data on the content (e.g. read/write/modify attributes of the file, author of the document, GPS location of a picture, etc.), and meta-data of the communication (e.g. sender, receiver, communication duration, communication starting date and time, communication channel, communication protocol used, etc.). In the context of this study, the cardinal interest lies on communication meta-data.

Communication meta-data is routinely gathered by telecom providers and Internet service providers as part of their business operations. Different laws and regulations exist in Europe and other countries that define the retention period of this data. The lawful interception of meta-data is *targeted* surveillance required by law enforcement authorities and is not considered as mass surveillance. The analysis of meta-data, despite the fact that it does not contain content, can reveal very detailed information about the person who has generated it.

Another potential source of information containing private data are Cookies. Cookies are text files that visited websites store on a user's local disk. Cookies allow for smarter and faster navigation, and are commonly used for personalizing website content, as well as ads and features by associated third parties. No evidence has been found that government agencies are leveraging the information that can be inferred from the data contained in Cookies through collaboration with commercial tracking companies.

The structured nature of meta-data is ideally suited for analysis using data mining techniques such as pattern recognition, machine learning, and information or data fusion. Meta-data analysis can reveal an extraordinary amount of information about people's habits and associations that when aggregated – data over time, or linked with other datasets - can expose even richer personal information and associational details. Unless special precautions are taken, few personal secrets of everyday life would withstand close analysis of meta-data.

Government agencies are intercepting meta-data either through their own technical capabilities, or accessing it through service providers on the basis of lawful requests, or under threat of fines. They also possess powerful capabilities to break system protections and to infiltrate systems and networks by applying advanced hard and software technology.

Commercial surveillance technology vendors are selling software applications and tools for surveillance purposes as advanced solutions for lawful communications data (including both meta-data and content) interception, collection, processing and/or analysis. Clients are governments, intelligence organizations, national security and law enforcement agencies which use these intelligence platforms and tools for collecting, processing and analysing both, mass and targeted communications data.

The legal context for commercial surveillance technology vendors is defined in different national and international laws, agreements and regulations. The Wassenaar Agreement, a comprehensive international treaty on export controls, including surveillance technology and undersigned by 42 states, has been extended in 2013 to law enforcement/intelligence gathering tools and IP network surveillance systems or equipment. Notwithstanding, the report of the UN OHCHR of June 2014 states that in most states, legal standards are either non-existent or inadequate to deal with the modern communications surveillance environment.

But also national security agencies themselves have developed a number of highly sophisticated hard and software interception tools that enable them to penetrate networking equipment, monitor mobile phones and computers and divert or even modify data without being noticed.

A special focus in the endeavour of mass surveillance is on breaking encryption that may prevent access to relevant data for intelligence and law enforcement agencies. Software flaws in the implementation of encryption algorithms can lead to vulnerabilities which may be easily exploitable, regardless of the complexity, the theoretical strength or quality of the applied encryption technique. Security agencies have managed to exploit such vulnerabilities, allegedly by introducing backdoors in encryption standards, but have had only limited success with traditional cryptanalytic attacks.

The new generation of encryption technology is proficient enough to avoid deterministic brute force attacks and provides the most reliable protection against unauthorized data access if its implementation and configuration parameters are well set up. Major attacks occur when implementations of current encryption technologies do not faithfully comply with their specifications, or when bugs and flaws – sometimes deliberately – are injected at code level. This is the reason for calling for a policy action that guarantees European citizens access to certified, resilient and open source implementations of different encryption specifications.

For an end user it is practically impossible to detect whether meta-data generated while navigating through the web, sending mails, or establishing other communications through Internet is being analysed or used by third parties and even less, if a system is subject to a complex attack orchestrated by powerful opponents like government agencies. Citizens can protect their privacy by applying safety conscious practices and using special software tools and services that help hiding their digital traces. Firewalls, anti-virus software, Virtual Private Networks, anonymizing proxies and networks and, most importantly, cryptography are technical means accessible to end users. But even though it is possible to hinder unauthorized access to private data or meta-data by applying a mix of different protection mechanisms, there is no means for guaranteeing total immunity against such attacks.

Policy options that are considered of help in reducing the risk of privacy intrusion by mass surveillance in a short to mid-term timeframe are: a) the promotion of open source operating systems and applications that allow for constant inspection and scrutiny by a large community of experts and verification and validation bodies and b) investing in and stimulating the integration of user friendly, utility-like software solutions.

The threat posed by mass surveillance practices can however not be solved on a technical terrain. Intelligence and security agencies will always have a competitive advantage in winning a race for technological supremacy in Internet security due to the resources at their command. The problem needs to be addressed on a political level. An adequate balance between civil liberties and legitimate

national security interests needs to be established, based on a public discussion that empowers citizens to decide upon their civil rights affected and the societal values at stake

1 INTRODUCTION

The disclosure of controversial mass surveillance programmes by intelligence and national security agencies has evoked an international debate on the right of citizens to be protected from illegitimate or warrantless collection and analysis of their data and meta-data. The focus of this discussion is on the rights and obligations of governments related to mass collection and processing of Internet and telecommunication data and meta-data and the technical capabilities of governmental institutions for doing so.

This report aims at identifying what are the risks of data breaches for users of publicly available Internet services such as web browsing, email, social networks, cloud computing, or voice communications, via personal computers or mobile devices, and what are the possible impacts for the citizens and the European Information Society.

It explains the nature and importance of meta-data in Internet and telephone communications, and presents the latest technology advances allowing the collection and analysis of user data and their meta-data on a massive scale for surveillance purposes. The report also analyses the current legal framework for the use and commercialisation of such technologies in the European Union and internationally and identifies technological and organisational measures to protect the data and meta-data and reduce the risks identified.

Finally, the study documents best practices and technical options available to citizens for mitigating the risk of surveillance. Possible technical short term policy options are proposed in support of the risk reduction measures identified by the study.

2 DOCUMENT STRUCTURE AND METHODOLOGICAL APPROACH

2.1 Format conventions

Specific formatting conventions are used throughout the document for highlighting and denoting different elements, depending on their character or significance:

- Text elements that are considered of major importance are highlighted in **Bold Font.**
- Proper names are enclosed by "quotation marks".
- Citations and quotations are marked in "*Italic Font, enclosed by quotation marks*"
- References to literature and other sources are given as Footnotes[1]. All URL references appearing in this report have been accessed in the period from September to November 2014.

- Summaries of the principal and most relevant information are framed in boxes

2.2 Document Structure

This report is structured according to the four research themes defined in the original tender of this study on Mass Surveillance. Chapter 1 contains an introduction to the problem space and documents the objectives of this study as defined in the original tender. Chapter 2 explains the formatting conventions and structure adopted, as well as the methodological approach applied for elaborating the report.

Chapters 3 to 6 cover the respective research themes and expose a synthesis of the research results and findings achieved on the respective theme. Detailed answers to each of the 35 questions related to the four research themes that were posed in the original tender are given in the ANNEX, which is published as a separate document.

Chapter 7 summarizes the proposed technical and short to mid-term policy options for counteracting current mass surveillance practices and reducing their risk for the individual citizen and the civil liberties of the society at large.

Chapter 8 recaps the conclusions of the study.

A list of abbreviations used can be found at the end of the document.

2.3 Methodological approach applied

Due to the delicate and sensitive nature of the general topic and the specific questions at hand, it turned out to be difficult, or in some cases quite simply impossible, to access detailed and verifiable first-hand information for researching certain issues. For the same reason, several experts have rejected requests to provide feedback and comments on the findings of this study.

This situation led the team of authors to abandon the initially envisaged gathering of experts' opinions based on an online questionnaire and adopt a methodological approach that initially focussed on the collection of information through desktop research. Large parts of the gathered information are based on classified information that was revealed by whistle-blowers or investigative journalists. Since it is difficult to scientifically validate and verify such leaked confidential information, the authors aimed to stick to renowned and serious publishers (i.e. newspapers) and tried to refrain as much as possible from using information published in Internet that cannot be verified (i.e. blogs, personal opinions). The information gathered has furthermore been verified by comparing coherence and consistence of

[1] Example of a footnote

the information from various sources. Scientific research publications were referenced where possible, although it must be said that only very few scientific papers on relevant topics for this study could be identified.

In a second phase, the information has been contrasted, adapted and in some cases extended through a number of unstructured interviews with and reviews by subject matter experts. The authors acknowledge and would like to thank the following experts for their contributions to this report: *Prof. Nigel Smart, University of Bristol; Matteo E. Bonfanti PhD, Research Fellow in International Law and Security, Scuola Superiore Sant'Anna Pisa; Prof. Fred Piper, University of London; Caspar Bowden, independent privacy researcher; Maria Pilar Torres Bruna, Head of Cybersecurity, Everis Aerospace, Defense and Security; Prof. Kenny Paterson, University of London; Agustín Martin and Luis Hernández Encinas, Tenured Scientists, Department of Information Processing and Cryptography (Cryptology and Information Security Group), CSIC; Alessandro Zanasi, Zanasi & Partners; Fernando Acero, Expert on Open Source Software; Luigi Coppolino,Università degli Studi di Napoli; Marcello Antonucci, EZNESS srl; Rachel Oldroyd, Managing Editor of The Bureau of Investigative Journalism; Peter Kruse, Founder of CSIS Security Group A/S; Ryan Gallagher, investigative Reporter of The Intercept; Capitán Alberto Redondo, Guardia Civil; Prof. Bart Preneel, KU Leuven; Raoul Chiesa, Security Brokers SCpA, CyberDefcon Ltd.; Prof. Hugo Scolnik, Departamento de Computación, Universidad Buenos Aires*

3 CURRENT PRACTICES OF INTERCEPTION AND ANALYSIS OF END-USER META-DATA

Meta-data is data that is produced when electronic communication channels, like Internet or telephony are used and that provides information about the time, the origin (i.e. the originating IP address or IMSI), the destination, the location, the duration and the frequency of communications carried out. Meta-data does, however, not contain the content of communications.

Meta-data is considered personal data under EU legislation, but not so in all foreign legislation (e.g. USA). Meta-data data is routinely gathered by the respective telecom providers and ISPs as part of their business operations. **The analysis of meta-data, despite the fact that it does not contain content, can reveal very detailed information about the person who has generated it**. Examples show that meta-data available to telecom providers, combined with other publicly accessible information on the web, can be used to generate a detailed trace of activities and movements of targeted individuals[2]. In the context of intelligence services, meta-data is data that "*describes content, events, or networks associated with SIGINT targets*" as defined in a 2009 draft report prepared by the NSA's inspector general[3].

3.1 Types of Meta-Data and their retention

Meta-data is generally considered "data about data". In the context of communications, meta-data can refer to either the content (communicated message) or the communication itself. Therefore, **there are two types of meta-data that must not be mixed up**: **meta-data** that provides data **on the content** (e.g. read/write/modify attributes of the file, author of the document, GPS location of the photo scene, etc.), **and meta-data of the communication** (e.g. sender, receiver, communication duration, communication starting date and time, communication channel, communication protocol used, etc.). In the context of this study, the cardinal interest lies on communication meta-data.

From a legal perspective, the communication meta-data is the only existing meta-data, as content meta-data is considered to be part of the content and travels end-to-end embedded in the content.

Communication meta-data can furthermore **be subdivided into two different types: Telephony meta-data and Internet meta-data** (also called Internet Protocol (IP) meta-data). For an email message, for instance, the meta-data would include the sender and recipient email addresses. It does not contain the subject line or the text of the email, since these are part of the email content. Likewise, telephone communication meta-data would at least include the called and the calling number, as well as the duration of the call, but in practice covers much more information[4].

As described in a declassified order ruled by the FISA Court which required collecting **telephony meta-data** of a company, this meta-data **includes** "*comprehensive communications routing information (e.g.* ***originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number****, etc.),* ***trunk identifier, telephone calling card numbers, and time and duration of the call****. Telephony meta-data does not include*

[2] http://www.zeit.de/datenschutz/malte-spitz-data-retention/ and https://www.bof.nl/2014/07/30/how-your-innocent-smartphone-passes-on-almost-your-entire-life-to-the-secret-service/

[3] https://www.aclu.org/files/natsec/nsa/20130816/NSA%20IG%20Report.pdf

[4] cf. ANNEX Question 1

the content of the communication, or the name, address or financial information of a subscriber or customer"[5]. The meta-data information, also classed as transactional information, **can also include the cell site location data**, i.e. the nearest cell tower a phone was connected to[6].

IP meta-data can be collected for services that run over IP protocol (e.g. VoIP, email, HTTP-based services such as "Facebook", "Twitter", Internet searches, etc.) or that IP runs on top of (e.g. GPRS, Ethernet, etc.)[7].

In contrast to telephony meta-data, **multiple parties are involved in IP meta-data interception** since the transportation of IP-based services over the Internet involves "*access providers on each end of the communications, transport operators, core network operators, and providers of services"*[8]. Moreover, the separation of the IP communication in several communication layers (Open Systems Interconnection (OSI) layers[9]) makes it difficult to establish and identify which IP meta-data can be gathered. ETSI published a set of specifications in order to support IP lawful interception for telecommunication service providers and network providers[10].

> The lawful interception of meta-data is a targeted surveillance required by Law Enforcement Authorities and is not considered as mass surveillance.

Communication meta-data is routinely gathered by telecom providers and ISPs as part of their business operations and different laws and regulations exist in Europe and other countries that define the retention period of this data.

In Europe no mandatory retention period for communication meta-data exists, since the Court of Justice of the European Union declared invalid the Directive 2006/24/EC[11] of the European Parliament on 8 April 2014[12]. This invalidated Directive had previously established a mandatory retention period for meta-data for a minimum of 6 months and a maximum of 2 years.

The UK has approved the Data Retention and Investigatory Powers Act 2014 (DRIP Act), which establishes that providers can be required **to retain meta-data for up to 12 months** and that this data may be used as evidence by law enforcement.

Australia is currently discussing data retention legislation that would require providers to store meta-data for up to 2 years.

There is no legal obligation for data retention by communication providers in the USA. However, **US law enforcement can obtain access to meta-data stored by providers under the Stored Communications Act[13] (SCA)**, which also establishes mandatory data storage for up to 180 days upon government request.

[5] http://www.dni.gov/files/documents/0708/BR%2009-09%20Primary%20Order.pdf
[6] http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order
[7] https://tools.ietf.org/html/rfc3924
[8] AQSACOM, Lawful interception for IP networks, White Paper. March 2010.
[9] Recommendation, I. T. U. T. X. 200 (1994)| ISO/IEC 7498-1: 1994. Information technology–Open Systems Interconnection–Basic Reference Model: The basic model
[10] http://www.etsi.org/technologies-clusters/technologies/security/lawful-interception
[11] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF
[12] http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf
[13] http://www.gpo.gov/fdsys/pkg/STATUTE-100/pdf/STATUTE-100-Pg1848.pdf

3.2 The role of commercial Cookies and trackers

ENISA's work on Cookies[14] provides a comprehensive explanation on what Cookies are, how they work and the privacy and security concerns they raise. In summary,

> Cookies are text files that visited websites store on a user's local disk. The Cookies allow for smarter and faster navigation, and are commonly used for personalizing website content, as well as ads and features by associated third parties.

Cookies allow for state management over the HTTP (Hypertext Transfer Protocol) protocol which is stateless by nature. In order to overcome this situation, the Cookies were created as part of Internet standards to keep state information. Cookies are generated and modified by website servers, stored on client's local disks and transmitted in every interaction between the server and the browser.

In terms of life-span, **there are two main types of Cookies**: 1)**session Cookies that are temporarily stored in memory** and deleted once the connection session times out or when the browser is closed; and 2)**persistent Cookies that** span over sessions and **remain stored on the user's local disk**, even when the browser is closed, until their expiration date. While session Cookies' purpose is to keep state information within sessions, **persistent Cookies are used for relating subsequent sessions or visits to a website**.

> The information that can be stored in and extracted from Cookies is diverse and ranges from user registration and log-in information (e.g. credentials and other identifiers), user preferences and settings, session data, data cached by the site, records of user browsing activity, and other information that can be retrieved in future sessions, including personally identifiable information provided to the website by the user.

With such a wide variety of possibilities, it is not surprising that **advertisement and surveillance organisations are exploiting Cookies, which can be easily accessed without the need for authentication,** to collect and compile tracking information on the browsing history and online behaviour of users.

The lack of transparency and control over their data are the main reason why users have started to block or delete Cookies and to adopt best practices for increased privacy, such as the FTCs recommendation for a "Do Not Track" mechanism[15]. Following this trend of respecting consumers concerns, Cookies are not always accepted and various browsers avoid their use in the default settings or block all third party Cookies.

Cookies have limited utility for collecting data across applications or devices as they are specific to a unique login session, a unique device and a unique browser, or application. This limits the capability of Cookies to master user location data and keep track of the user identity across platforms. For these reasons,

> The use of traditional Cookies is now being superseded by other state management solutions that overcome Cookies limitations.

[14] http://www.enisa.europa.eu/activities/identity-and-trust/privacy-and-trust/library/pp/cookies

[15] Federal Trade Commission. (2010, December 01). FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers. Retrieved from ftc.gov: http://www.ftc.gov/opa/2010/12/privacyreport.shtm

The Future of the Cookie Working Group[16] of Interactive Advertising Bureau (IAB) is working in pushing cookie-free solutions that can address simultaneously all requirements of the three involved players: consumers, publishers (creators, facilitators and/or owners of website contents) and third parties. In their whitepaper "Privacy and Tracking in a Post-Cookie World"[17], IAB explores a set of four different technologies that could replace the Cookies, and which address the three stakeholder types' needs with different degrees of success.[18]

> Whatever the future alternative to Cookies, in order to be consistent with existing regulatory and self-regulatory standards, they need to ensure transparency to Internet users on which data is stored or transmitted to the website, as well as which types of statistical analysis is performed with such data, for what purposes and with whom it is shared.

In addition, new solutions need to let users choose to opt-out for websites not tracking their data, similar to opt-out mechanisms that current Cookies technologies provide. In most cases, current solutions still lack browser plugins or other mechanisms for such transparency or control.

As highlighted by IAB, one of the most important factors for the cookie alternatives to be widely adopted by the Internet industry and its trustworthiness ensured, is the need of being conceived and deployed as open solutions. **The technologies shall neither be proprietary nor licensed by** one or a few **commercial organisations**. **They should be as openly accessible as possible, if not directly embedded in Internet standards** that are widely supported by public authorities all over the globe.

These demands also stem from the observation of questionable practices of on-line advertisement agencies. The ever evolving powerful techniques they use **have given these companies the ability to tailor the publicity to individuals at the cost of disclosing their privacy.** Personal information like age, gender, purchase intent, interests, parents, but also health related and financial information are covered by advertisers' inference techniques. These techniques are becoming increasingly sophisticated, and **user tracking is evolving to cross-platform tracking**, so companies can retarget users who switch from desktop to mobile devices.

A number of privacy groups, the Center for Digital Democracy, U.S. PIRG, and the World Privacy Forum have filed a formal complaint[19] with the U.S. Federal Trade Commission (FTC), urging them to investigate data collection "Wild West" involving real-time advertising auctions and data exchanges.

However, neither in a statement of US President Barack Obama in which he announces *new restrictions* […] *to better protect the privacy of ordinary Americans and foreigners from government surveillance"* and in which *"he offered no hint that American spies have routinely seized that* [tracking] *data"*[20], nor in the documents leaked by Edward Snowden, any evidence can be found for a cooperation of intelligence agencies with advertisement companies:

> "*Nothing in the Snowden revealed secret reports indicates that the* [online advertising] *companies cooperated with the spy agencies to share the information; the topic is not addressed*."

[16] http://www.iab.net/member_center/committees/working_groups/Future_of_the_Cookie_Working_Group
[17] http://www.iab.net/media/file/IABPostCookieWhitepaper.pdf
[18] cf. ANNEX Question 3 for more detailed information
[19] http://www.centerfordigitaldemocracy.org/protect-consumer-privacy
[20] http://www.nytimes.com/2014/01/28/world/spy-agencies-scour-phone-apps-for-personal-data.html?_r=0

3.3 Meta-data analysis for mass surveillance purposes

The **analysis of (communication) meta-data** is subject of discussion, because it **may reveal more private information than the content itself**. Todays increased data collection and novel approaches for data representations and mathematical modelling coincide with the development of powerful database technologies that provide an easy access to the massive amounts of collected data[21]. These include technologies to deal with non-structured data as well as structured data.

"Big Data" is a term encompassing **the use of techniques to capture, process, analyse and visualize potentially large datasets** in a reasonable timeframe, not accessible to standard IT technologies. By extension, the platforms, tools and software used for this purpose are collectively called "Big Data technologies"[22]. This type of technologies deals with huge amounts of distributed and heterogeneous data such as structured data (e.g. meta-data) and non-structured data (e.g. voice or video). Furthermore, data collection and analysis is being conducted at a velocity that is increasingly approaching real time[23].

> The structured nature of the meta-data is ideally suited for analysis using data mining techniques such as pattern recognition, machine learning, and information or data fusion.

These knowledge-discovery-in-databases (KDD) techniques are rapidly evolving and providing new innovative tools such as support for vector machines, genetic algorithms, classification and regression trees, Bayesian networks, and hidden Markov models, to make better use of this explosion of information[21].

As pointed out by Professor Edward Felten[24] it is difficult to summarize all the sensitive information that can be revealed by processing only meta-data (not content). But suffice it to say that

> Meta-data analysis can reveal an extraordinary amount of information about people's habits and associations.

As Felten explains: "*Calling patterns* [deduced from meta-data] *can reveal when we are awake and asleep; our religion, if a person regularly makes no calls on the Sabbath, or makes a large number of calls on Christmas Day; our work habits and our social aptitude; the number of friends we have; and even our civil and political affiliations*."

When meta-data is aggregated – data over time, or linked with other datasets - it can expose even richer personal information and associational details. Analysis of this kind of meta-data can reveal the network of individuals with whom they communicate, commonly called a "social graph". "*Data-mining systems for national security use are designed to link any common identifying numbers of any kind and look for correlations, geographical intersections of location data, and patterns in online social relationships.*

> *Unless special precautions are taken, few personal secrets of everyday life would withstand close analysis of meta-data*".[25]

Big data technologies are critical for mass surveillance purposes since they provide the necessary tools for processing and analysing vast amount of heterogeneous data in a reasonable timeframe.

[21] http://epic.org/misc/nrc_rept_100708.pdf
[22] Big Data – A new world of opportunities, NESSI White Paper, December 2012
[23] Big Data: Seizing opportunities, preserving values. US Government report. May 2014.
[24] Professor of Computer Science and Public Affairs , as well as Director of the Center for Information Technology Policy , at Princeton University
[25] http://blog.privacystrategy.eu/public/published/Submission_ISC_7.2.2014_-_Caspar_Bowden.pdf

Snowden's revelations have also shown the use of Big Data technologies. "Boundless Informant" is a Big Data analysis and data visualization tool developed and used by the NSA. The objective of this tool is to count and categorize the meta-data of both, Internet and telephony communications[26].

3.4 Complicity between mass surveillance organizations and other parties

> Internet monitoring is the act of intercepting data packets over Internet Protocol. The infrastructure that supports the Internet includes physical infrastructure and electronic systems (such as communication switches, routers, servers, etc.) to connect the world. Internet monitoring can take place across any point of this infrastructure, depending on what information shall be collected[27].

Secret US Government documents leaked by Edward Snowden reveal that the US **intelligence services have obtained copies of the Internet traffic** transmitted through the US major domestic fibre-optic cable networks.[28] This so called "Upstream collection" [29] is carried out on four nodes in which Internet wires are tapped. In the case of the US, the data collection is conducted under different Law Authorities: Transit Authorities, Foreign Intelligence Surveillance Act (FISA) and FISA Amendment Act of 2008 (FAA)[30].

The American Civil Liberties Union (ACLU) published a schematic diagram representation of the NSA surveillance over the major communication switches, routing stations, and access points of telecommunication systems. According to ACLU, **this type of data collection includes both access to gateways through which phone calls are routed as well as access to other telecommunication equipment** (such as routers, switches, etc.) **through which Internet traffic data flows**[31].

In June 2013, the media also reported that **the British intelligence agency GCHQ intercepts, collects and stores data from the fibre-optic cable network** which carries international phone and Internet traffic data[32].

The US is connected to 63 countries by fibre-optic cables; France to 60; Portugal to 59; UK, to 57; Italy to 47; Spain to 41; Germany to 40; Greece to 37 .

> Telecom operators, Internet organizations and government agencies have bought, installed and maintained software and equipment for phone and Internet traffic interception[33].

In case of Tunisia, the German company Trovicor GmbH provided voice and data interception on cell phones[34].

Different **media reports suggest that cooperation takes place between national security agencies** on one hand and ISPs, telecom **and** cloud **providers** on the other hand, **for intercepting and accessing**

---

[26] http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining
[27] https://www.privacyinternational.org/sii/technologies/internet-monitoring
[28] https://www.eff.org/nsa-spying
[29] http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/3
[30] http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#doc/2
[31] https://www.aclu.org/files/pdfs/eavesdropping101.pdf
[32] http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa
[33] http://www.wired.com/2011/01/as-egypt-tightens-its-internet-grip-tunisia-seeks-to-open-up/
[34] http://www.bloomberg.com/news/2011-12-12/tunisia-after-revolt-can-alter-e-mails-with-big-brother-software.html

Internet and telephony meta-data and content. These accusations have been confirmed in some cases and resolutely repudiated in others.

The telecom operator **Vodafone revealed the existence of secret wires** that allow government agencies to intercept all conversations on its networks under the law in place. This practice is widely used in some of the 29 countries in which Vodafone operates in Europe and beyond[35]. Google has not only rebutted accusations of having (voluntarily) collaborated with NSA, but also (together with 7 other Internet companies) issued a letter to the US Senate[36] in which they demand a Global Government Surveillance Reform.

But data collection is also carried out by requesting telecommunication operators or Internet agencies to hand over phone and Internet related data to intelligence agencies under **law orders and the threat of fines**, as happened in the Verizon case[37,38]. As indicated in the white paper released by the US Government, "*under the telephony meta-data collection program, **telecommunications service providers, as required by court orders issued by the FISC, produce to the Government certain information about telephone calls**, principally those made within the United States and between the United States and foreign countries*"[39,40].

However, given the tools listed in NSA's ANT catalogue[41], it becomes clear that

> National security agencies have the means for penetrating networking equipment, monitoring mobile phones and computers and diverting or even modifying data without being noticed[42].

Data **interception using such covert techniques implies that the organization which has been attacked is not aware of it** and therefore no collaboration from their side is needed for collecting this data.

There are a number of confirmed cases which exemplify the use of techniques for penetrating third party systems with the objective of retrieving data:

The so-called "stingray" is a device that can be used to **track a suspect's location** and engage in other types of surveillance[43]. The more generic term for the device is "IMSI catcher"[44]. IMSI catchers imitate a wireless carrier's network equipment and in doing so, they send and receive signals to and from all mobile devices in the local area on the same network[40]. This surveillance tool can collect information about targeted devices as well as their geographical locations.

In august 2014, the web portal "Heise.de", based on information of leaked classified documents, revealed the existence of a mass surveillance technology, developed by GCHQ and codenamed

[35] http://www.theguardian.com/business/2014/jun/06/vodafone-reveals-secret-wires-allowing-state-surveillance

[36] https://www.reformgovernmentsurveillance.com/

[37] http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

[38] http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#doc/1

[39] http://www.theguardian.com/world/2013/aug/09/obama-legal-background-surveillance-nsa

[40]https://www.documentcloud.org/documents/750211-administration-white-paper-section-215.html

[41] https://www.eff.org/files/2014/01/06/20131230-appelbaum-nsa_ant_catalog.pdf

[42] http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html

[43] https://www.aclu.org/blog/national-security-technology-and-liberty/court-uncovering-stingrays-troubling-new-location

[44] http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf

HACIENDA, which **scans open ports on all servers** connected to the Internet **searching for vulnerabilities to be exploited**[45].

The FinSpy[46] **malware**, part of the commercial intrusion kit FinFisher, collects and encrypts a wide range of data from the infected device. The FinSpy Mobile component provides recording of common communications such as voice calls, emails and SMS/MMS, file download from the infected device, as well as location tracking[47]. Furthermore, this malware employs a myriad of techniques **designed to evade detection and resist any kind of analysis**[48].

Other examples are the **production and publishing of fake copies of the most popular websites** on the Internet by surveillance organisations **with the objective of using them for "drive-by" infections**. Once the user has opened the website a malware is installed on the computer and the mass surveillance organization can gain access to the user's networks. According to "Der Spiegel",

> GCHQ created a fake LinkedIn website in order to collect information related to mobile communication companies and billing companies by targeting their employees[49]

In some cases the NSA has masqueraded as a fake Facebook server, using the social media site as a launching pad to infect a target's computer and files from a hard drive. In others, it has sent out spam emails laced with the malware, which can be tailored to covertly record audio from a computer's microphone and take snapshots with its webcam. The hacking systems have also enabled the NSA to launch cyberattacks by corrupting and disrupting file downloads or denying access to websites"[50].

> For an end user it is practically impossible to detect whether meta-data generated while navigating through the web, sending mails, or establishing other communications through Internet is being analysed or used by third parties,

with the exception of the use of Cookies by third party advertisers that can be observed through the placement of "customised" ads on web pages. Both, **malware technology and IP monitoring technology vendors claim their tools are invisible to the target**: "*Remote Control System" is totally invisible to the target. It bypasses protection systems such as antivirus, antispyware and personal firewalls*[51]"; "*… POSEIDON is totally invisible in a communication network and cannot be identified*[52]. Or as Bruce Schneier, a renowned security and cryptography expert puts it in an article published by the "Guardian": "[NSA's TAO has a] *variety of tricks to get* [exploits] *on to your computer. Your anti-virus software won't detect them, and you'd have trouble finding them even if you knew where to look*"[53]

The perfect means for a citizen to prevent analysis of personal meta-data is simply not producing it, which essentially means not using electronic communication mechanisms. This is of course not a feasible alternative and **the situation can therefore only be addressed by practices and solutions that would help to reduce, or hide, the generated meta-data**.

---

[45] http://www.heise.de/ct/artikel/NSA-GCHQ-The-HACIENDA-Program-for-Internet-Colonization-2292681.html?hg=1&hgi=3&hgf=false

[46] See also Section 5.1.1

[47] Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri and John Scott-Railton. For Their Eyes Only: The Commercialization of Digital Spying. Citizen Lab and Canada Centre for Global Security studies, University of Toronto. May 2013.

[48] https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/

[49] http://www.spiegel.de/international/world/ghcq-targets-engineers-with-fake-linkedin-pages-a-932821.html

[50] https://firstlook.org/theintercept/2014/03/12/nsa-plans-infect-millions-computers-malware/

[51] https://www.privacyinternational.org/sii/companies/Hacking_Team

[52] https://www.privacyinternational.org/sii/document/441689-poseidon-ip-information

[53] http://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance

There are a number of available techniques that citizens can use to protect their privacy online. The techniques to use depend on the type of communication, the device and platform used for communication and the life-cycle of data that shall be protected.

One of the first and most obvious steps for achieving this is to **restrict the use of Cookies in the browser settings**. Most browsers include options for "stealth" navigation, which impede the storage of navigation data (images, text, Cookies, history, etc.). This does, however, influence the user experience, since preferences for a particular page or services which are normally stored in Cookies cannot be maintained. It must also be said that **this option offers virtually no privacy protection beyond the local level**, because visited websites can for example be identified by matching a user's IP address on the server end.

Other techniques are related to **hiding the IP address** when surfing on the Internet and the **application of full end-to end encryption**, both, concerning communication channel and content. Even if full protection is not possible and agencies such as NSA are suspect of having tried to break some encryption algorithms[54], cryptography experts[55] do still recommend using encrypted communications for the protection of the meta-data. Even the whistle-blower Edward Snowden stated that: "*properly implemented* ***strong crypto systems are one of the few things you can rely on***"[56]. Similarly, ProPublica[57] journalist Julia Angwin declares: "*ProPublica has written about the NSA's attempts to break encryption, but we don't know for sure how successful the spy agency has been, and security experts still recommend using these techniques*"[58]. Her article recommends using encryption for user data both, at transfer and at rest.

A number of technical options available to citizens for preventing and counteracting mass surveillance practices are outlined in Chapter 7.

[54] http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?_r=0

[55] http://www.technologyreview.com/news/519171/nsa-leak-leaves-crypto-math-intact-but-highlights-known-workarounds/

[56] http://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower?CMP=twt_gu#block-51bf3588e4b082a2ed2f5fc5

[57] http://www.propublica.org/

[58] http://www.propublica.org/article/privacy-tools-encrypt-what-you-can

4 CRYPTOGRAPHY RELIABILITY IN A "POST SNOWDEN" WORLD

The revelations of Edward Snowden demonstrate the **lack of awareness of Internet stakeholders** – first of all, the average Internet users - **on security breaches** such as deliberate cryptography implementation flaws in certain software/hardware platforms.

> The change of focus of some agencies after the World Trade Center attack[59] from lawful[60] interception (targeted surveillance) to mass surveillance converts the essence of cryptography from being an end-to-end security solution to a tool prone to be used for compromising the privacy of millions of citizens.

The Heartbleed[61] and Go-to-fail[62] bugs are clear examples that illustrate this statement. **Both flaws can be exploited to massively break cryptography that is utilised in millions of servers and mobile devices worldwide**. The publication and awareness of such flaws coincides with concrete movements of national security agencies[63] which raise suspicions among the community about their prior knowledge of the origin, deployment and exploitation of these bugs.

Cryptography implementations derive from cryptography specifications[64] and these are based on the willingness of deploying security policies over connected systems with the aim of assembling reliable and trustworthy ICT platforms and systems.

The deprived control of these cryptography chains (from legal and specification readiness to implementation) has created a range of uncontrolled IT products (and product families) that are implementing faulty algorithms (deliberately or not) which do not comply with their original specification purposes. The principal conclusion that can be drawn from this analysis is that

> A process is needed that allows to check, validate and certify that cryptography chain implementations are correctly mapped to their requirements and thereby guaranteeing the correctness of their behaviour and functioning.

Beyond unintended cryptography implementation glitches[65], a number of media reports directly accuse **certain stakeholders** of **purposefully pursuing the inclusion of backdoors in encryption technologies**. The collaboration of NSA with RSA with the objective of gaining access to encrypted information by introducing a flawed random number generator in RSA's algorithm is one of the most prominent cases[66].

Other forms of breaking encryption are related to **social engineering techniques and** intrusion techniques that allow **intercepting data before it is getting encrypted**. Although these techniques are not directly exploiting cryptography vulnerabilities, it must be pointed out that

---

[59] '[…]The current PRISM and other NSA activities and their relationship to other intelligence services and private companies in the US further illustrates the limitations of powers of the judiciary (FISA) over intelligence activities […]' – From the study of National programmes for mass surveillance of personal data in EU Member States and their Compatibility with EU Law.

[60] https://www.documentcloud.org/documents/409136-21-200810-iss-prg-amesys.html#document/p9/a119301

[61] http://heartbleed.com/

[62] https://gotofail.com/

[63] http://www.bloomberg.com/news/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers.html

[64] For example TLS specification: http://tools.ietf.org/html/rfc5246

[65] Exploiting weaknesses (bugs, software design flaws and backdoors) in the encryption program to allow decrypting the information without the need for obtaining the encryption keys from one of the two end-points

[66] http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220

> For attackers, obtaining encryption keys through adequate intelligence techniques on one of the two end-points is todays' principal challenge.

This was, for instance, the strategy applied in the so called Celebgate[67] hack, where phishing attacks, combined with brute force were used to compromise authentication credentials.

4.1 Current and upcoming cryptography problems

The new generation of encryption technology is proficient enough to avoid deterministic brute force attacks if its implementation and configuration parameters are well set up.

> Major attacks occur when implementations of current encryption technologies do not faithfully comply with their specifications, or when bugs and flaws – sometimes deliberately – are injected at code level[68],[69].

However, mass surveillance attacks are not only confined to a specific encryption factor. There are many other means (social engineering, malware, Trojans, worms) of exploiting IT-systems, as the following examples of exploits compromising encryption and other security mechanisms show:

"goto fail" SSL vulnerability

Secure Socket Layer (SSL) is a protocol utilized to encrypt and authenticate server connections. For exchanging information in a secure way, the web browser and the server have to share a key. In this case, the server must send a series of initial parameters that must be digitally signed. This signature has to be verified by the client (navigator).

In some proprietary implementations (such as Apples iOS) for verifying this piece of code (signature) a 'goto fail' instruction was (either deliberately or not) duplicated in the source of the verification code, which led to a severe vulnerability of the SSL protocol that would allow anyone to eavesdrop on the secured connections by applying a man in the middle attack.

The 'goto fail' flaw affected Apple mobile products that run iOS 6 and iOS 7 as well as desktop products that run OS X 10.9 (Maverick). iOS 6 was launched in September 2012, which means this vulnerability existed about two years before it was published and patched.

Heartbleed

Heartbleed is a security bug revealed in April 2014. It appeared in an OpenSSL cryptography library which is commonly utilized for implementing TLS (Transport Layer Security). Its vulnerability proceeds from the improper validation on the implementation of the "Heartbeat" extension of TLS. This bug is categorized as a buffer over-read that consents reading more data than should be permitted. At the time of disclosure, around half a million of the Internet's secure web servers certified by trusted authorities were alleged to be vulnerable to the attack, permitting theft of the servers' private keys and users' session Cookies and passwords[70].

Shellshock

Beside Heartbleed, Shellshock has been identified as a bug that possibly affects millions of workstations running on Linux and Apple's Mac OS. The bug was discovered in a software component called Bash (Bourne-Again Shell) which is included in many Linux/Unix systems as the default command-line interface. Due to this vulnerability, it is possible to execute random commands

[67] http://www.dailydot.com/technology/apple-icloud-brute-force-attack-march/

[68] https://gotofail.com/

[69] http://heartbleed.com/

[70] http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html

and take control of the system utilizing Bash. **More than 500 million devices could be infected by this flaw, which seems to have existed since** version 1.03 of Bash that was released in September **1989**. There are already numerous patches available that (sometimes partially) solve the problem, but not all affected devices and servers have been patched already at the time of writing this document.

Phishing attacks: Apple iCLOUD. Celebgate // The Fappening

Recent Phishing attacks that have compromised services provided by Apple's iCLOUD were prominently covered in all types of media. Attackers targeted celebrities and exposed some of their private photos that were saved on the iCloud platform. The attackers used Phishing techniques to access these private areas and files on iCloud. Phishing attacks consist in tricking users into revealing their login credentials by using spoofed emails, websites and the like. In the case of "Celebgate", Apple determined and confirmed that **the hacks did not breach security measures and were not based on encryption failures, but on social engineering attacks**. The victims had received legitimate looking company emails requiring private information (personal material, passwords, credit card numbers, etc.) which they had answered. Hackers used an intelligent brute force approach to crack the stars' secret questions by making repeated guesses using personal information available online. After the Celebgate phishing attack other exploits such as the Kelihos (Waledac) botnet, capable of sending (spam) emails to specific Apple customers, appeared for exploiting the iCloud system.

McAfee, an antivirus vendor, tested end users' skills for identifying phishing emails and showed that

> 80% of 16.000 users fell for at least one in seven phishing emails.

Currently anti-malware companies do provide protection against phishing attacks (Symantec, Kaspersky, Trend, Panda, etc.), but

> Many final users do not adequately protect their computer by updating the latest patches of Operating Systems and/or applications.

Also, suspicious requests on personal information are generally answered without applying a minimum of precaution (and/or common sense) and thus handing over personal and intimate data to potential attackers.

Botnets

Botnets are networks of devices infected with malware that are remotely controlled by one or more attackers and used to perform distributed tasks on behalf of their "owners". Botnets are primarily used for spamming or supporting distributed denial of service (DDoS) attacks. The infection of a computer with the malware required for forming part of a botnet, is commonly achieved through drive-by infections (a malicious website downloads and installs the malware on the computer when the user visits it) or by emails with infected attachments. Security companies such as Afferent Security Labs, Symantec, Trend Micro, FireEye, Umbra Data and Damballa have announced offerings to counter botnets.

APT attack : advanced persistent threats. Industrial field: dragonfly

Dragonfly is another attempt to attack industry and particularly **the electricity sector**. Eastern European countries and Russia collaborated in developing a sophisticated attack on electrical companies based in NATO countries[71] with the objective to disrupt their services. Dragonfly is a compendium of attacks which alternates phishing techniques with the usage of RAT (Remote Access Tools) based backdoors such as "Oldrea" (also known as "Havex" or "Energetic Bear"). Oldrea extracts an infected computers' information once it is installed and sends this information in an encrypted way to a server controlled by attackers. Then by adapting and using the "Karagany" Trojan the attackers are able to run additional plugins, such as tools for collecting passwords, taking

[71] http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat

screenshots, and cataloguing documents on infected computers. Finally, through "trojanizing" different Industrial Control System equipment, the attacker could eventually succeed in sabotaging a power grid. Therefore, **Dragonfly is a complex attack that employs multiple attack vectors**: phishing, exploit kits, remote access tools and Trojans.

Zero-day vulnerabilities

A zero-day vulnerability is a defect in software that is unknown to the vendor and that is **subject to potential exploitation** until the vendor becomes aware and fixes it. Vendors usually release a patch or software update in order to fix security flaws, once they are detected and published. Discussions on zero day vulnerabilities can be found in specialized and private security forums and web pages, but there does also exist a "black/grey market" in which zero day vulnerabilities are sold[72]. **It is suspected that national security agencies, as well as criminal organisations make use of this offer, in order to devise new exploits for which no known remedy exists**[73].

Brute force attacks

Brute force attacks[74] are well known attacks that **explore all or part of possible values in order to extract the password of an end user**. The strength of a brute force attack is inversely proportional to the complexity of employed encryption keys. Indeed, **brute force is not dealing with cryptography vulnerabilities but with key vulnerabilities**. The simpler the key (for instance, by generating passwords of 4 numbers), the easier it is to extract the key by this mechanism.

Today brute force attacks are often used and quite efficient when preceded by a social engineering attack which reveals part (or all) of the encryption key, or provides knowledge that helps to reduce the possible values for extracting the target's key (Celebgate is a clear example for this.)

> The level of user awareness related to these issues is substantially low and thus, it is important to make the end user understand that implementation errors and bugs are normally fixed by upgrading and updating software and components. This means that it is the user's own responsibility to keep the applications properly updated.

Web technology is encrypted through SSL/TLS technology. **The protocol itself is correct** and is able to maintain confidentiality, integrity and therefore users' privacy, **but concrete encryption implementations have shown to contain bugs**.

A protocol is usually defined by its common formal reference specification. This specification gets implemented by different parties, which inevitably leads to different code bases. OpenSSL[75], for instance, is an open source library often used in Linux platforms. The Heartbleed bug detected in (some of) these implementations shows that **even open source code** which is scrutinized and reviewed by a large community of developers and which had been deployed and operative for years **does not guarantee to be free of any software flaw**.

> Software flaws in the implementation of encryption algorithms (e.g. in negotiation, or key exchange functions) can lead to vulnerabilities which may be easily exploitable, regardless of the complexity, or the theoretical strength and quality of the applied encryption technique. Since the implementation is the

[72] https://www.mitnicksecurity.com/shopping/absolute-zero-day-exploit-exchange
[73] http://insidecybersecurity.com/Cyber-General/Cyber-Public-Content/policy-debate-looms-on-us-role-in-market-for-zero-day-cyber-threats/menu-id-1089.html
[74] https://www.owasp.org/index.php/Brute_force_attack
[75] https://www.openssl.org/

critical part that defines the overall quality of encryption solutions, a process for guaranteeing the satisfaction of these indicators must be applied.

This **process should cover the design and engineering phase**, ensuring that appropriate measures are taken to **avoid injecting software errors, but also consider certification of the final product code** by external independent certification bodies. NIST is providing such a service[76], through which it informed the public about a weakness (that could be exploited as a backdoor) of the Dual_EC_DRBG encryption algorithm and "*recommends that current users of Dual_EC_DRBG transition to one of the three remaining approved algorithms as quickly as possible*"[77]

The quality and reliability of a specific encryption implementation, or service, **can be compared by evaluating** some **objective indicators**, which are:

- Asymmetric cryptography usage for authentication
- Key strength or Passphrase strengthening
- Cryptography algorithms combination
- Dynamic key re-generation capacity
- Hidden containers
- Pre-boot authentication
- Multiple keys usage for a particular process
- Hardware acceleration in particular situations, explicitly designed for cryptography.

Such an evaluation can be performed statically by analysing one by one each of the implementations for the encryption services, not their specification[78].

The increasing concern of citizens about their privacy is pushing more and more Internet service providers towards offering (communication) services that are secured and encrypted by default. One of the last decisions in this direction was Apple's and Google's announcement[79] of the imminent introduction of fully encrypted (voice and text) communications in their operating systems product family for smartphones. Google also announced in March 2014 that its Gmail service is using "*an always-on HTTPS connection and encrypting all Gmail messages moving internally on its servers*"[80]. Also "Whatsapp", a text-based message application with more than 500 million users worldwide, has switched to encrypting the communication between the phones and their servers[81]. Google's new SPDY gateway[82] is another attempt to perform secured transfers over Internet.

The Electronic Frontier Foundation has published a table depicting the current state of encryption practices concerning the major Internet companies[83] which shows that

DropBox, Facebook, Google, Microsoft, Sonic.net, Spideroak, Twitter and Yahoo do implement all encryption best practices suggested by the EFF. Other service providers like Amazon, Apple, FourSquare, LinkedIn, MySpace and tumblr, among others, do still lag behind when it comes to enabling encryption across their networks.

[76] http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html
[77] http://www.nist.gov/itl/csd/sp800-90-042114.cfm
[78] http://www.csjournals.com/IJCSC/PDF2-1/Article_22.pdf
[79] http://www.bbc.com/news/technology-29276955
[80] http://nakedsecurity.sophos.com/2014/03/21/google-switches-gmail-to-https-only/
[81] https://www.whatsapp.com/faq/en/general/21864047
[82] http://www.google.com/patents/US20130297814
[83] https://www.eff.org/deeplinks/2013/11/encrypt-web-report-whos-doing-what

When a browser connects to a secure HTTPS[84] server, it first sends some security parameters which establish the security configuration, also called "cipher suite", of the connection. The problem with SSL is that once an attacker gets hold of the common private key, all information exchanged in sessions that have been encrypted with this key can be decrypted. The **Perfect Forward Secrecy (PFS) technique makes it more difficult to decrypt data in retrospect** because each session has its own private key (no common private key like in SSL is used).

Perfect Forward Secrecy **(PFS) is very good solution[85] for preventing access for mass surveillance purposes**. It uses new key generations for each session and if a security breach occurs, only the key being used in a particular session is compromised but never all the data transfer in previous sessions. **The main technical problem with Perfect Forward Secrecy is its performance and throughput[86]**. Compared to normal asymmetric algorithms it requires much more CPU cycles for being executed (15-27% throughput increase). This decrease in load-times of web pages would be the trade-off for achieving higher levels of security and is the reason why PFS is not enabled on the majority of websites, including a number of popular trade and retail sites, as well as large banks[87].

> Perfect forward secrecy means that any recorded traffic from past sessions remains useless even if the long-term server keys are subsequently revealed. It seems essential that perfect forward secrecy becomes universally used.

However, it should be mentioned that these **attempts to increase the privacy of end users by enabling strong encryption by default are not welcome by all stakeholders**. James B. Comey, the director of the FBI, in a speech published on their website[88] is insistently warning on the danger of the law enforcement "going dark" as a consequence of these encryption efforts. Comey (and others) argues that "*law enforcement needs to be able to access communications and information* [i.e. evidence] *to bring people to justice*, but that with "*sophisticated encryption* [being available to end users for securing their conversations], *there might be no solution, leaving the government at a dead end – all in the name of privacy and network security*". He goes even so far as to call on the U.S. Congress to make unlockable encrypted devices as announced by Apple unlawful[89].

4.2 Malware in platforms and end-points

Traditionally, malware has been inoculated on platforms with the highest rates of impact in industry and society, resulting in Windows PCs being the primary target of hackers and attackers. This situation has led Microsoft to prioritize security aspects through its Trustworthy Computing Initiative.[90]

Linux systems do apparently get less targeted by attackers. But their increased usage in server stacks (e.g. LAMP) together with recently published flaws (see Heartbleed and Shellshock), make this system more and more interesting for hacking attacks.

With the advent of ubiquitous mobile computing and the Internet of Things (IoT) the situation is changing. The ever **growing number of wireless** connected (heterogeneous) **devices,** sensors and

[84] HTTPS makes use of the SSL/TSL protocol
[85] http://www.theregister.co.uk/2013/06/26/ssl_forward_secrecy/
[86] http://vincent.bernat.im/en/blog/2011-ssl-perfect-forward-secrecy.html
[87] http://www.computerworld.com/article/2473792/encryption/perfect-forward-secrecy-can-block-the-nsa-from-secure-web-pages--but-no-one-uses-it.html
[88] http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course
[89] http://www.washingtonpost.com/blogs/the-switch/wp/2014/10/17/fbi-director-comey-calls-on-congress-to-stop-unlockable-encryption-good-luck-with-that/
[90] http://www.microsoft.com/en-us/twc/

activators that lead to changing usage patterns **makes attackers shift to these platforms**. They can be attacked and potentially damaged by applying new and innovative intrusion approaches that may lead to a highly negative societal impact.

> A novel hardware scenario is the advent of the smartphone which encompasses computer features and resources but additionally incorporates voice, mobility and camera services that make the smartphone the platform which exposes the largest attack surface.

Indeed, as leaked documents show, national security agencies have dedicated much effort to implement tools for exploiting not only mobile and smartphone connections, but also the endpoint[91] itself.

4.3 Cryptography and cyber warfare arena

Cyber-warfare is a new frontier on the geopolitical strategy battlefield. Actually, the Tallin Manual[92] defines and converts a cyber-attack as a rudimentary war attack.

Some media reports directly accuse Asian manufacturers of purposefully including backdoors in their chips. The most prominent of these accusations is based on a paper published by Sergei Skorobogatov, a student of Cambridge University, in which he claims to have identified a backdoor in Actel/Microsemi's ProASIC3 chip[93]. However, a subsequent discussion of the findings in the security community showed that the backdoor (a JTAG debugging interface) was already included in the software design of the chip, that was developed by Actel, an American company[94].

In 2011, the US government released the White House Cyber Policy Review[95], warning of risks related to the delocalization of manufacturing plants: "*The emergence of new centers for manufacturing, design, and research across the globe raises* ***concerns about the potential for easier subversion of computers and networks through subtle hardware or software manipulations****. Counterfeit products have created the most visible supply problems, but* ***few documented examples exist of unambiguous, deliberate subversions***." This suspicion has led Western countries and particularly the Five Eyes coalition to prohibit the usage of certain Chinese built equipment in intelligence agencies[96].

But it's not only the Asian countries that are allegedly designing stealth backdoors into their products. Documents revealed by Edward Snowden affirm that the NSA is secretly and routinely intercepting "*routers, servers, and other computer network devices being exported from the U.S. before they are delivered to the international customers*. ***The agency then implants backdoor surveillance tools, repackages the devices with a factory seal, and sends them on****. The NSA thus gains access to entire networks and all their users*."[97]

> However, there are no evidences that the affected product vendors have cooperated with the NSA to install the backdoors.

[91] http://cryptome.org/2013/12/nsa-ant-mobilfunk.pdf
[92] https://www.ccdcoe.org/tallinn-manual.html
[93] https://www.cl.cam.ac.uk/~sps32/ches2012-backdoor.pdf
[94] http://www.cl.cam.ac.uk/~sps32/microsemi_re.pdf
[95] http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
[96] http://securityaffairs.co/wordpress/16748/hacking/spy-agencies-ban-on-lenovo-pcs-due-to-backdoor-vulnerabilities.html
[97] Greenwald, G.: No Place to Hide: Edward Snowden, the NSA, and the U. S. Surveillance State, Metropolitan Books, New York (2014)

In fact, all affected vendors claimed they were unaware of the vulnerabilities their systems could have or of any modification that could have been done to these systems. Edward Snowden said in a recent interview

> "*The Companies did not know it.* […] *the companies couldn't have imagined that the intelligence communities would break in the back door,* […] *but they did, because they didn't have to deal with the same legal process as when they went through the front door*" [98]

Other reports suggest that the NSA is also collaborating with major vendors of encryption technology with the objective of gaining access to encrypted information. This is achieved by introducing a flawed generation of random numbers that serve as seeds for encryption in the RSA algorithm[99].

A "Der Spiegel" report claims that the NSA is using a program out of their ANT toolbox catalogue that "*attacks the firmware in hard drives manufactured by Western Digital, Seagate, Maxtor and Samsung, all of which, with the exception of the latter, are American companies*"[100]

Summarising this information,

> It is not possible to pinpoint specific countries or even regions that tend more than others to include malware in hard or firmware. It rather looks as if different parties in all relevant production areas may be using such a strategy if national or security interests are concerned.

4.4 Telecommunication sector

Concerning the telecommunication sector, three main issues are addressed from a security point of view:

- Governmental disruption on Telecom operators[101]. According to "Washington Post" and "Forbes"[102], the NSA paid Telecom Operators such as Verizon and AT&T for access to 81% of all international phone calls into the US.
- Network vulnerabilities attack. It stresses on the attacks to 2G and 3G networks which are possible due to the fall-back mechanism that enables 3G connections to switch to 2G, a protocol that can easily be intercepted.
- Malware in the mobile device/handheld. New viruses, Trojans and backdoors are multi device, multi-platform and oriented to mobile devices (such as StealthGenie or mSpy[103]). Mobility, GPS, Gyroscope and Camera factors **increment the potential attack surface of mobile devices** compared to traditional PC or server vulnerabilities.

There are different ways to attack GSM networks:

- Cryptographic attacks
- OTA attacks (Over The Air)

[98] http://www.thenation.com/article/186129/snowden-exile-exclusive-interview#
[99] http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220
[100] http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html
[101] The NSA and GCHQ allegedly had secret access to the network of Deutsche Telecom
[102] http://www.forbes.com/sites/robertlenzner/2013/09/23/attverizonsprint-are-paid-cash-by-nsa-for-your-private-communications/
[103] http://www.mspy.com/en/

- Attacks from operators
- Memory corruption attacks
- Protocol vulnerabilities

The **encryption of 3G networks covers only the connection** between the end user phone and the operator base node (base station), the rest of communications are not encrypted.

GSM uses a variety of protocols: user identification, user authentication and data and voice transmission. Those algorithms are distributed among the GSM operator, the mobile phone and the SIM. Data and voice transmission encryption is implemented by A5 protocol, once the user is authenticated in the network. The A5 protocol has 3 different versions A5/1, A5/2 and A5/3. The A5/1 protocol used in GSM and responsible for maintaining the privacy of communications has been broken through reverse engineering. **It is possible to decipher GSM communications in real time**, intercepting voice and data from any user[104].

The 2G standard also has been broken and **3G connections can be handed over to 2G connections and thus be subject to attacks**. This is, for instance, the strategy applied by 3G Cat, an IMSI/IMEI/TMSI Catcher[105] offered by the Israeli company Ability. As long as operators do not eliminate the 2G protocol, there will always be an access to eavesdrop voice and data during the transmission.

The protocol used for ciphering 3G is denominated Kasumi[106] (A5/3). Kasumi is based on an encryption technique called Misty that belongs to a subgroup of Feistel[107] techniques. KASUMI is an agile implementation of traditional Misty technique of 128 bits. **The simplification of the algorithm has evoked new vulnerabilities**, such as the so-called "sandwich attack", which can break an A5/3 encryption "*in less than two hours on a single PC*"[108]

4G is a new generation protocol which supports all Internet Protocol (IP) based communications. But since it is based on the TCP/IP protocol **the 4G protocol inherits both, the potential and the weaknesses of TCP/IP**, drawing particular attention to the large amount of hackers with IP knowledge.

Neil Cook, chief technology officer at Cloudmark, a US based security company, claims that **4G is "*inherently less secure*" than previous mobile protocols**[109]. "*Before 4G, all voice and data traffic between the user's device and the core of the network was encrypted and tightly-controlled by the mobile operator*". "***Many operators*** *around the world, including some in Europe,* ***have chosen to deploy 4G leaving the traffic between the core network and some or all of their cell sites un-encrypted***," said Patrick Donegan, senior analyst at Heavy Reading[109]. The portion of the network which is unencrypted by default is called backhaul. Most operators in Europe (not all) encrypt this network fragment with IPsec.

> The current vulnerabilities of telecommunication protocols of all generations, combined with the extensive attack surface presented by mobile devices make these devices an easy target for attacks.

[104] http://www.interceptors.com/decrypt-system/GSM.html
[105] http://www.interceptors.com/intercept-solutions/detects-parameters-3G-networks.html
[106] http://en.wikipedia.org/wiki/KASUMI
[107] http://en.wikipedia.org/wiki/Feistel_cipher
[108] http://eprint.iacr.org/2010/013.pdf
[109] http://www.telegraph.co.uk/technology/internet-security/10951812/4G-inherently-less-secure-than-3G.html

Other secure voice networks projects include the Secure Communication Interoperability Protocol (SCIP)[110], an application protocol designed by the US Department of Defense (DoD) and the NSA to operate independently of the characteristics of the underlying network channel. SCIP uses public cryptography (suite B) and is approved by NATO for protecting secret information.

[110] http://cryptome.org/2012/07/nsa-scip.pdf

5 EFFICIENCY OF COMMERCIAL PRODUCTS FOR DOING MASS SURVEILLANCE

Mass surveillance is a business sector in which commercial companies are selling software applications and tools for surveillance purposes as advanced solutions for lawful communications data[111] (including both meta-data and content) interception, collection, processing and/or analysis for intelligence organizations, national security, governments and Law Enforcement Agencies (LEA). The vendors provide these organizations with intelligence platforms and tools that collect, process and analyse both, mass and targeted communications data.

While lawful interception warranted by court orders and based on reasonable evidences of unlawful or terrorist activities **is a necessary and legitimate instrument** for intelligence, security and LEAs, the **indiscriminate interception of communication data** without evidence **is considered a threat to civil liberties** such as the right to freedom of opinion and expression. These civil liberties are essential human rights in democratic societies and of particular importance for safeguarding independent journalism and political opposition.

> Mass surveillance practices can only be hindered, but not be completely avoided on a technical terrain. Equilibrium between legitimate national security interests and civil liberties has to be found on the political level and must be based on a public discussion of the societal and civil values affected and at stake.

5.1 Commercially available mass surveillance products

A HRC report on the right to freedom of opinion and expression[112] defines five different modalities of communications surveillance:

1. Targeted communications surveillance
2. Mass communications surveillance
3. Access to communications data
4. Internet filtering and censorship
5. Restrictions on anonymity

A presentation during the ISS (Intelligence Support Systems for lawful interception, electronic surveillance and cyber intelligence gathering) World Middle East 2014 conference introduced the top ten Internet challenges faced by law enforcement, which are the following[113]:

[111] Meta-data definition: information about an individual's communications (e-mails, phone calls and text messages sent and received, social networking messages and posts), identity, network accounts, addresses, websites visited, books and other materials read, watched or listened to, searches conducted, resources used, interactions (origins and destinations of communications, people interacted with, friends, family, acquaintances), and times and locations of an individual, including proximity to others. Ref: Human Rights Council, UN. A.HRC.23.4: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, April 2013.

[112] Human Rights Council, UN. A.HRC.23.4: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, April 2013. http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

[113] https://www.documentcloud.org/documents/1215458-1299-telestrategies-presentation-challenges.html#document/p46/a178126

- fibre bandwidth growth, which concerns DPI and fibre optical probes vendors.
- smartphones,
- encryption,
- social media monitoring,
- increasing data volume, being the solution based on Big Data analytics.
- tactical surveillance, related to geo-fenced calls and 3G and 4G antenna coverage.
- all IP (Long Term Evolution) infrastructure, replacing circuit switched networks.
- dark web, which is enabled by TOR and Bitcoin[114].
- dark email, being of special interest two initiatives to an all encrypted email world: IETF's Prism-proof email protocols[115] and dark mail alliance.
- regulatory shortcomings, related to the Laws that support the Lawful Intercept. According to the presentation, **most of these Laws are outdated and are voice circuit switched networks based**.

A number of vendors are addressing these challenges and openly advertise the features and capabilities of their products:

- Verint[116], headquartered in Melville, NY, offers a product portfolio including "*mass interception solutions for nationwide networks and tactical solutions for GSM networks*".
- Nice[117], announces its NiceTrack Mass Detection Center as a "*fully-integrated platform providing nationwide interception, monitoring and analysis*".
- Amesys[118], a French company part of the Bull group, sells its "Eagle" surveillance system capable of both, lawful and mass interception.

Other providers like Clear Trail[119] apply a more discreet marketing strategy and do not publicly expose product details.

While **the sale of these commercially available surveillance tools is restricted to state or governmental authorities** and many vendors do explicitly state this policy on their respective websites. However, the UNHRC Report on the promotion and protection of the right to freedom of opinion and expression highlighted the sale of these tools to governments of states with a questionable democratic and human rights record:

> *Mass surveillance technologies are often sold to countries in which there is a serious risk that they will be used to violate human rights, particularly those of human rights defenders, journalists or other vulnerable groups.*[112]

Countries like Libya, Bahrain, Syria, Egypt and Tunisia have reportedly used or are using software distributed by the principal security vendors in this market. Morgan Marquis-Boire states in a report on the commercialization of digital spying that "*while the majority of these companies (surveillance vendors) claim to sell their products to a restricted client base of law enforcement, military, and intelligence agencies, this report shows another example of* ***commercial network intrusion tools being used against dissidents in countries with poor human rights records***." [120]

[114] https://bitcoin.org/
[115] http://prismproof.org/index.html
[116] http://www.verint.com/index
[117] http://www.nice.com/
[118] http://www.amesys.fr
[119] http://www.clear-trail.com/
[120] Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri and John Scott-Railton. For Their Eyes Only: The Commercialization of Digital Spying. Citizen Lab and Canada Centre for Global Security studies, University of Toronto. May 2013. https://citizenlab.org/storage/finfisher/final/fortheireyesonly.pdf

5.1.1 Highlighted Vendors

The following sections describe some of the major vendors of commercial surveillance software and tools which have been accused of providing countries that violate human rights with surveillance technology

5.1.1.1 Gamma Group

Gamma Group is an UK/Germany based company that "*provides National and State Intelligence Departments and Law Enforcement Agencies with advanced technical surveillance and monitoring solutions and advanced government training as well as international consultancy*"[121].

FinFisher is a commercial intrusion kit distributed by Gamma Group and is **considered to be one of the most advanced surveillance solutions in the market**. This product includes Trojans to infect PCs, mobile phones, other consumer electronics and servers, as well as technical consulting. The FinSpy spyware software can be considered as FinFisher's remote monitoring product. FinSpy captures information from an infected computer, such as passwords and Skype calls, and sends the information to a FinSpy command & control server.

In 2013, the Citizen lab in the University of the Toronto published a map of FinFisher proliferation around the world, which shows the results of scanning for characteristics of FinFisher Command and Control servers[122] that have been found in 25 countries: Australia, Bahrain, Bangladesh, Brunei, Canada, Czech Republic, Estonia, Ethiopia, Germany, India, Indonesia, Japan, Latvia, Malaysia, Mexico, Mongolia, Netherlands, Qatar, Serbia, Singapore, Turkmenistan, United Arab Emirates, United Kingdom, United States and Vietnam.

However, the authors of the investigation pointed out that the list of servers might be incomplete due to the large diversity of ports used by FinFisher servers. Furthermore, they said that **discovery of a FinSpy command and control server in a given country is not a sufficient indicator to conclude the use of FinFisher by that country's law enforcement or intelligence agencies**. In some cases, servers were found running on facilities provided by commercial hosting providers that could have been purchased by actors from any country.

5.1.1.2 Hacking Team

Hacking Team[123] is a surveillance software vendor headquartered in Milan, Italy, that offers "offensive" capabilities for LEAs and intelligence agencies. They state about their Remote Control System solution that: "*In modern digital communications, **encryption is widely employed to protect users from eavesdropping**. Unfortunately, **encryption also prevents law enforcement and intelligence agencies from being able to** monitor and **prevent crimes and threats** to the country security. **Remote Control System (RCS) is a solution designed to evade encryption by means of an agent directly installed on the device to monitor**. Evidence collection on monitored devices is stealth and transmission of collected data from the device to the RCS server is encrypted and untraceable*."

Their customer policy claims that "*we don't sell products to governments or to countries blacklisted by the U.S., E.U., U.N., NATO or ASEAN. We review potential customers before a sale to determine whether or not there is objective evidence or credible concerns that Hacking Team technology provided to the customer will be used to facilitate human rights violations.*"

Several media reports and **IT security experts have found traces of their software in** countries with a questionable position about human rights such as **Morocco and United Arab Emirates.**[120]

[121] https://www.gammagroup.com/Default.aspx
[122] https://citizenlab.org/storage/finfisher/maps/5-clicktwice-highrez.jpg
[123] http://www.hackingteam.it/

5.1.1.3 Blue Coat

Blue Coat[124] is a US based company that is specialized in online security but it is well known in the surveillance market for its Deep Packet Inspection (DPI) technology based equipment. This surveillance solution has allegedly been sold to countries such as Syria and Burma (Myanmar). [125]

IT researchers from the Citizen Lab of the University of Toronto carried out an investigation on Blue Coat devices and highlighted that **Blue Coat solutions**, capable of filtering, censorship and surveillance, **are being used around the world**. They found 61 Blue Coat ProxySG devices and 316 Blue Coat PacketShaper appliances in the following locations[125]:

- Blue Coat ProxySG: Egypt, Kuwait, Qatar, Saudi Arabia, the UAE.
- PacketShaper: Afghanistan, Bahrain, China, India, Indonesia, Iraq, Kenya, Kuwait, Lebanon, Malaysia, Nigeria, Qatar, Russia, Saudi Arabia, South Korea, Singapore, Thailand, Turkey, and Venezuela.

5.2 Legal context for mass surveillance tools and services

In December 2012, the European Union banned the export of information technology that can be used by repressive regimes to censor information, conduct mass surveillance and track people's movements[126]. The USA has also established sanctions against a list of countries, using the blocking of assets and trade restrictions to accomplish foreign policy and national security goals[127]. The list of countries includes Iran, North Korea, Sudan and Syria among others.

> A total of 42 countries already negotiated the inclusion of surveillance technology into the most comprehensive international treaty on export controls, the Wassenaar Arrangement (WA)*[128]*. In 2013 new export controls in surveillance and law enforcement/intelligence gathering tools and IP network surveillance systems or equipment were agreed among the WA participating States.

In October 2014, the European Commission added specific forms of surveillance technology to the EU control lists on dual use items[129]. **This control enables European Commission to identify the accountability of selling, transferring and exporting surveillance technology by the private sector**.

Surveillance is subject to different international and national legal norms:

General public international law

As stated by Emeritus Professor Douwe Korff:

Surveillance by one state over the Internet activities and electronic communications of citizens and officials of another state with which the first state is not at war at that time, without the express consent of the other state, and which involve illegal activities by agents of the first state perpetrated within the territory of the other state, is a violation of the sovereignty of the targeted state. This is a rule of primary international law[130].

Moreover,

---

[124] https://www.bluecoat.com/

[125] https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/

[126] http://www.europarl.europa.eu/news/en/news-room/content/20121207IPR04411/html/Ban-exports-of-information-technology-to-repressive-regimes

[127] http://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx

[128] http://www.wassenaar.org/introduction/origins.html

[129] http://ec.europa.eu/transparency/regdoc/rep/3/2014/EN/3-2014-7567-EN-F1-1-ANNEX-1.Pdf

[130] Expert Opinion prepared for the Committee of Inquiry of the Bundestag into the "5EYES" global surveillance systems revealed by Edward Snowden, Committee Hearing, Paul-Löbe-Haus, Berlin, 5 June 2014.

…surveillance of citizens and officials of one state-party to an international human rights treaty by agents of another state-party to that treaty, from the territory of the latter state, but which violates the obligations of the latter state party under that treaty, not only violates that treaty but (since it harms the interests of the targeted state and its officials and citizens) also constitutes an internationally unlawful act against the state whose citizens and officials are affected. That is a rule of secondary international law.

International and European human rights law

International human rights law is mainly treaty-based. The International Covenant on Civil and Political Rights (ICCPR) is the International human rights treaty and the European Convention on Human Rights (ECHR) is the European human rights treaty.

The provisions in the ECHR and the ICCPR (on the rights of private life, freedom of expression, freedom of information, and freedom of association) all stipulate or imply that those rights can only be restricted or interfered with on the basis of "law"; and that such restrictions or interferences must serve a "legitimate aim", and must be "necessary" to achieve that aim.

These **aims include public safety, prevention of crime, protection of morals and of the rights of others, and national security**. The UN has published a declaration on the use of surveillance technologies and their impact on human rights, specifically on the right of privacy:

***In most States, legal standards are either non-existent or inadequate to deal with the modern communications surveillance environment**. As a result, States are increasingly seeking to justify the use of new technologies within the ambits of old legal frameworks, without recognizing that the expanded capabilities they now possess go far beyond what such frameworks envisaged. **In many countries, this means that vague and broadly conceived legal provisions are being invoked to legitimize and sanction the use of seriously intrusive techniques**.* [131]

The UN states that **when surveillance is conducted lawfully, the data collected can be necessary and effective for the law enforcement purposes**. But **mass interception technology eliminates any considerations of proportionality**, enabling the State to collect personal data without gaining authorization for each individual case of interception and this situation creates interference with privacy. Moreover, **a company that provides mass surveillance technology to States without adequate safeguards** in place or where the information is otherwise used in violation of human rights, the company **risks being complicit in or otherwise involved with human rights violation**.

> As reported by the UN Special Rapporteur on the right to freedom of opinion and expression, "*the private sector has been complicit in developing technologies that enable mass or invasive surveillance in contravention of existing legal standards*"[132].

International and European data protection law

In 1995, the first (and still the main) EC directive on data protection[133] was adopted, followed by a specialised subsidiary directive on privacy and electronic communications in 2002 (the "e-Privacy

[131] A/HRC/27/37: The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights. 30 June 2014.

[132] Human Rights Council, UN. A.HRC.23.4: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, April 2013.
http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

[133] 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, 23 November 1995, OJ L.281, p. 31ff.

Directive"[134]). In 2006, the e-Privacy Directive was amended by the so-called "Data Retention Directive"[135].

In Europe, **data protection is seen as an essential pre-requisite for the protection of other freedoms**, including freedom of thought and freedom of expression. But the law allows for exceptions which must be: *a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system.*

But in a crucial recent judgment, *the Court of Justice ruled that* ***the Data retention Directive*** *failed to meet these requirements, because it imposed departures from the core data protection principles that were not proportionate to the stated aim of the Directive[130]. The Directive* ***was fundamentally flawed because it*** *both* ***lacked sufficiently "clear and precise rules"*** *to circumscribe the capturing of data,* ***and "sufficient safeguards against abuse"****, the Court concluded that in adopting the Data Retention Directive in the form it did, "the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality".* [136]

5.3 Effectiveness of surveillance products and resources needed

Due to the lack of operational information on mass surveillance tools it is only possible to judge on their effectiveness and the skill levels needed to operate them, based on publicly available information on some of these tools. The most detailed publicly accessible feature description of a specific surveillance tool is the product information of the FinFisher suite, published on Wikileaks.[137]

This surveillance suite is composed of different components along the three product vectors "Remote Monitoring & Infection Solutions", "Tactical IT Intrusion Portfolio" and "IT Intrusion Training Program". While some of the components do not require IT-trained personnel for being operated, others require the operating personnel to have solid knowledge about where or what to look for in a targeted system and for interpreting the information and data they retrieve from target systems.

The **operation of** the proper **FinFisher components is comparable to the operation of** most **mainstream software**, judging by the screenshots of their user interfaces exposed in the product portfolio. The FinSpy user manual[138] gives detailed instructions on how to install and operate the software, reads like an installation manual of any other software package on the market and does not require extensive IT knowledge to understand and follow its instructions. The user interfaces of the different components include options for multiple data views (including pre-defined and user adaptable reports), structural analysis, definition of importance levels, filters and colour codes for facilitating the processing of the intercepted data.

---

[134] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, commonly referred to as the e-Privacy Directive), 31 July 2002, OJ L 201, p. 37ff.

[135] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 13 April 2006, OJ L105, p. 54ff.

[136] Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, of 8 April 2014, available at:
http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=12322
For an early analysis, see:
http://eulawanalysis.blogspot.co.uk/2014/04/the-data-retention-judgment-cjeu.html

[137] https://wikileaks.org/spyfiles4/index.html

[138] https://wikileaks.org/spyfiles4/documents/FinSpy-3.10-User-Manual.docx

The Remote Control System, another surveillance tool offered by Hacking Team[139] and which is installed on target systems via Email attachments, drive-by infection or malicious java applets, **allows its controllers to monitor mouse coordinates, several instant messenger apps, location, internal webcam, clipboard contents, key strokes, running applications, web URLs, screen shots, internal microphone, calendar data and alerts, device information and address book contents**.

> The usage and operation of commercial mass surveillance tools does not require exceptional technical or personnel resources which could only be provided by state or government agencies.

The resources required to process and analyse the data gathered with such tools depend on the adopted surveillance approach and the size of data. While targeted lawful interception produces a limited set of data that may be handled with conventional IT resources, **the indiscriminate gathering of large amounts of data**, as is the case with mass surveillance, **requires massive resources for processing it**.

Much has been written in the media about the purpose and capacities of the data centre the NSA is about to complete building in Utah. The NSA itself does not comment or publish any details on the project, which has led to speculations that the reason behind this datacentre is the objective of archiving (part or the entire) Internet traffic data during a limited period, **so as to be able to inspect it retrospectively**. The estimations of experts on the projected storage capacities of this data centre fluctuate between 12.000 picabytes and various zetabytes or even yotabytes[140]. Since it is not possible to precisely determine the final storage capacity (which is classified information) and despite the fact that this is only one among various data centres the NSA maintains[141],

> It is not possible to make a qualified statement on the *current* interception and storage capacities of the NSA, nor that of other national intelligence agencies. This does however not question national intelligence agencies' general ability of intercepting and storing IP and mobile data:

Based on the documents leaked by Snowden, NSA's **Boundless Informant** big data analysis and data visualization tool **is capable of processing more than 97.000 million Internet data records and 124.000 million telephony data records during a 30-day period**. These data records only include meta-data[142].

"Der Spiegel" reports on monitoring capabilities in **Germany for the period between 10 December 2012 and 8 January 2013**, where **more than 552 million telephony and Internet data were accessed**. The same report numbers the collection of **60 million telephony meta-data in Spain** and **46 million telephony meta-data in Italy** in the same period.

Other leaked documents show the volume of telephony meta-data gathered worldwide that **FASCIA**, NSA's huge database which contains DNR (telephony meta-data), **can manage almost 5.000 million records per day**[143].

Experts predict a continuous increase in storage capacities for the future, but already today companies do manage (distributed) database systems of over 10 EB storage capacity. This suggests that

[139] See also section 5.1.1.2

[140] http://www.forbes.com/sites/kashmirhill/2013/07/24/blueprints-of-nsa-data-center-in-utah-suggest-its-storage-capacity-is-less-impressive-than-thought/

[141] http://www.washingtonpost.com/world/national-security/nsa-growth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871_story.html

[142] http://www.theguardian.com/world/interactive/2013/jun/08/boundless-informant-nsa-full-text

[143] http://apps.washingtonpost.com/g/page/world/what-is-fascia/637/#document/p1/a135288

providing adequate storage capacities for intercepting large amounts of data (even in its raw format) **will not be a technical or organisational problem in the future** and that the possibilities of intelligence agencies being (technically) able to "*pull a complete backup of all Internet traffic in real-time*" are real.

But this does not mean that this information would be immediately accessible. Only the un-encrypted data could be directly analysed, while encrypted data would need to be decrypted first. **The effort for deciphering encrypted data may potentially be huge**, depending on the relative amount of such scrambled data and the strength of the encryption keys (assuming their intact integrity) and technologies used.

> The computing effort required to perform the complex algorithms needed for analysing huge amounts of (Big) data is what is generating the bottleneck in today's endeavour to use the strategy of retrospective inspection for surveillance purposes.

5.4 Cryptography and encryption analysis

One of the main objectives of mass surveillance tools and users thereof is to break encryption that may hinder access to relevant data for intelligence and LEAs. A presentation during ISS (Intelligence Support Systems for lawful interception, electronic surveillance and cyber intelligence gathering) World Middle East 2014 conference[144] proposed the following seven means for defeating encryption:

1. Crack the encryption code (256 and 1024 bit keys)
2. Coerce the private key holder (Certificate Authority) to turn the key over
3. Man in the Middle Attack
4. Introduce weakness in encryption standards (NIST issue)
5. Install spyware
6. Snare the messages before they are encrypted !!!
7. Or just collect the Meta-data

The Spy Files[145] catalogue published by Wikileaks lists a number of examples of commercial **tools that are able to listen to communications even if they are encrypted**. Examples are Hacking Teams' Trojan "Remote Control System", which is "*a stealth system for attacking, infecting and monitoring computers and smartphone*"' for targeted surveillance and pertaining to the category number 5 of the above listed strategies, or SSL Locksmith by ACCESSDATA[146], a solution which *works with any packet analysis or capture solution* […] *to reveal the content of encrypted network communications*".

Some National intelligence agencies are also suspect of having developed such kind of tools for undermining the encryption in secure communications.

> The NSA's program, codenamed "Bullrun" and GCHQ's counterpart, codenamed "Edgehill", serve to break the encryption in widely used online protocols, such as HTTPS, voice-over-IP and Secure Sockets Layer (SSL), which are used to secure online sensitive transactions:

[144] http://www.issworldtraining.com/
[145] https://wikileaks.org/the-spyfiles.html
[146] http://accessdata.com/solutions/cybersecurity/ssl-locksmith

"***By 2015, GCHQ hoped to have cracked the codes used by 15 major Internet companies, and 300 VPNs***." Another program, codenamed "Cheese Name", serves to select those "*encryption keys that might be vulnerable to being cracked by GCHQ supercomputers*". [147]

The Washington Post[148] documented the US$79.7 million research program *Penetrating Hard Targets project* of the NSA which included the research on the future development of "*a **cryptologically useful quantum computer***" which would allow "*breaking all public key encryption, including RSA, which is used for most secure websites and for encrypted e-mail conversations*." Such a tool would allow cracking most types of encryption by brute-force without the need of knowing the encryption keys. [149]

> Due to the lack of (access to) clear evidences, it is difficult to ensure whether these tools are only aimed at lawful targeted surveillance or also envisaged for mass surveillance purposes.

In order to use them in a massive scale they would need to be combined with powerful storage and processing capacities, which are not difficult to achieve with current IT technologies. The achievable scale would therefore depend mostly on the available economic resources invested in it.

Other approaches to defeating communications encryption **are the collaboration** of national security agencies **with commercial vendors of security tools in order to introduce weaknesses in encryption standards**. The case of NSA inducing backdoors in the standards for RSA's random number generator has been extensively documented[150],[151].

[147] http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security
[148] http://apps.washingtonpost.com/g/page/world/a-description-of-the-penetrating-hard-targets-project/691/
[149] http://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html
[150] http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf
[151] See also Section 6.3.4

6 TECHNICAL CREDIBILITY OF NATIONAL SECURITY AGENCIES' HACKING CAPABILITIES

6.1 Cooperation of private companies with national security agencies

A number of recent reports, most of which are based on material that was leaked by Edward Snowden, lead to the impression that **intelligence agencies are using the state of the art of science and technology to its highest extend possible, in order to gather SIGINT data**. There are widespread accusations in the media of voluntary, proactive and secret cooperation of telecom and Internet providers with national intelligence or security agencies. It is difficult, if not impossible, to confirm these accusations based on hard evidence, since such evidence could not be identified or accessed by the authors of this study.

Representatives or spokespersons of **all organisations that were publicly accused** of being suspicious **of having secretly cooperated with the NSA** in particular, **have strongly rejected these incriminations** and nine of those companies (AOL, Apple, DropBox, Facebook, Google, LinkedIn, MicroSoft, Twitter, Yahoo) have published a letter to the US Senate[152] in which they demand a Global Government Surveillance Reform.

The US Department of Justice has issued a statement on 27 January 2014[153] which announces new reporting methods for national security orders and **implicitly admits that corresponding requests of information disclosure to communication providers are being or have been issued**. This leads to the conclusion that

> Although the cooperation between large communication and service providers and the NSA may not have occurred on a voluntary basis, data has been made accessible by these companies to the NSA on the basis of lawful requests, or under the threat of fines.

Court documents unsealed in September 2014 confirm that "*the U.S. government threatened to fine Yahoo US$250,000 a day in 2008 if it failed to comply with a broad demand to hand over user communications*".[154] It is also known that a large number of requests for information disclosure have been and are being issued by **the US Foreign Intelligence Surveillance Court (FISA)**. This court **has been criticized for its lack of oversight and public control mechanisms** and, according to information published by the Electronic Privacy Information Center[155], has only rejected 11 out of 33949 warrant requests for electronic surveillance in the period from 1970 to 2012.

6.2 Hacking capabilities of national security agencies

The NSA elite cryptanalytic unit, the Office of Cryptanalysis and Exploitation Services (S31), a subdivision the Office of Tailored Access Operations (TAO), is composed of more than 1,500 cryptanalysts, mathematicians, scientists, engineers, and computer technicians who "*have had a remarkably large number of code-breaking successes against foreign targets*". These achievements "*were largely dependent on clandestine intelligence activities […] and not the more traditional cryptanalytic attacks on encrypted messages*". NSA's cryptanalytic unit was largely unsuccessful trying to "*crack the encryption*

[152] https://www.reformgovernmentsurveillance.com/
[153] http://www.justice.gov/opa/pr/joint-statement-attorney-general-eric-holder-and-director-national-intelligence-james-clapper
[154] https://cdt.org/insight/yahoo-v-u-s-prism-documents/
[155] http://epic.org/privacy/wiretap/stats/fisa_stats.html

protection used by the anonymizing service Tor", or files encrypted with PGP. [156],[157]. But recent reports on advances in LEAs efforts of compromising the TOR network and shutting down illegal websites in the deep web[158,159], puts this statement into a new perspective. It seems that the TOR network has lost its status of being a safe heaven for anonymous internet communication.

> The difficulties encountered for decrypting protections by brute force attacks has led the NSA to resort to clandestine techniques. For this purpose, the NSA employs an extensive set of tools[160] to covertly infiltrate computer networks and set up backdoors that allow them to take control over these networks and access and copy information *before* it is encrypted.

According to a report on the NSA tool Treasuremap[161], the Deutsche Telekom (along with another telecom provider), which in Germany alone provides 60 million customers with mobile, Internet and fixed lines, are marked on a network diagram showing "*SIGINT collection points*", i.e. an access point for cyber spies in their network. The classified presentation indicates that there exist "*13 covered servers in unwitting data centres in 16 countries worldwide*".

But obviously not only the USA maintains such kind of cyber-espionage programs. Namely

> The UK, Canada Australia and New Zealand, as members of the FiveEyes (FVEY) intelligence alliance; China, Russia, Israel, Iran[162], Pakistan, but also EU member countries like Germany, France and Italy, among others, have been reported to run government-sponsored cyber-espionage units or programs.

A recently leaked document on the customers of FinFisher, a cyber-espionage application, adds even more countries to this list. [163]

The question remains on how such secret cyber-espionage and hacking programs can be kept alive without being subject to leaks. The Snowden case – among other whistle-blower cases of lesser media coverage – shows that such leaks cannot be completely avoided. But the different national intelligence agencies do of course establish various means for preventing such leaks to happen.

To start with, the NSA requires all employees to sign a Classified Information Nondisclosure Agreement[164] and although no information is available on the respective practices in other national security agencies, it can be safely assumed that their employees must abide to similar NDAs.

Secondly, security agencies, like any other military or national defence organization, are organized in a strictly hierarchical structure in which the information is compartmented, such that **only very few unique persons (if at all) do have a total oversight of all activities**. This means that even if a specialist is working on a critical issue (e.g. related to surveillance) she may not be able to draw the connection to related actions and get the "big picture" of what she is contributing to ("[…] *in many of our foreign partners' capitals few senior Officials outside of their defence-intelligence apparatuses are witting to*

[156] http://www.foreignpolicy.com/articles/2013/10/15/the_nsa_s_new_codebreakers
[157] The part of the statement referring to TOR may have to be re-assessed based on the information concerning operation "Onymous". See also Section 6.5
[158] https://blog.torproject.org/blog/possible-upcoming-attempts-disable-tor-network
[159] https://blog.torproject.org/blog/thoughts-and-concerns-about-operation-onymous
[160] https://www.eff.org/files/2014/01/06/20131230-appelbaum-nsa_ant_catalog.pdf
[161] https://firstlook.org/theintercept/document/2014/09/14/treasure-map-presentation/
[162] http://www.cylance.com/operation-cleaver/
[163] https://wikileaks.org/spyfiles4/customers.html
[164] http://www.archives.gov/isoo/security-forms/sf312.pdf

any SIGINT connection to the U.S./NSA")[165]. This makes it much more difficult for an individual to gather sufficient information or insight in complex programs and therefore reduces the risk of someone becoming suspicious and/or being able to leak relevant and connected information.

Another influencing factor that prevents security relevant information to be leaked is the public opinion, or stance, in some countries. While, for instance, the public opinion in many European countries and Canada tends toward defending the whistleblowing of Edward Snowden, the US American society's opinion is split. This may be related to **different perceptions of societal values and principles in different nations**. The comment of the Director of the NSA on the priority of civil rights or security on NSA's website potentially helps to understand this argument[166].

6.3 Efficiency of intelligence services surveillance programs

The strategies applied by national security agencies for achieving the objective of gathering SIGINT data can be classified in 4 categories:

- Network intrusion (hacking)
- Infection of devices with secret backdoors (troyans, keylogger, etc.)
- Physical modification of hardware components
- Weakening, or breaking, publicly trusted encryption standards

6.3.1 Network intrusion

The advantages of hacking large network routers ("*such as CISCOs / Junipers / Huaweis*"[167]), include the possibility to

- add credentials, allowing a third party to log in anytime
- add/change routing rules (e.g. detour traffic to servers controlled by third parties)
- setup a packet capture capability (e.g. for "sniffing" credentials)
- weaken any VPN encryption capabilities on the router, forcing it to create tunnels that can easily be decrypted
- install a modified version of the Operating System with whatever pre-built-in functionality

When engineers of Stellar PCS, a German Satellite Communications Provider that provides Internet access to remote portions of the globe via satellite, were confronted with the contents of a leaked document on GCHQ's Treasuremap[168] application that showed the level of infiltration of the GCHQ into their network (including access passwords of other providers who rented Stellar PCS's infrastructure), the system administrator of Stellar PCS said that **with this access level the GCHQ would be able to change links, geo-locate users, or** "[…] ***shut down the Internet in entire African countries*** *that are provided access via our satellite connections*". [169]

6.3.2 Infection of devices with secret backdoors

The ANT catalogue[170] of NSA's Tailored Access Operations (TAO) group, lists a number of exploits which reveal surveillance powers that go beyond root access and into the hardware of different kinds of network devices, servers and handheld devices.

[165] https://www.eff.org/files/2014/04/09/20140313-intercept-nsa_cooperative_third_party_relationships.pdf
[166] https://www.nsa.gov/about/values/core_values.shtml (ref. Q1)
[167] https://www.eff.org/files/2014/04/09/20140312-intercept-five_eyes_hacking_large_routers.pdf
[168] https://firstlook.org/theintercept/document/2014/09/14/treasure-map-presentation/
[169] https://firstlook.org/theintercept/2014/09/14/nsa-stellar/
[170] https://www.eff.org/files/2014/01/06/20131230-appelbaum-nsa_ant_catalog.pdf

The data sheets on some of these exploits (e.g. DEITYBOUNCE[171], SCHOOLMONTANA) clearly indicate that these exploits infect the BIOS of the respective devices, so that it is in no way distinguishable from normal computer activity and **can only be discovered through forensic investigation of the physical data chip**. In the case of SCHOOLMONTANA the data sheet states that "[the] *implant will survive an upgrade or replacement of the operating system – including physically replacing the router's compact flash card*."

These are only two examples of ca. 50 tools and exploits documented in the NSA catalogue, which was created in 2008.

6.3.3 Physical modification of hardware components

Although not directly ascribed by evidence to being used by security agencies today, a technique called "transistor doping" is able to alter the correct behaviour of integrated circuits by modifying the crystalline structure of transistors.

Researchers of the University of Massachusetts have shown that by manipulating the Random Number Generator (RNG) that provides "*the starting random numbers with which to create encryption keys*", they were able to change the behaviour of the chip "*so that one particular number became a constant instead of a variable. This weakens any encryption that comes from keys created by that system*"[172] and consequently facilitates decryption by third parties that don't possess the full decryption key. According to the researchers, **such a hardware modification would not be detected by the chips' self-test and be virtually impossible to be detected by users**.

IEEE Spectrum[173] reports in 2008 that the US Department of Defense (DOD) launched the "Trust in Integrated Circuits program", with the aim of verifying the integrity of the integrated circuits (IC) that form part of military systems. The main concern that justifies this program is the DODs fear that chips which "*have been purposely fabricated with a hidden "backdoor" inside*" could be integrated in their military equipment and give enemy forces the possibility to remotely control or sabotage them (e.g. by activating so called "kill-switches").

A common practice, which has purportedly been used to infiltrate the Stuxnet virus in Iranian nuclear facilities, **is that of modifying the firmware of USB flash drives** (pen drives). This technique consists in reprogramming the USB controller chip so that it can infect the host system with malicious code[174]. There is little to no protection available (except for clean-room or white-room separation of systems from external devices) for preventing attacks that employ this infection technique, since **it does not get detected by malware or antivirus scanners** and since specific USB devices cannot (yet) be blocked by firewalls. It may not even be possible to eliminate injected vulnerabilities by reinstalling the operating software, if the attack code modifies the BIOS of the affected system.

6.3.4 Weakening, or breaking, publicly trusted encryption standards

Much has been written about the effort of security agencies in gaining access to keys that would allow deciphering information encrypted by different encryption technologies. This battle goes back to the early 90s, when Phil Zimmerman, the creator of PGP, a public domain cryptology application, was subject of a criminal investigation by the US Government, accusing him of exporting munition

[171] http://resources.infosecinstitute.com/nsa-bios-backdoor-god-mode-malware-deitybounce/
[172] G. Becker, F. Regazzoni, C. Paar, W. Burleson, Stealthy Dopant-Level Hardware Trojans, University of Massachusetts, TU Delft, Ruhr-Universität Bochum
[173] http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch
[174] https://srlabs.de/badusb/

without license (Cryptosystems using keys larger than 40 bits were then considered munitions within the definition of the US export regulations[175])

More **recent information blames the NSA of having paid US$10 million to the RSA**, an American computer and network security company, **in a deal that "*promulgated a flawed formula for generating random numbers*"** in RSA's BSafe software, "*that is used to enhance security in personal computers and many other products*"[176] This flaw would facilitate cracking encryptions that have been scrambled by the "Dual Elliptic Curve Deterministic Random Bit Generator" (Dual EC DRGB) algorithm used by BSafe. The **RSA has categorically denied the allegation** of having "*entered into a "secret contract" with the NSA to incorporate a known flawed random number generator into its BSAFE encryption libraries*". The NSA did not comment on the accusations.

However, other information published by New York Times, the Guardian and ProPublica does sustain and even extend the accusation of the NSA secretly defeating Internet privacy and security[177], revealing that

- a 10-year NSA program against encryption technologies made **a breakthrough** in 2010 **which made "*vast amounts*" of data** collected through Internet cable taps **newly "*exploitable*"**.
- the NSA spends US$250 million a year on a program which, among other goals, **works with technology companies to "*covertly influence*" their product designs**.
- a GCHQ team has been working to **develop ways into encrypted traffic on the "big four" service providers**, named as Hotmail, Google, Yahoo and Facebook

A statement from the Office of the Director of National Intelligence says that "[…] *the fact that NSA's mission includes deciphering enciphered communications is not a secret, and is not news. Indeed, NSA's public website states that its mission includes leading "the U.S. Government in cryptology … in order to gain a decision advantage for the Nation and our allies"*." It also adds that the information disclosed in the referred media "*reveal specific and classified details about how we conduct this critical intelligence activity. Anything that* [these] *disclosures add to the ongoing public debate is outweighed by the road map they give to our adversaries about the specific techniques we are using to try to intercept their communications in our attempts to keep America and our allies safe and to provide our leaders with the information they need* […]"[178].

In an effort to maintain the mentioned decision advantage by means of technological advantage, the NSA is performing **a US$79.7 million research program** titled "Penetrating Hard Targets"[179] **with the objective to build a quantum computer** able to break the majority of the encryption standards on the Internet. It must however be pointed out that quantum computing today is still rather a theoretical concept than a ready-to-implement engineering solution. Experts predict that **it would take at least five more years to attain the kind of quantum computers that the NSA wants**.

The documented facts and information lead to the conclusion that

> Governmental agencies do in fact possess powerful capabilities to break system protections and to infiltrate systems and networks by applying (a mix of) state of the art technology.

Even though it is possible to hinder such unauthorized intrusions by applying different protection mechanisms, **there is no means for guaranteeing total immunity against such attacks**.

---

[175] http://en.wikipedia.org/wiki/Pretty_Good_Privacy
[176] http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220
[177] http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security
[178] http://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption
[179] http://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html?hpid=z1

6.4 Credibility of accusations on mass surveillance

Despite the rebuttal of many accusations, particularly those related to collaborations between commercial Internet companies and national security agencies, **the authors of this report were not able to identify technical rebuttals of the revealed NSA documents**, neither through revision of literature, nor through the statements of technical experts on the respective subject matter. Although **this absence of technical refutations cannot be equated to being a validated proof of credibility or technical coherence of Snowden's revelations**, it can be asserted that

> The technical feasibility of the tools and practices applied by national security agencies is not disputed by any of the relevant technical communities.

The statements that can be found in some of the original leaked documents directly contribute to confirm the global coherence and consistency of the published accusations. So does a slide from the fund of Snowden documents that presents the "New Collection Posture" of the NSA with the six bullet points "*sniff it all, know it all, collect it all, process it all, exploit it all and partner it all*"[180]. This can only be interpreted as the NSA having "*explicitly embraced* [General Keith B.] *Alexander's*[181] *motto of omniscience as its core purpose*"[182].

The reports on indiscriminate collection of private information on the web, **which have neither been denied nor admitted by the NSA**, do substantiate the validity of the allegations published by the media in relation with the Snowden documents: "*nine of 10 account holders found in a large cache of intercepted conversations* […] *were not the intended surveillance targets but were caught in a net the agency had cast for somebody else*".[183]

6.5 Efficiency of solutions to fight mass surveillance

The security solutions on the market available for users to protect themselves against any type of surveillance fall basically into five categories:

- antivirus programs
- firewalls
- VPNs
- encryption tools
- anonymizing services and tools

Antivirus programs do provide a good level of protection for known malware, viruses, Trojans and even malicious URLs, spam, or rootkits. They do apply different strategies for detecting (and eventually disinfecting) malicious software, which are based on the identification of signatures (or patterns), or on heuristic methods.

A **firewall** is either a software application or a hardware appliance that can block in- and outgoing network traffic on a device, based on defined rules and depending on the communication ports and/or protocols used.

---

[180] https://edwardsnowden.com/wp-content/uploads/2014/05/newcollectionposture.pdf

[181] Four-star General Keith Brian Alexander was the Director of NSA from 2005 to 2013. He also held the position of Chief of the Central Security Service (since 2005) and Commander of the United States Cyber Command (since 2010)

[182] Greenwald, G.: No Place to Hide: Edward Snowden, the NSA, and the U. S. Surveillance State, Metropolitan Books, New York (2014)

[183] http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html

A **Virtual Private Network (VPN)** is a private network that makes use of public network structures, requiring authenticated access and employing different security and encryption techniques, in order to guarantee the privacy of data exchanged between two endpoints.

Encryption tools are software applications that encrypt and decrypt data or communication channels, applying different algorithms and cipher suites.

Anonymizing services and tools are proxies that provide anonymity and privacy for users when accessing servers in the Internet. This is achieved by obscuring the client's IP address and the "path" that was taken for accessing a server. This makes it impossible for third parties to gather information about which servers a user is accessing and for the accessed server to gather the IP address of the client accessing it.

> All of these security solutions have their particular weaknesses that could allow attackers to break their protection.

Antivirus programs may fail when it comes to zero-day-attacks. If such a zero-day-attack makes use of new techniques (or signatures/patterns) that are not covered by the knowledge base of the antivirus application, it may not be detected.

Firewalls can be bypassed by applying different types of attack (e.g. MITM, DNS spoofing, DDoS, Rootkits, etc.). VPNs also can be compromised in various ways[184] and are subject to attacks that "*take advantage of misconfigurations and poorly managed implementations*"[185].

Encryption, which **appears to be one of the strongest means to protect from privacy violations**, is only as good as the algorithms and cipher sets used. Despite the fact that encryptions employing keys of 1024bits or longer are theoretically impossible to decipher with today's available computing power, a number of recent reports suggest that some **security agencies have made significant progress in cracking certain types of encryption** so that "*vast amounts of encrypted Internet data which have up till now been discarded are now exploitable*"[186].

The TOR network, an anonymizing service, **was only recently compromised in a joint operation of international LEAs – labelled operation "Onymous"** - that targeted illegal websites which are only accessible through the TOR network[187]. Information concerning this and other attempts of intelligence, security and LEAs to weaken or break the anonymizing service provided by TOR suggest that the network cannot be trusted anymore.

The ability of a user to effectively own and administrate private data furthermore conflicts with the use of cloud services. In this case the data will be entirely submitted to the policies and mechanisms of the cloud provider. Some providers provide back-end services for encrypting data (which could also be prone to weak encryption algorithms or keys), while others leave encryption to the responsibility of the user (which reduces the risk of the provider being able to decrypt this data). Also **a variety of meta-data can be acquired from the user activity in the Cloud**, since data manipulation (for example, growing in size), sharing, and uploading/downloading can be analysed to determine certain behaviour patterns.

It can therefore be concluded that

> The application of a combination of the above described security and privacy solutions does provide an advanced level of protection from mass surveillance

[184] http://www.nta-monitor.com/files/whitepapers/VPN-Flaws-Whitepaper.pdf
[185] https://www.ncp-e.com/fileadmin/pdf/techpapers/NCP-Attack-Vectors-WP.pdf
[186] http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security
[187] http://www.theguardian.com/technology/2014/nov/11/operation-onymous-flaws-tor

practices. End-to-end encryption of communication channels and content does constitute a *theoretically* unbreakable security mechanism. But even if applied in combination, these solutions cannot guarantee total immunity against complex attacks.

In a final note it should be mentioned that **the use of encryption may have an antagonizing effect**: Encrypted communication is particularly attracting the interest of government agencies. As an article on the EFF website puts it "[…] ***the NSA is allowed to hold onto communications solely because you use encryption***. *Whether the communication is domestic or foreign, the NSA will hang on to the encrypted message forever, or at least until it is decrypted. And then at least five more years*"[188]

6.6 Threats and opportunities of using foreign OS and applications in public administration

The major advantages of using commercial software and equipment are related to the fact that they are thoroughly tested for their operation, are being continuously updated and that their supplier is liable for potential consequences of malfunctions, errors and bugs. In the case of some OS and applications (suites), their vast deployment has led to a "de facto standard", which is even further leveraged through agreements with hardware manufacturers. Millions of users, including large parts of public administration worldwide, are using Microsoft Windows and Microsoft Office in their daily work. Interoperability issues with alternative OS and applications, for instance in the Open Source software market, along with the costs of migration are the primary reasons for many organisations to stick with the status quo.

One of the biggest concerns when using commercial software and equipment is their "black-box" character (i.e. their internal functioning is unknown to the user) and the potential security issues that may derive from it. Open Source software does eliminate this concern through the openness of its code, which allows for constant inspection and scrutiny by a large community of experts. **This does, however, not guarantee that Open Source software is error free (or less prone to errors than commercial software)**. The "Heartbleed" bug in the OpenSSL protocol implementation, which is deployed in millions of servers worldwide, had remained for years in the source code before it was detected and fixed[189]. This means that

While the level of confidence in adequate security levels of commercial software and equipment is based on trusting the provider, in the case of Open Source software and equipment this confidence can be built on a user's own inspection and scrutiny.

An example of an administration having migrated their IT infrastructure to Open Source is the German city of Munich. The goal of this migration was clearly to achieve more autonomy from providers and lower IT-costs were merely a "*welcome side-effect*". Their experience show that such a migration "*requires careful analysis and planning, as well as a clearly defined goal*". A lot of testing was required before introducing new tools, so as to ensure that the operation of the administration did not get interrupted. They also state that the "*lack of acceptance and outright resistance* [of the involved staff] *can be more substantial obstacles to the deployment of a software solution than any technical problem*".[190]

[188] https://www.eff.org/deeplinks/2013/06/depth-review-new-nsa-documents-expose-how-americans-can-be-spied-without-warrant
[189] http://heartbleed.com/
[190] https://joinup.ec.europa.eu/elibrary/case/declaration-independence-limux-project-munich-0

Some experts claim that it is impossible to guarantee security and privacy while using Windows OS, since the US administration's close ties to Microsoft as an American company will always give them a competitive edge over other countries when it comes to exploiting vulnerabilities in the OS code. **This does NOT imply that backdoors are built in purposefully, but that the perpetual pipeline of zero day vulnerabilities caused by (unintended) software flaws opens way for backdoors**. The crucial question is therefore who has knowledge of such zero day vulnerabilities (and the potential to exploit them) for how long before they become public.

Initiatives like the Qube-OS project[191] try to address this issue by developing Open Source Operating Systems that are designed to provide strong security, which in the case of Qube OS is achieved by applying a "**Security by Compartmentalization"** approach.

Another critique voiced by security and privacy advocates is that Europe does too little to encourage the development of security and privacy related tools and that the available funding instruments (i.e. H2020) insist in that such applications need to be cross-platform, which in itself is an "incongruent idea". The information exposed in this document makes very clear that

> Achievable levels of security and privacy are very much depending on the *specific* platforms and technologies used and security and privacy issues must therefore be addressed in a platform-specific way.

[191] https://qubes-os.org/

7 TECHNICAL AND POLICY OPTIONS PROPOSED FOR MITIGATING THE IDENTIFIED RISKS

7.1 Best practices for preventing cryptography problems

Cryptography problems have been outlined in Chapter 4 and can be summarised by the four major weaknesses or attack strategies:

1. Obtaining "encryption keys" through adequate intelligence operation on one of the two end-points.
2. Exploiting security vulnerabilities (backdoors, side channel attacks, bugs, viruses, APT, BotNets, etc.) in the set-up of one or both of the "end-points".
3. Exploiting weaknesses (bugs, software design flaws and backdoors) in the encryption programme to enable decrypting the information without the need of possessing the original encryption key(s) from one of the end-points.
4. Zero-day attacks

The following **safeguarding practices** are recommended as measures **for preventing the four major security problems related to cryptography**:

1. It is recommended to **generate strong encryption keys** (both symmetric and asymmetric ones) in order to **make it as difficult as possible for attackers to derive these keys from related information** (e.g. birthdate, license plate, etc.) by employing social engineering attacks. These keys should be:
   - Long (**>8 characters**) and generated by **using a mix of alphanumeric and special symbols**.
   - Random numbers
   - Dynamic (i.e. keys should be renewed periodically)

   Table 1 shows the relation between the length of a password (i.e. number of characters) and the average effort needed to break it.

Number of characters in Password	Average days needed to crack password
10	5
11	306
12	18.976,5
13	1.176.549
14	72.946.048

Table 1: Relation between password length and effort for cracking it (source theWire[192])

   PGP tools[193] make this possible by using a public/private encryption infrastructure. PGP's public/private key generator allows creating strong encryption keys that ensure high confidentiality and integrity factors.

2. The problem of exploiting vulnerabilities is **addressed by *security by default* and *security by design* paradigms**. The first one refers to **using the most secure configuration of software programs as default** (which is not necessarily the most user-friendly, or performance-effective one, but often the best option to avoid backdoors); the second refers to the engineering phase of a particular software product and the consideration of security requirements from its early stages.

[192] http://www.thewire.com/technology/2012/08/advice-hacker-password-security-best-practices/56343/
[193] http://www.openpgp.org/

Both paradigms help to avoid vulnerabilities in the engineering and operation phases, but **need a validation or certification scheme** which guarantees that IT products do not contain any known security vulnerabilities.

3. The problem of cryptography weaknesses cannot be prevented by end users, but needs to be addressed by the vendors of cryptographic software. Their **implementations of encryption standards need to be verified, validated and certified** in order to avoid unfixed protocol vulnerabilities in the different versions of the implementation of the protocols and interoperability problems caused by different implementations (from a functional and non-functional point of view).
4. The protection against zero-day attacks is practically impossible to achieve for end users. However, there are a number of **recommended steps that** help to **reduce the impact of a potential attack** which should be particularly applied in corporate environments:
   - **Prevention**
     Users should apply security best practices which include the **installation of firewalls and other perimeter security devices** and **keeping operative systems, applications and particularly antivirus tools updated at any time**. Furthermore, it is a good practice to regularly execute security audits on the systems, in order to detect software vulnerabilities as early as possible.
   - **Real time monitoring and protection**
     A number of tools like **Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS)**, security monitoring tools, etc. are available that either prevent from, or alert of malware infection. The deployment and usage of these tools helps in reducing the impact of malware and virus infections by allowing devising early solutions in form of patches and updates.
   - **Planned incident response**
     When a company is affected by a zero day attack it is crucial to have **appropriate incident response procedures** implemented, including roles and responsibilities, to minimize damage and business disruption.
   - **Preventing the spread**
     Spread prevention basically consists in **isolating networks** and opening only those that are necessary for the continuity of the business

7.2 Technical options for mitigating surveillance risk

There are a number of technical options available to citizens for counteracting mass surveillance, first and above all, encryption, a statement that is shared and confirmed by the security community and Edward Snowden, who says that

> *"Properly implemented strong crypto systems are one of the few things that you can rely on."*[194]

The following sections list a (non-exclusive, unordered and not prioritized) number of tools and applications that can be used by citizens to defend the privacy of their online communications and data.

[194] http://www.guardian.co.uk/world/2013/jun/17/edward-snowden-nsa-files-whistleblower

7.2.1 Encryption of data at rest (stored data)

Hard drive encryption on PCs: The technique consists in either encrypting entire partitions of a hard drive, or only individual files stored in a partition. Examples of tools that allow doing so are the following:

- **DiskCryptor**[195]: DiskCryptor is an open-source encryption solution for Microsoft Windows that offers encryption of the entire computer hard drive or individual disk partitions (including the system partition), or external storage devices (USB, DVD disks, etc.). DiskCryptor provides a broad choice in configuration of booting an encrypted operating system (OS). It uses AES-256, Twofish, and Serpent, or combinations thereof to carry out encryption.
- **TrueCrypt**, is a free and open-source program which was very popular, but has been **discontinued** in May 2014. TrueCrypt supported Microsoft Windows, OS X and Linux, and allowed on-the-fly encryption of individual files, entire hard drives, entire partitions, or storage devices such as a USB flash drives or external hard drives. To this aim three different algorithms were available: AES, Serpent, and Twofish, and five different cascaded combinations of them. There are two forks of the original source code that claim to have taken over the development of the future TrueCrypt: https://truecrypt.ch/ (TCnext) and https://ciphershed.org/.
- **FileVault**[196]: Is an Apple Macintosh built-in encryption system that is installed on most recent Mac computers. The current FileVault 2, which works with OS X Lion or later, uses full disk, XTS-AES 128 encryption to allow on-the-fly encryption (real time, i.e. as data are stored) of the contents of the entire drive. FileVault 2 requires that OS X Recovery is installed on the boot drive.
- **BitLocker**[197]: Is a Microsoft built-in encryption system that works in Ultimate and Enterprise editions of Windows 7 and Pro and Enterprise editions of Windows 8.1. BitLocker allows to encrypt entire drives.
- **PGP**[198] is an encryption application that was first developed by Phil Zimmerman in 1991 and has evolved under different owner companies. In 2010 PGP has been acquired by Symantec and is now only available through this company. However, an implementation of openPGP is available as freeware from the GnuPG[199] website.

Encryption of a smartphone's hard drive: Apple doesn't let users encrypt their smart phone's hard drive or the files on it, though the operating system (< iOS 8) will encrypt passwords and some other files if a passcode is used on the device. Apple will also let users encrypt their phone's backup files on iTunes or iCloud. It is also possible to use Find my iPhone to remotely "wipe," or delete the data on an iPhone or iPad if it is lost or stolen. With the rollout of iOS 8 all data on the phone is encrypted by default. Google's Android operating system lets users encrypt their phone hard drive.

Encryption of data in the cloud: These technologies enable data to be stored encrypted in the cloud, using an encryption key that is owned by the data owner and usually stored on the hard drive of the device accessing the cloud. All files are safely encrypted on the user's device before being transferred to the cloud.

The cloud storage services SpiderOak[200], Wuala[201], BoxCryptor[202] , Cloudfogger[203], Seafile[204] (open source), SparkleShare[205] (open source), and Pydio[206] (open source) are examples of such technologies.

[195] https://diskcryptor.net/wiki/Main_Page
[196] http://support.apple.com/en-us/HT4790
[197] http://windows.microsoft.com/en-us/windows7/products/features/bitlocker
[198] http://www.symantec.com/products-solutions/families/?fid=encryption
[199] https://gnupg.org/
[200] https://spideroak.com/
[201] https://www.wuala.com/

The mechanism used differs from the current widely used Dropbox[207] approach which does use encryption (256-bit AES algorithm) for storing user data, but the data is not encrypted locally and the encryption key of the data stored in the cloud is not owned, nor known by the user, only by Dropbox.

The drawback of the user storing the encryption key is that she needs to be in control of the security of such key, because in case the key is compromised or lost, the data could not be recovered.

7.2.2 Encryption of data in transfer

- **HTTPS Everywhere[208]**: This software is the result of collaboration between The Tor Project and the Electronic Frontier Foundation. HTTPS Everywhere is an add-on for Mozilla Firefox, Google Chrome, and Opera that encrypts communications with many major websites, allowing private browsing. The software helps in the definition of HTTPS rule-sets to define which domains are redirected to HTTPS and how. The enhancement over HTTPS is marketed as: "*Many sites on the web offer some limited support for encryption over HTTPS, but make it difficult to use. For instance, they may default to unencrypted HTTP, or fill encrypted pages with links that go back to the unencrypted site. The HTTPS Everywhere extension fixes these problems by using a clever technology to rewrite requests to these sites to HTTPS*." Note that **not all websites are able to work with HTTPS Everywhere**, although an increasing number does.

7.2.3 Protection for email services

- **Prism-proof email (PPE) protocol**[209]: PPE by IETF enables encrypted email conversations based on PKI. The preferred cipher set is RSA-2048, AES-256 and SHA-2-512. PPE *puts every individual in charge of their own personal PKI hierarchy. The root of this hierarchy is a personal master key that does not expire until it is either replaced by a new root key or the holder dies.* Therefore, the user of PPE does not need to rely on Trusted Third Parties. Currently PPE does only support Live Mail but support for more webmail services is expected in the future.
- **Bitmessage**[210]: is a protocol for trustless decentralized peer-to-peer encrypted communications. *It encrypts messages, masks the sender and receiver of messages from others, and guarantees that the sender of a message cannot be spoofed, without relying on trust and without burdening the user with the details of key management*[211].
- **Sendinc**[212]: is free a web-based encryption email service for end-to-end encryption. Sendinc uses 256-bit SSL encryption code and works with any email client, and from any web-enabled device.
- **Enigmail**[213]: is a data encryption and decryption extension for Mozilla Thunderbird and the SeaMonkey Internet suite. It enables writing and receiving email messages signed and encrypted with the OpenPGP standard. Enigmail works under Microsoft Windows, Unix-like, and Mac OS X operating systems.

---

202 https://www.boxcryptor.com/
203 http://www.cloudfogger.com/en/
204 http://seafile.com/en/home/
205 http://sparkleshare.org/
206 https://pyd.io/
207 https://www.dropbox.com/
208 https://www.eff.org/https-everywhere
209 http://prismproof.org/index.html
210 https://bitmessage.org/wiki/Main_Page
211 https://bitmessage.org/bitmessage.pdf
212 https://www.sendinc.com/
213 https://enigmail.net/home/index.php

- **Mailvelope**[214]: is a browser add-on for Google Chrome and Firefox that offers encrypted email communication based on OpenPGP. It can be configured to work with nearly any web mail provider, e.g. Gmail, Yahoo, Outlook and GMX.
- **Gnu Privacy Guard**[215] protocol: *GnuPG is a complete and free implementation of the OpenPGP standard as defined by RFC4880 (also known as PGP).* GnuPG allows encrypting email conversations provided both ends use it, similarly to OTR protocol.
- **StartMail**[216]: StartMail offers easy-to-use PGP encryption and TLS based secure email exchange.
- **GPG Tools**[217]: GPG Suite is a free software tool suite that includes GPG Mail and GPG key management among other features. GPG Mail is an open source plugin for Apple's built-in Mail program that allows encryption features (encrypt, decrypt, sign and verify mails) based on OpenPGP.

7.2.4 Protection for Voice (and Video) Communication

- **Cellcrypt**[218]**:** Cellcrypt is an application that provides full end-to-end encryption for cell phones running Android, iOS, or Blackberry OS. It supports networks from GSM/GPRS to 4G, as well as private and public Wi-Fi and satellite networks. Cellcrypt needs to be installed on all the devices involved in a connection, in order to be able to establish an encrypted communication channel.

- **Celltrust**[219]: The CellTrust Mobile Collaboration Suite is only available as an enterprise level application for Android and iOS cell phones. It provides full end-to end encryption on Wi-Fi, 3G, 4G and LTE networks through a mobile business number that separates corporate and personal communication. The CellTrust Mobile Collaboration Suite includes features for SMS accountability and traceability, SMS and voice storage and recording services, as well as voice communication tracking and tracing mechanisms, which, despite being designed for enabling corporate control and oversight, could be misused - at corporate level – for monitoring employees.

- **OSTN**[220]**:** *OStel is a public test-bed of the Open Secure Telephony Network (OSTN) project, an effort with the goal of promoting the use of free, open protocols, standards and software, to power end-to-end secure voice communications on mobile devices, as well as with desktop computers.* OSTN clients are available for all desktop and cell phone OS and supports all mobile networks from GSM to 4G/LTE and Wi-Fi, but does not support encrypted calls to the landline.

- **Omnisec**[221]**:** Omnisec, a Swiss based information and communication security Company, is offering a Secure Mobile Solution that is based on an off-the-shelf Samsung Galaxy S2 with hardened Android Operating System. This system provides a "*safe, worldwide-applicable all-IP encryption system, enabling absolutely secure voice communication and text messaging for all classification levels up to Top Secret*" on all networks, but only between Secure Mobile Phone Omnisec 230 devices.

[214] https://www.mailvelope.com/
[215] https://www.gnupg.org/
[216] https://live.startmail.com/
[217] https://gpgtools.org/
[218] http://cellcrypt.com/
[219] http://www.celltrust.com/
[220] https://ostel.co/
[221] http://www.omnisec.ch

- **Seecrypt**[222]**:** Seecrypt, a company headquartered in South Africa, offers a subscription service for Android, iOS, Blackberry, or Windows powered cell phones, that allows to establish encrypted voice communication over IP. This means that a cell phone needs to be connected to the Internet for the service to work.

- **SilentPhone**[223]**:** SilentPhone is a subscription service of SilentCircle, a Swiss based security company founded, amongst others, by Phil Zimmerman, the inventor of PGP and Jon Callas, creator of Apple's Whole Disk Encryption. SilentPhone enables Android and iOS devices to establish end-to-end encrypted voice and text communications between two subscribed devices worldwide. It also provides outbound calls to non-members, including landlines in a number of countries.

- **Redphone**[224]**:** Redphone is an Open Source application for Android devices that provides encrypted voice communication and data storage.

- **Jitsi**[225]**:** Jitsi is an Open Source multi-platform for video-conferencing and messaging, that "*supports some of the most popular instant messaging and telephony protocols such as Facebook, Google Talk, AIM, ICQ, MSN, Yahoo! Messenger.*"

- **Tox**[226]**:** Is a distributed Open Source video-conferencing and messaging application under development. Currently only development versions of the source code are available for compilation.

7.2.5 Protection for Web browsing

- **TOR**[227]: is free software for Windows, Mac OS X, Linux/Unix, and Android together with an open network that helps protecting the confidentiality of the communications by making it difficult to do traffic analysis. TOR establishes a network of virtual tunnels (encrypted connections) between source and destination that is incrementally built. *Instead of taking a direct route from source to destination, data packets on the Tor network take a random pathway through several relays that cover your tracks so no observer at any single point can tell where the data came from or where it's going. Tor only works for TCP streams and can be used by any application with SOCKS support.*

  There are a significant number of tools that do exploit TOR system capabilities and network, for example **Tails**[228] free open-source operating system, and other tools explained in the sections below.

  It must be noted that very recent successes of security, intelligence and LEAs in breaking the anonymisation provided by the network have put the reliability of this service in serious doubt[229].

- **I2P**[230]: is an anonymous overlay network similar to TOR, although working with a different architecture. It allows users to anonymously browse the web, chat, send emails and transfer files.

- **Tunnelling or VPN services:** Technology to create Virtual Private Network (VPN) connections allows private networks to be extended over public networks, such as the Internet. The VPN

[222] https://www.seecrypt.com/
[223] https://silentcircle.com
[224] https://whispersystems.org/
[225] https://jitsi.org/
[226] https://tox.im/
[227] https://www.torproject.org/
[228] https://tails.boum.org/
[229] https://blog.torproject.org/blog/thoughts-and-concerns-about-operation-onymous
[230] https://geti2p.net

services prevent users IP-addresses from being visible to third parties. There are a multitude of VPN service providers and prices. Detailed information on collections and ranking of such services is also available in the Web (see for example [231] and [232]). The risk is that **not all VPN services used today are as anonymous as they claim**; some of them do log network traffic which might reveal users IP-addresses and other data. Torrentfreak reports on the logging policies of VPN services[233].

- **Do Not Track**[234]: The Tracking Preference Expression or commonly known Do Not Track (DNT) is a working draft standard by W3C. DNT is a HTTP mechanism that allows the website visitors inform the websites of their preferences regarding tracking. Most major web browsers (Mozilla Firefox, Safari, Internet Explorer, Chrome and Opera) have the mechanism in place and the user only needs to turn it on to enable the allow/do not allow tracking signal be sent in the HTTP headers. Nevertheless, due to its voluntary character, most websites do not honor the method and disregard the signal or they do honor it but misinterpret the preferences[235]. In consequence, **the method has so far been unsuccessful**.
- **Blur**[236]: Formerly named DoNotTrackMe, Blur is a product that among other features (such as encrypted passwords, masked emails, masked cards and auto-filling) supports tracker blocking on web browsing activity. Blur is available as add-on versions for the Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, and Apple Safari browsers. It offers also integrated mobile experience for Android and iPhone.
- **Disconnect**[237]: is an open-source software that lets the user visualize and block the websites that invisibly track the user personal information. Disconnect is available for Chrome, Firefox, Safari and Opera web browsers and the mobile version as DisconnectMobile for Android. Disconnect needs permission to create a virtual private network (VPN) connection to enable the user disabling tracking by third parties and lets him/her mask the IP address and the location of the VPN servers, in order to browse privately. The program can also anonymize search queries in the search engine of choice by blocking identifying Cookies.
- **NoScript**[238]: is a free and open source add-on for Firefox, SeaMonster and other Mozilla-based browsers. The add-on gives users the power to specify the sites they trust and only those trusted websites will be allowed to execute active content like JavaScript, Java, Flash and other plugins. NoScript is therefore a powerful protection against cross-site scripting attacks and clickjacking attacks.
- **Orweb**[239]: is a free private browser for Android. It uses TOR to evade tracking and circumvent network restrictions. The application offers a flexible Cookie control, so that users can hide information on which device is being used and block Flash code from being executed. Orweb requires the free Orbot plugin being installed too.

[231] http://www.top10bestvpn.com/?kw=anonymous%20vpn&c=49593689771&t=search&p=&m=e&adpos=1t2&Dev=c&devmod=&mobval=0&a=1031&gclid=CJifhKacjMICFXDItAodT3EAXQ

[232] http://www.abine.com/blog/2013/vpn-that-protects-your-privacy/

[233] https://torrentfreak.com/which-vpn-services-take-your-anonymity-seriously-2014-edition-140315/

[234] http://www.w3.org/TR/tracking-dnt/

[235] http://www.computerworld.com.au/article/545777/_do_track_oh_what_heck_go_ahead/

[236] https://dnt.abine.com

[237] https://disconnect.me/

[238] http://noscript.net/

[239] https://play.google.com/store/apps/details?id=info.guardianproject.browser&hl=en

- **Onion Browser**[240]: This application allows iOS users to access the TOR network, encrypting their communications and hiding their IP addresses.

7.2.6 Protection for Chat

- **TorChat** *is a decentralized anonymous instant messenger that uses TOR hidden services as its underlying Network, in other words it communicates over the TOR network through the .onion URL protocol*[241]. The use of TorChat provides end-to-end encryption for secure text messaging and file transfers. TorChat versions run on Windows, Linux and both iPhone and Android smart phones. TorChat for Mac users is still in beta version. The program is free open source and is available in GitHub[242].
- **Off-the-Record Messaging**[243] (OTR) protocol serves to encrypt instant messaging conversations over the instant-messaging service of choice, such as gChat or AIM. Both ends in the conversation need to install a software client that supports the OTR protocol, create the keys and then verify each other's encryption keys (in order to avoid man in the middle attacks[244]). OTR uses a combination of the Diffie–Hellman key exchange with 1536 bits group size, the AES 128 and the SHA-1 hash function. Some of the implementations include:
    - **Pidgin**[245]: is free and open source software that runs on Windows, Linux, and other UNIX operating systems and supports multiple chat networks such as AIM, ICQ, Google Talk, Jabber/XMPP, MSN Messenger, Yahoo!, Bonjour, Gadu-Gadu, IRC, Novell GroupWise Messenger, Lotus Sametime, SILC, SIMPLE, MXit, and Zephyr.
    - **Adium**[246]: is free and open source software for Mac OS X that supports AIM, MSN, XMPP (Jabber), Yahoo, and more.
    - **MirOTR**[247]: is a plugin for allowing OTR over the Miranda[248] open-source Instant Messaging service.
    - **Cryptocat**[249]**:** This popular and easy-to-use open source software allows instant set up of encrypted chats based on OTR protocol. Cryptocat versions run in Chrome, Firefox, Safari, Opera, OS X and iPhone platforms.
    - **Jitsi**[250]: a free and open source multiplatform for VoIP, videoconferencing and instant messaging that runs with Windows, Linux and Mac OS X. It supports AIM, ICQ, Google Talk, MSN Messenger, Yahoo!, SIP, and XMPP (Jabber).
    - An **OTR library in C#** licensed under The Code Project Open License (CPOL) is available for Windows, Linux and Android platforms[251].

[240] https://itunes.apple.com/us/app/onion-browser/id519296448?mt=8
[241] http://www.deepdotweb.com/jolly-rogers-security-guide-for-beginners/tor-chat/
[242] https://github.com/prof7bit/TorChat
[243] https://otr.cypherpunks.ca/
[244] https://freedom.press/encryption-works#otr
[245] https://pidgin.im/
[246] https://www.adium.im/
[247] http://code.google.com/p/mirotr/
[248] http://www.miranda-im.org/
[249] https://crypto.cat/
[250] https://jitsi.org/
[251] http://www.codeproject.com/Articles/644318/Off-The-Record-OTR-Security-Protocol

7.2.7 Protection for Web searches

- **DuckDuckGo**[252]: is a popular search engine that does not collect personal information of its users, and therefore all the users are served the same search results for a given search term.
- **Ixquick**[253]: is a metasearch engine that encrypts all searches and claims that it does not record the user's IP address, nor share any personal user information with any third party search engine or with the provider of its sponsored results[254]. *It does, however, collect and store "limited" user information – the date and time of a search, as well as the browser and platform used for the search*[255].
- **Startpage**[256]: is a search page offered by Ixquick that provides Google search results combined with the privacy policy of Ixquick. *Like DuckDuckGo, Startpage doesn't use Cookies, it immediately discards IP addresses, and it doesn't keep a record of searches performed*[257]. Startpage removes from each search query all identifiable information about the searcher, and submits the query to Google search engine. This way, Google cannot trace back the query to the searcher, only to Startpage servers.
- **Blekko**[258]: search engine is also privacy-conscious. *Blekko does log personally identifiable information, but deletes it within 48 hours. In contrast, Google stores this information for 9 months – and then anonymizes it without actually deleting it*.
- **Ask**[259]: The Ask search engine provides a feature setting "AskEraser" which allows the user to indicate search preferences and enforce that Cookies are deleted and only a single cookie is left (indicating that AskEraser is enabled). When AskEraser is enabled, the search activity will be deleted from Ask.com servers (not from third parties). The search history will be logged if a critical error occurs (until recovery) or under a law enforcement request.

7.2.8 Privacy aware Operating System

It is recommended that users install security and privacy aware operating systems (OS) on their devices, in order to prevent malware to be installed and/or executed, prevent attackers from accessing the software running on the device, ease the creation of VPNs and tunnelling over untrusted connections and support a number of other security features. In the last years some robust implementations have appeared. Two of the most popular are:

- **Qubes**[260]: *Qubes is an open-source operating system designed to provide strong security for desktop computing using Security by Compartmentalization approach. Qubes is based on Xen, the X Window System, and Linux, and can run most Linux applications and utilize most of the Linux drivers*. Qubes follows a Security by Isolation approach by facilitating the creation of multiple security domains implemented as lightweight Virtual Machines (VMs) running under the Xen hypervisor. The implementation provides strong isolation among these domains so that an attacker who manages to compromise a domain cannot access all the software running in the other domains.
- **OpenBSD**[261]: OpenBSD is a free, open-source multi-platform 4.4 Berkeley Software Distribution (BSD)-based UNIX-like operating system. Proactive security and cryptography are two of the

[252] https://duckduckgo.com/
[253] https://ixquick.com/
[254] https://www.ixquick.com/eng/privacy-policy.html?
[255] http://searchengineland.com/scroogles-gone-heres-who-still-offers-private-searching-112275
[256] https://startpage.com/
[257] http://www.howtogeek.com/113513/5-alternative-search-engines-that-respect-your-privacy/
[258] http://blekko.com/
[259] http://www.ask.com
[260] https://qubes-os.org/
[261] http://www.openbsd.org/

features highlighted in the product together with portability, standardisation and correctness. Its built-in cryptography and packet filter make OpenBSD suitable *for use in the security industry, for example on firewalls, intrusion-detection systems and VPN gateways*[262].

- **TAILS**[263] Tails is a complete operating system, designed to be used from a DVD, USB stick, or SD card that, by relying on the TOR anonymising network, aims to preserve privacy and anonymity. Tails comes with several built-in applications pre-configured with security in mind.

7.3 Short to mid-term policy options for controlling mass surveillance

The following sections describe short to mid-term policy options that derive from the findings exposed in this document and that are considered appropriate by a number of experts for attempting to restrain indiscriminate mass surveillance both, from a technological and a regulatory point of view. Long term policy options to this respect are described in part 2 of this study.

7.3.1 EU initiative to implement a resilient implementation for encryption

The EU should invest in resilient open source implementations of different encryption specifications that can be verified and validated for correctness. The establishment of a Certification Body for such implementations, as mentioned in the policy options of part 2 of this study is directly related to this recommendation and would contribute to sustaining efforts for providing users with unbreakable cryptographic protection.

7.3.2 Promotion of open protocols, open implementations, open systems

The EU should promote and foster the development and usage of open protocols, open implementations and open systems in general. "Open" in this context refers to the public and transparent accessibility of such elements, which enables public scrutiny, control and verification of their respective functionality.

7.3.3 Regulation of Telecom security and encryption standards

The EU should regulate Telecom Operators to apply security mechanisms in form of adequate encryption over their entire networks, avoiding backhauls.

7.3.4 Invest in user awareness creation ("know the digital traces you are leaving")

The EU should invest in making users aware of the digital traces they leave when utilizing electronic media and the information profiles that can be generated making use of these traces. This should include information on how users can reduce their digital footprint by following behavioural rules and applying encryption and anonymising principles.

7.3.5 Increase citizen empowerment by regulating and investing in data/information transparency

The EU should invest in and promote data and information transparency for empowering citizens to take qualified decisions about the treatment of their data. This includes information about who, under which conditions, where and when can access private data and what is being done with it. Users should have the option to configure the level of visibility of their data (possibly assisted by intelligent privacy agents or wizards).

[262] http://en.wikipedia.org/wiki/Openbsd
[263] https://tails.boum.org/about/index.en.html

7.3.6 Invest in integrated platform specific security and privacy apps

The EU should invest in the development of integrated *platform specific* security and privacy suites, that are easy to setup and use, even for very unexperienced final users. Security and privacy solutions should become a utility.

7.3.7 Regulations that require applications to adopt maximum privacy settings as default

The EU should promote regulations that require application and service providers, particularly in the Cloud business, to adopt maximum privacy and security settings as default in their offerings.

8 CONCLUSIONS

Mass surveillance practices by intelligence and security agencies have caught the interest of media and the public at large since the publication of the secret documents leaked by Edward Snowden. Mass surveillance is a reality today and has been applied for years by national intelligence agencies of a number of countries, namely those allied in the Five Eyes coalition, but also including EU members and other countries.

The agencies involved in mass surveillance practices justify these methods with the doctrine of pre-emptive prevention of crime and terrorism and adopt the principle of omniscience as its core purpose. This objective of intercepting all communication taking place over Internet or telephone networks is in many cases pursued by applying questionable, if not outright illegal intrusions in IT and telecommunication systems. This strategy accumulates an amount of information that can only be processed and analysed by systems of artificial intelligence, able to discern patterns which indicate illegal, criminal, or terrorist activities.

While warranted and lawful interception of data on targeted suspects is a required and undisputed tool for law enforcement to access evidence, the generalised approach of information gathering through mass surveillance is violating the right to privacy and freedom of speech. The delegation of decisions on suspicious data patterns or behaviour of citizens to intelligent computer systems is furthermore preventing accountability and creating the menace of an Orwellian surveillance society.

Many citizens are not aware of the threats they may be subject to when using the Internet or telecommunication devices. As of today, the only way for citizens to counteract surveillance and prevent breach of privacy consists in guaranteeing uncorrupted end-to-end encryption of content and transport channel in all their communications.

Due to the amount/complexity/heterogeneity of tools this is however a task too complex to achieve for most of technically unexperienced users. This situation calls for both, awareness creation and the provision of integrated, user friendly and easy to use solutions that guarantee privacy and security of their communications.

But policy makers must understand that the problem of mass surveillance cannot be solved on a technical terrain, but needs to be addressed on a political level. An adequate balance between civil liberties and legitimate national security interests has to be found, based on a public discussion that empowers citizens to decide upon their civil rights affected and the societal values at stake.

LIST OF ABBREVIATIONS

ACLU	American Civil Liberties Union
AES	Advanced Encryption Standard
APT	Advanced Persistent Threat
BIOS	Basic Input/Output System
CGHQ	Government Communications Headquarters (UK)
DDoS	Distributed Denial of Service
DNT	Do Not Track
DOD	(US) Department of Defense
DPI	Deep Packet Inspection
DRIPA	Data Retention and Investigatory Powers Act
EB	Exabytes
EFF	Electronic Frontier Foundation
ETSI	European Telecommunications Standard Institute
FISC/FISA	Foreign Intelligence Surveillance Court/Act
FTC	Federal Trade Commission
FVEY	Five Eyes Intelligence Alliance (USA, Canada, UK, Australia, New Zealand)
GPRS	General Packet Radio Service
GPS	Global Positioning System
HTTP	Hypertext Transfer Protocol
IC	Integrated Circuit
IC	Intelligence Community
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IMEI	International Mobile station Equipment Identity
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IP	Internet protocol
IPS	Intrusion Prevention System
ISP	Internet Service Provider
KDD	Knowledge Discovery in Databases
LEA	Law Enforcement Agency
NSA	National Security Agency (of the USA)
OSI	Open Systems Interconnection
PGP	Pretty Good Privacy (open source encryption tool)
RFC	Request for Comment
RNG	Random Number Generator
SCA	Stored Communications Act
SIGINT	Signals Intelligence
SIM	Subscriber Identity Module
SSL	Secure Socket Layer
TAO	Tailored Access Operations (a division of NSA)
TOR	The Onion Ring Network
URL	Uniform Resource Locator
USB	Universal Serial Bus
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

This document identifies the risks of data breaches for users of publicly available Internet services such as email, social networks and cloud computing, and the possible impacts for them and the European Information Society. It presents the latest technology advances allowing the analysis of user data and their meta-data on a mass scale for surveillance reasons. It identifies technological and organisational measures and the key stakeholders for reducing the risks identified. Finally the study proposes possible policy options, in support of the risk reduction measures identified by the study.

This study covers the analysis of the existing generation of network services and applications at the time of the study (2014) and the short to mid-term technical measures and policy options suitable for counteracting mass surveillance practices and guaranteeing privacy and security of electronic communication channels.

This is a publication of the
Directorate for Impact Assessment and European Added Value
Directorate-General for Parliamentary Research Services, European Parliament

PE 527.409
ISBN: 978-92-823-5535-0
DOI: 10.2861/269619
CAT: QA-05-14-155-EN-N