EUROPEAN PARLIAMENT

Science and Technology Options Assessment (STOA)

Mass Surveillance

Part 2 – Technology foresight, options for longer term security and privacy improvements

STUDY

EPRS | European Parliamentary Research Service

Scientific Foresight (STOA) Unit
PE 527.410

EN

Mass Surveillance

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

Part 2 – Technology foresight, options for longer-term security and privacy improvements

Study

IP/G/STOA/FWC-2013-1/Lot4/SC1

December 2014

PE 527.410

The STOA project "Mass surveillance – Risks, Opportunities and Mitigation Strategies – Part 2 Technology foresight, options for longer-term security and privacy improvements" was carried out by Capgemini Consulting, part of Capgemini Netherlands BV.

AUTHORS

M. van den Berg
P. de Graaf (editor)
P.O. Kwant
T. Slewe

The authors acknowledge and would like to thank the following experts for their contributions to this report: *Mr Axel Arnbak, University of Amsterdam (NL), Mr Brent Bilger, Vice-President Solutions Architecture at Vidder (USA), Mr Caspar Bowden, independent privacy researcher (UK), Dr Christian Doerr, University of Delft (NL), Mr Rickey Gevers, forensic investigator at Digital Investigations (NL), Ms Monika Maglione, Mr Michael Palmer and Ms Cecilia-Joanna Verkleij (EC-DG Home), Mr Gopal Padinjaruveetil, Chief Security and Compliance Architect Capgemini US (USA), Mr Rejo Zenger and Mr Hans de Zwart, Bits of Freedom (NL).*
Also we relied on the insights of the Capgemini Cyber Security Community of Practice, in particular: *Mr Jule Hintzbergen, Mr Cees de Kuijer, Mr Guido Voorendt, Mr Jan Willem de Vries and Mr Jack van 't Wout.*

STOA RESEARCH ADMINISTRATOR

Peter Ide-Kostic
Scientific Foresight 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 November 2014
Brussels, © European Union, 2014

DISCLAIMER

The content of this document is the sole responsibility of the author and any opinions expressed therein do not necessarily represent the official position of the European Parliament. It is addressed to the Members and staff of the EP for their parliamentary work. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

PE 527.410
ISBN: 978-92-823-6389-8
DOI: 10.2861/55669
CAT: QA-06-14-228-EN-N

Abstract

The main objective of part two of this study is to provide the European Parliament with policy options, based on technology foresight, with regard to the protection of the European Information Society against mass surveillance from a perspective of technology and organisational foresight. Four scenarios with two to four technology options each were developed in this study, leading to twenty-three policy options.

Current risks of data breaches, their impact on European citizens and the European Information Society are outlined in part one of the study, which is also published by STOA. Part two of the study also covers short- and medium-term technology measures and policy options for counteracting mass surveillance and protecting the privacy and security of electronic communication channels.

This study is accompanied by an Annex (B), which provides detailed answers to the twenty-one questions arranged in four themes, as drafted in preparatory work by STOA.

CONTENTS

MANAGEMENT SUMMARY

The main objective of this study is to provide the European Parliament and specifically the LIBE Committee with more technological background information and possible policy options, based on technology foresight, with regard to the protection of the European Information Society against mass surveillance from a perspective of technology and organisational foresight. Four scenarios with two to four technology options each were developed in this study.

Policy options for the 'Promote adoption' scenario

Promote end-to-end encryption

Stimulate **awareness of the necessity of using encryption** by initiating a media campaign, as awareness of privacy risks is quite low.

Increase the **knowledge level of end-users**, both individuals and responsible departments in organisations, by setting up an **independent platform** where users can find information on tools, implementation, *do's and don'ts* etc.

Support product security tests by independent institutions such as the Electronic Frontier Foundation that help users make better-informed choices. Support can be a financial contribution, but also promotion of the results. Alternatively the EU can set up its own regular **product security test programme**.

A parallel option is to **stimulate user-friendliness of end-to-end encryption solutions**, for instance by promoting existing user-friendly end-to-end encryption solutions for e-mail, messaging, chat etc. Dedicated **funding or participation** in open-source software end-to-end encryption solutions is also an option to specifically improve user-friendliness.

If the market does not provide security with end-to-end encryption by itself, **regulation** should be considered, obliging service providers and/or Internet service providers to provide end-to-end protection as standard for data in transit. An additional benefit of regulation would be a **concrete political discussion on the balance** between privacy and law enforcement and national security, at European and/or national level. The outcome of this debate should be implemented in national legislation.

Promote open-source software

Although it is not a universal remedy, open-source software is still an important ingredient in an EU strategy for more security and technological independence. The **quality of the lifecycle processes** of open-source software is crucial for its security – more than technology.

Support and fund maintenance and/or audit of important open-source software: open-source initiatives, some of them widely implemented for security and privacy[1], need funding to keep going and be audited (with regard to both code and processes).

Initiate a European "*Open-Source Bug Bounty Programme*" or finance existing programmes, as an alternative to intervening directly with specific open-source software programmes.

Set up certification schemes for a limited set of critical types of open-source software, implemented by technical tests (e.g. penetration tests, code reviews). To support this, the EU should draft and maintain an **agenda of critical open-source software** for its citizens and companies.

[1] such as OpenSSL, TrueCrypt/Ciphershed, GPG, Tor, OwnCloud, etc.

Promote and stimulate EU ICT services: Cloud, social media, search engines

A consumer-market-oriented approach to European social media, Cloud services and search engines is a desirable option, although not the easiest, since the European market is open and fragmented and major platforms are available for all *current* service categories.

We therefore propose stronger **legal limits on exporting personal data** than those offered by the forthcoming data-protection regulation (mainly transparency on location, informed consent by individual). This would give European ICT players the time and legal space necessary to create demand for specific EU solutions. **Liability and substantial fines** for non-compliance will also provide a strong stimulus for action.

Promote secure software development

Promote the **use of existing guidelines** for secure software development, such as the OWASP Top 10. Security is not a job only for 'Security', but for all staff involved in designing, developing, maintaining and exiting software. Draft **EU guidelines** for secure software development with the software industry. Challenge software suppliers to adhere to secure software development guidelines, **leveraging the buying power** of the EU institutions.

Certification of software is also a policy option, but given the magnitude of software in circulation and under development, this should start with a very specific focus, for instance browsers, operating systems and mobile apps. The next step could be **product liability for (some) software** to protect users from risks resulting from insecure software – risks they themselves usually cannot assess or mitigate.

Policy options for the 'Build Confidence' scenario

Security baselines

Implement **EU Security Baseline regulations** to build confidence by ensuring a minimum level of security measures for critical information infrastructure elements in the EU.

EU Coordinated Disclosure

EU **rules or guidelines for facilitating a process of 'coordinated disclosure'** help with the discovery and fixing of more software vulnerabilities, whilst protecting those disclosing within the rules. An **EU guideline on Coordinated Disclosure** should be issued. **A (trusted) national coordinator** should monitor to ensure that reported vulnerabilities are fixed.

Policy options for the 'Disrupt(ive Innovation)' scenario

Certification schemes

The key policy option with regard to encryption schemes is to establish an **EU standardisation body or certification authority for encryption standards**. Such a certification scheme should be complemented by a **legal framework which, for example, imposes liability** on non-compliant Internet service providers. Ideally such an EU standardisation body would **cooperate internationally** with the US National Institute for Standards and Technology and other national agencies on the process level (way of working) and principles, to avoid negative effects of regionalisation.

European Internet Subnet

To prevent network routing information from being intercepted for metadata analysis purposes by a third party, the EU in theory could **physically or logically separate the network** from the rest of the world. This is not the way forward. Other approaches such as **deperimeterisation**, at data and application level, must be implemented instead.

Regulations on certified hardware and software for major Internet access points in the EU would raise the overall security of the European part of the Internet.

Policy options for the 'Innovate' scenario

Stimulate Research & Development into reduced trackability/traceability and detection of surveillance

Let the EU set up a dedicated research project to **design or redesign Internet protocols** to minimise the trackability of users. **Regulate** to implement an option in **consumer devices to block** the sending of messages that reveal the location of the user (with an opt-in for users).

Fund **open-source tools** that enhance privacy/block traceability. **Impose a**n obligation (in cases where it is not possible to avoid traceability) to show a **message to users warning** them that they can be traced. Or even stronger: **impose non-traceability as a requirement** as part of security by design for (personal and/or or mobile) devices.

'Fix the Internet' – promote improvement of inherently insecure protocols

More secure open standards for Internet protocols in the EU could be **stimulated** by supporting **individual contributions** and setting up a **dedicated long-term research & development effort** in cooperation with the academic world, Internet service providers, the Internet Engineering Task Force and others to research and co-develop open standards.

Finally, if protocols are considered to be insecure (which most are) and a cure is not easily obtained, then **depreciation of that protocol** is in order, ultimately by public **regulation**.

Data-centric security

Set up a specific EU **research & development programme** on data-centric security, especially implementation concepts and more specifically those for individual users.

Overall conclusions

Despite the many technology foresight options, there is no single technological solution to help citizens better manage their privacy risks in the light of mass surveillance and other threats against their privacy. Work needs to be done on a number of technologies to achieve a robust security posture, and this work should start now.

Given the open nature and general technological state of the Internet and local ICT environments, the technology-based policy options to pursue in combination are:

- **End-to-end encryption** is one of the strongest ways to protect data during communication, but ease of use and (proactive collective) implementation must be pursued to achieve sufficient scale in terms of the number of users. Furthermore, Europe should set up its own **certification schemes** for encryption standards, to mitigate the risk of backdoors. Bear in mind that should **quantum computing** become available, this and other encryption options should be deemed obsolete immediately.

- **Deperimeterisation at data and application** level, not network level, to protect access to critical data. Data-centric approaches and software-designed parameters offer much more flexible application, regardless of the underlying (Internet) infrastructure.
- Increase EU technological independence through **verifiably secure open-source software ("SOSS")**. Improving the quality of lifecycle management processes of key open-source software platforms is essential, as is certification of these platforms. The EU should invest in code review and certification schemes and facilities for open-source software.
- The EU should increase its efforts to fix structural security problems with Internet protocols which undermine security against all sorts of cyber threats.
- Finally, the EU should set up an independent institute for **certification** of encryption standards and key open-source software platforms.

These technology options should be accompanied and supported by legal, financial and promotional arrangements. A tougher posture than that currently proposed in the forthcoming EU **Data Protection regulation** on personal data export, for instance, would create the breathing space that European (open-source software) ICT needs to build up a substantial market position and enough scale to survive independently.

Product liability and leveraging the **purchasing power of the EU and its Member States** are other ways to stimulate the market to produce more secure ICT, fit for secure use in the EU.

Several developments will challenge the technologies described. Quantum computing was mentioned, but undoubtedly (other) **surveillance technologies** are under development as well. The **Internet of Things** (IoT) will dramatically widen the possibilities for surveillance and pose new security and privacy risks as well. With IoT the average citizen will have even less influence on what data he or she shares, when and with whom. The privacy and security aspects of IoT are barely discussed at present.

The **Big Data** that the Internet of Things generates is of specific interest for **marketing** too, providing valuable data on consumer behaviour and well-being. The focus on privacy with regard to mass surveillance should not draw attention away from other intrusions.

Finally, it is not technology, but **political debate** that determines where the balance should be between privacy and law enforcement, intelligence and marketing. Leaving the balance up to technological and market forces will most probably be unsatisfactory for all sides.

1. INTRODUCTION

1.1. Background

The revelations by Edward Snowden in 2013 on practices of mass electronic surveillance of EU and other citizens have led to (and revived) countless discussions on the alleged capabilities of nations, proportionality of the means used, risks to privacy and data protection, the effectiveness of EU law and other issues. To achieve greater clarity on these and other matters, the European Parliament issued its Resolution (2013/2682(RSP)) of 4 July 2013, instructing the Committee on Civil Liberties, Justice and Home Affairs (LIBE) to conduct an in-depth inquiry into the issue of mass electronic surveillance.

1.1.1. LIBE committee report

In March 2014 the European Parliament adopted the report *'on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs'* (2013/2188(INI)).

The report takes the view that this crisis could be used as an opportunity for Europe to develop a strong and autonomous IT capability (including IT systems, equipment, services, Cloud computing, encryption and anonymisation). In order to *'regain trust, such a European IT capability should be based, as much as possible, on open standards and open-source software and if possible hardware, making the whole supply chain from processor design to application layer transparent and reviewable.'*

The final EP resolution of 12 March contains many recommendations that could be further explored, including (but not limited to):

- *"Promote the use of open-source software in all environments where IT security is a concern; (…)*
- *Promotion of EU search engines, EU social networks, European IT service providers, European IT key elements (such as client-server operating systems); (…)*
- *Promotion of encryption of communication in general, including e-mail and SMS; (…)*
- *The use of open-source standards, developing European elements for grid coupling, e.g. routers; (…)*
- *Certification scheme for IT hardware, including testing procedures (at EU level), to ensure the integrity and security of the products."*

The political and public discussion inside and outside the European Parliament on mass electronic surveillance practices by foreign intelligence services has meanwhile led to the political notion of a 'European Internet'[2]. This notion also invites more exploration.

1.2. Objectives of this study

Although quite extensive in terms of the numbers of hearings and other sources investigated, the extent and impact of the LIBE inquiry would benefit from more insight into possible mitigation strategies. What are the concrete (technical) risks and opportunities in current IT? And what are longer-term options?

The European Parliament has therefore initiated the study *'Mass surveillance – What are the risks for citizens and the opportunities for the European Information Society? – What are the possible mitigation strategies?'* This study comprises two independent parts executed in parallel by two different teams. Part 1 focuses on the risks and opportunities raised by the current generation of network services and applications. Part 2

[2] Financial Times, Angela Merkel backs EU internet to deter US spying, 16 February 2014, http://www.ft.com/intl/cms/s/0/dbf0081e-9704-11e3-809f-00144feab7de.html, accessed on 2 November 2014.

focuses on the technology foresight, options for longer-term security and privacy improvements. This report is on part 2 only.

The main objective of this study is to provide the European Parliament, and specifically the LIBE Committee, with (more) background information and possible policy options to protect the European Information Society against mass surveillance from a technology and organisational foresight perspective, taking the recommendations of the February report one or more steps further.

1.3. Key questions

Key questions to be answered in this study are:

- How to achieve a balance over the long term within the next 10 years, from a technological and organisational foresight perspective, between the need for individual privacy and the needs of the organisations legally in charge of law enforcement and/or national security;
- What are the long-term technology and organisational foresight options to reduce the risks of mass surveillance of EU citizens while preserving adequate preventive and reactive investigation capabilities for governmental agencies in charge of law enforcement and/or national security?
- Who are the main key players and stakeholders involved in implementing the different foresight options identified and what are their corresponding challenges and opportunities, what are the implementation barriers and how can they be overcome?
- What are the corresponding policy options?

To answer these key questions, STOA defined four relevant themes, largely based on earlier studies:

- Research Theme 1: Identify, categorise and evaluate what technological initiatives are ongoing for the redesign of the Internet;
- Research Theme 2: Explore the feasibility of the concept of a secure "European Internet Subnet" as part of the "Global Internet";
- Research Theme 3: Advantages and disadvantages of relying on the use of open source for improving the security and privacy of IT products and services and the Internet
- Research Theme 4: Advantages and disadvantages of a shift towards "End-to-end user encryption".

Each of the themes is underpinned by a subset of mostly technology-oriented questions. The answers to each of these questions can be found in the annexes, with a higher-level description in chapter 2.

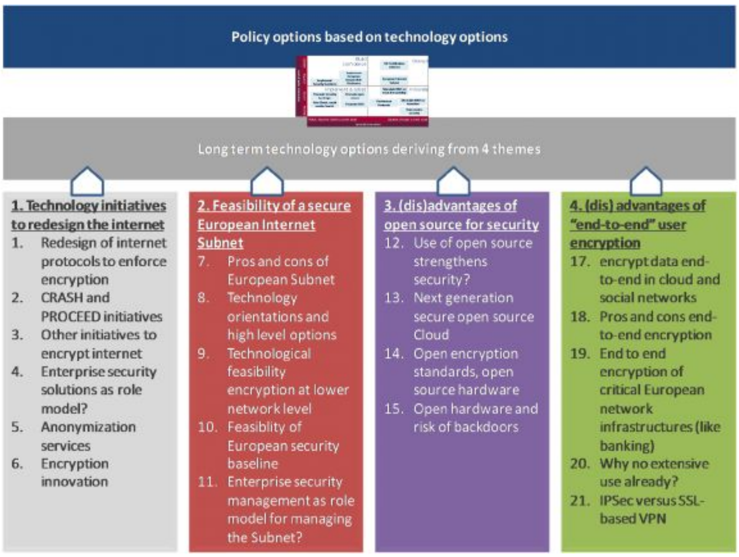

Policy options based on technology options
Long term technology options deriving from 4 themes
1. Technology initiatives to redesign the internet
1. Redesign of internet protocols to enforce encryption
2. CRASH and PROCEED initiatives
3. Other initiatives to encrypt internet
4. Enterprise security solutions as role model?
5. Anonymization services
6. Encryption innovation
2. Feasibility of a secure European Internet Subnet
7. Pros and cons of European Subnet
8. Technology orientations and high level options
9. Technological feasibility encryption at lower network level
10. Feasiblity of European security baseline
11. Enterprise security management as role model for managing the Subnet?
3. (dis)advantages of open source for security
12. Use of open source strengthens security?
13. Next generation secure open source Cloud
14. Open encryption standards, open source hardware
15. Open hardware and risk of backdoors
4. (dis) advantages of "end-to-end" user encryption
17. encrypt data end-to-end in cloud and social networks
18. Pros and cons end-to-end encryption
19. End to end encryption of critical European network infrastructures (like banking)
20. Why no extensive use already?
21. IPSec versus SSL-based VPN

Figure: Structure of content of study

Each of the researched topics in all four themes resulted in long-term (or sometimes short-term) technological and organisational options to mitigate the security and privacy risks associated with mass surveillance, but not all were considered feasible or deemed to be effective in balancing security and privacy against legal mass surveillance. The options that were considered feasible or effective were supplemented with the additional concepts that are advocated. An example is the idea of a European (EU) coordinated disclosure guideline to help find vulnerabilities in software much sooner by leveraging the expertise of volunteers. Another example is the reduction of traceability of mobile and fixed devices.

All technology/organisational options were grouped into four new clusters, based on four scenarios deriving from two mutually exclusive dimensions (see chapter 2). For each technology option one or more policy options were added.

1.4. Methodology

The technology and organisational foresight and policy options are based on a substantial amount of external, recent, scientifically justifiable sources, expertise of the authors and social media.

Research instruments

The breadth of the topics in Annex B (the 'themes') and additional subjects required extensive research efforts. In order to answer all key questions and 21 questions in four themes as mentioned in paragraph 1.3, over 200 **documents** and articles, eight official **interviews** (as well as numerous off-the-record conversations) and comments on **social media** (both dedicated to this study and relevant but not related) were studied and processed in the period from August to November 2014. Numerous **informal discussions** within the core team and in the worldwide Capgemini cyber security community were also organised, as a source for analysis, respondents for interviews and validation of findings.

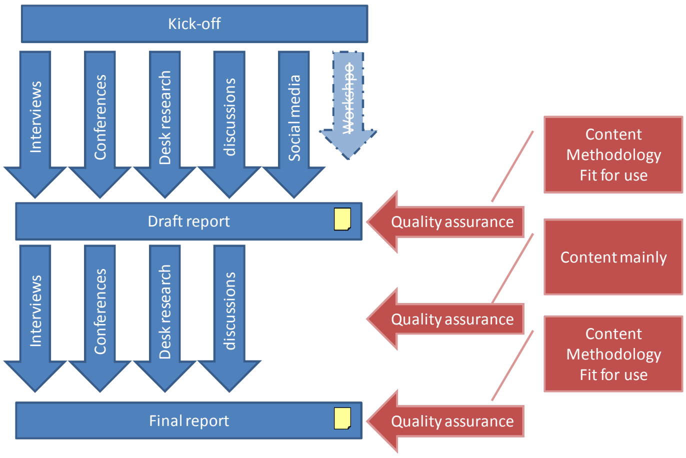


Figure: research methodologies used[3]

Social media as an interactive research instrument was somewhat disappointing: with 11 comments by six unique users, the response was quite low, despite the fact that we chose the largest information security community available online: the Information Security Discussion Group on LinkedIn (233,792 members, when checked on 24 November 2014). We abandoned this instrument in mid-October 2014, since the efforts far outweighed the results.

The main reasons for these meagre results were abundant competition from more or less related issues and the high level of our own questions. More concrete topics such as "*NSA-proof e-mail*" attract far more attention. Even supporting blogs with more concrete content could not turn the tide.[4] On the positive side, social media channels did provide good sources for the topics covered throughout the research project.

Not included in the figure as a source are the lessons learned from many earlier discussions with other privacy and Internet security experts and the core team members' own experience. Although not specifically gathered for this study, these past discussions and experience shaped the vision and insights of the authors.

Research team for Part 2

This report was drafted as part of a two-pronged study, with both parts under the direction of STOA. Part 1 of this study was conducted by Tecnalia. The two teams liaised at project management level, for the purpose of keeping the two parts connected, identifying major overlaps and sharing resources.

[3] Please note that our initial proposal (as requested) included a workshop, which is pivotal for turning a wide set of topics into a focused report with supported policy options. The event would also provide a communication 'anchor' for social media activities, something concrete to refer to. The research administration decided to cancel this workshop, however, so the research team put more effort into interviews, desk research, conference attendance and informal discussions.

[4] Such as: http://www.capgemini.com/blog/capping-it-off/2014/10/do-eu-security-baselines-make-the-internet-more-secure; http://www.capgemini.com/blog/capping-it-off/2014/10/open-source-software-as-technology-option-for-more-security-and-privac-0

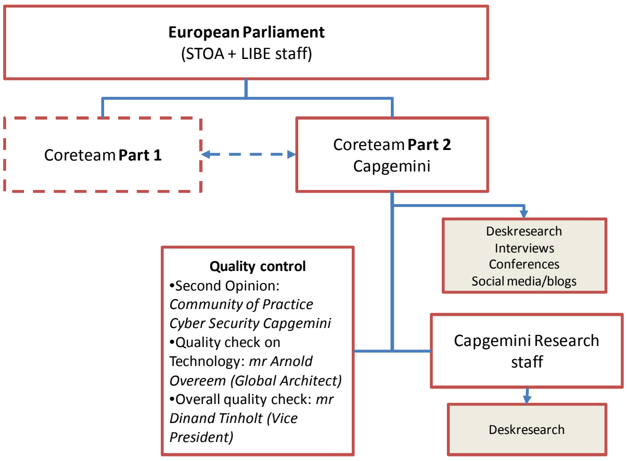

European Parliament
(STOA + LIBE staff)
Coreteam Part 1
Coreteam Part 2
Capgemini
Deskresearch
Interviews
Conferences
Social media/blogs
Quality control
•Second Opinion: Community of Practice Cyber Security Capgemini
•Quality check on Technology: mr Arnold Overeem (Global Architect)
•Overall quality check: mr Dinand Tinholt (Vice President)
Capgemini Research staff
Deskresearch

Figure: structure of research team for Part 1

The core team of Part 2 consisted of four Capgemini cyber security experts with extensive experience in the public sector and financial services industry, both in technology and (national) policy preparation. This team conducted most of the desk research and all of the interviews, conference attendance, social media activity and informal discussions. The core team was supported by the Capgemini back-office (open-source) research staff based in India.

Quality control

The core team used several mechanisms to ensure quality of content, methodology and fitness for use, besides the valuable **feedback from LIBE and STOA** staff members during the kick-off and mid-term meeting. These other mechanisms were:

- A **second opinion** on the first findings was organised through a formal discussion with members of the Capgemini Cyber Security Community of Practice in the Netherlands. This formal discussion helped shape the translation from technology foresight options to policy options and brought up some additional technology foresight options with their complementary policy options.
- **Quality check of content and methodology**: on the initial and final draft, performed by Mr Arnold van Overeem, Global Architect for Capgemini.
- **Quality check of fitness for use and methodology:** on initial draft and final draft, by Mr Dinand Tinholt, Vice President EU for Capgemini.

1.5. Contents of this study

In chapter 2 the report presents the technology and organisational foresight options, organised in four scenarios. These options mainly build on Annex B, in which 21 foresight topics, grouped over four themes, are explored. For each foresight option, the corresponding policy options are described. Chapter 2 ends with closing thoughts on overarching subjects or topics that do not fit within the earlier foresight options. In chapter 3, all policy options from the previous chapter are summed up along the lines of the same scenario, ending with an overall conclusion. In the annexes the reader can find sources (A), foresight options in four themes (B) and a list of abbreviations (C).

2. TECHNOLOGY AND ORGANISATIONAL FORESIGHT OPTIONS

During research for this study (conferences, interviews, desk research, social media research and discussions) and in earlier studies many technological and organisational options were advocated to restore the balance between security and privacy of EU citizens and corporations and the legitimate interests of law enforcement and intelligence. The focus of the majority of these technological and organisational options is to increase security and privacy, starting from the basic assumption underlying this study: that a balance should be restored by moving towards improved privacy and security. We collected these options 'bottom-up' and structured them later in the process. At this stage no selection was made in terms of legal, political or (current) technical feasibility. Only manifestly unfeasible options were left out.

In structuring these options, two dimensions were deemed the most exclusive – in the sense that there was no direct, apparent correlation between the two: level of innovation and level of intervention. The level of innovation of options ranges from promoting the use of existing technologies (or making them more user-friendly) to building up a complete new technological world and many things in between. In ICT terms, one might say the options are either to patch the current world to optimise what is already there or to deliver an entirely new update mitigating risks substantially. Patching or updating usually has consequences in terms of costs and time.

The level of required or suggested governmental (national or EU) intervention also varies. The 'light' options require active promotion and stimulation or financing (of R&D, for example). Heavier interventions involve legislation or an active role on the part of the EU (and/or Member States) in realising actual products or services.

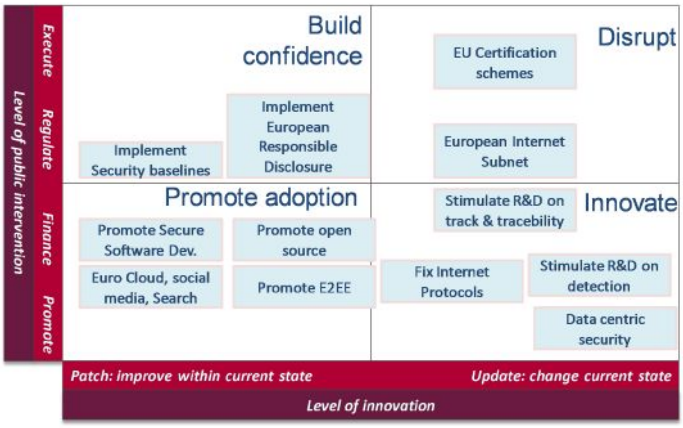

Level of public intervention
Execute
Regulate
Finance
Promote
Build confidence
Implement Security baselines
Implement European Responsible Disclosure
Disrupt
EU Certification schemes
European Internet Subnet
Promote adoption
Promote Secure Software Dev.
Promote open source
Euro Cloud, social media, Search
Promote E2EE
Innovate
Stimulate R&D on track & tracebility
Fix Internet Protocols
Stimulate R&D on detection
Data centric security
Patch: improve within current state
Update: change current state
Level of innovation

Figure: four scenarios defined by level of innovation and level of public intervention

The resulting non-exclusive scenarios and corresponding foresight options are:

1. **Promote adoption:** decrease existing technological vulnerabilities for citizens with options that are not very innovative in a technological sense, yet the duration of adoption makes them a long-term solution:
   1. Promote end-to-end-encryption (E2EE) (mainly: lowering barriers for adoption)
   2. Promote open-source software (stimulate open-source software development and maintenance processes)
   3. Promote and/or stimulate Euro Cloud Services: Cloud, social media, search engines

4. Promote secure software development and security by design

Please note that the use of existing and emerging security and privacy technologies is discussed in Part 1 of this Study.

2. **Build confidence:** measures to improve trust between Member States without the use of disruptive changes in technology:
    1. Create and Promote EU Coordinated Disclosure Guidelines
    2. Create and Promote security baselines and ensure they are used

3. **Disrupt or disruptive innovation:** Increase European technological independence to mitigate structural vulnerabilities[5]:
    1. Improve certification schemes + auditing of hardware, software and encryption used in the EU
    2. Create a European Internet Subnet (in several varieties)

4. **Innovate:** smart fixes to mitigate structural technological vulnerabilities:
    1. Stimulate R&D into reduced trackability/traceability of mobile and fixed devices
    2. 'Fix the Internet' – promote improvement and replacement of inherently insecure protocols
    3. Stimulate R&D on detection of surveillance
    4. Stimulate R&D on data-centric security

These options are non-exclusive in the sense that one does not exclude the other. Options can be combined; in some cases, this is very advisable. The two most extreme options were not investigated: 1. do nothing and accept the risk; 2. redesign the Internet.

In the following paragraphs we describe each of the remaining options, answering the key questions: How does this option help balance the need for individual privacy and the needs of the organisations legally in charge of law enforcement and/or national security, preserving adequate preventive and reactive investigation capabilities? Who are the main key players and stakeholders involved and what are their corresponding challenges and opportunities? What are the implementation barriers and how can they be overcome? And finally: what are the corresponding policy options?

2.1. Promote adoption: decrease existing technological vulnerabilities

2.1.1. Promote end-to-end encryption

With end-to-end encryption, (or E2EE), messages are encrypted on the sender's computer and decrypted on the recipient's device. Telecom providers, ISPs and service providers such as Google, Facebook, Tencent or Microsoft only see encrypted information. Thus these companies cannot disclose (readable) copies to government agencies, even with a court order. In this way E2EE offers an improved level of confidentiality of information and thus privacy, protecting users from both censorship and repression and law enforcement and intelligence.

Strong cryptographic software is available to those who want to use it, as E2EE software has existed since the 1980s. They include PGP (e-mail encryption software released in 1991), OTR ("off the record", for

[5] Not included is extreme disruption: start from scratch. The Internet was never designed for confidentiality. A complete new Internet from top to bottom could take all current concerns into account, with the obvious risk of missing additional new concerns. However, such a scenario is not deemed to be realistic.

secure instant messaging) and the Internet telephony apps Silent Circle and Redphone and newer ones such as Proton Mail, DIME (aka Dark Mail) and specific plug-ins for Chrome, Firefox and other browsers.

> A sufficient key length and size is necessarily to ensure protection: 128 bits for symmetric encryption or longer is advisable, but this also depends on the algorithm employed. Larger keys are possible (Blowfish can handle 448 bits, for instance, and AES demands 256 bits). The longer the key, the more time it takes to break it. Please see also Annex B, number 6. *Latest technology prospects related to encryption*.

Newer E2EE tools not only encrypt data, but also encrypt metadata (e.g. DIME and ProtonMail).[6]

As described in Annex B, 17 and 19, there are several valid reasons why E2EE is not used more extensively, for instance for person-to-person communication by e-mail or instant messaging:

- Technological (availability of tools, complexity of installation, user base, user-friendliness, guaranteed authenticity of communications)
- Psychological (privacy awareness, motivation to protect, knowledge to use)
- Social (E2EE is considered paranoid in a specific group or organisation)
- Political (E2EE prohibited)

E2EE does, however, provide a fairly high level of security against mass surveillance, although not against software or hardware backdoors (on the device, after the 'end'). At some point the user has to access his or her information, in order to read or modify it. But given the public statements by several law enforcement agencies in November 2014[7] that possibilities should exist for accessing the content of encrypted communications, E2EE is considered to be a good line of defence for individual users. Since the users of these products might be either criminals or well-meaning citizens, a *political* discussion is needed to balance the interests involved in this instance. This is discussed further below.

Key players involved and challenges

End-users

E2EE offers no protection against software or hardware backdoors (on the device, after the 'end'). At some point the user has to access his or her information in order to read or modify it. Targeted attacks, for instance with screen scrapers or key loggers, can also still be carried out to obtain the desired information from the user's device. Protection is therefore not complete.

One of the best-known problems of encryption software is user-friendliness, or the lack of it.[8] Even if it has been acknowledged many times, it is still hard to make E2EE easy to use and users value convenience

[6] Gallagher, Ryan (2013), 'Meet the "Dark Mail Alliance" Planning to Keep the NSA Out of Your Inbox', http://www.slate.com/blogs/future_tense/2013/10/30/dark_mail_alliance_lavabit_silent_circle_team_up_to_create_surveillance.html and Levison, Ladar, 'Lavabit's Dark Mail Initiative', https://www.kickstarter.com/projects/ladar/lavabits-dark-mail-initiative/posts, both accessed on 17 October 2014.

[7] These include Europol, FBI, Metropolitan Police. See below.

[8] Whitten, Alma and J. D. Tygar (1999), 'Why Johnny Can't Encrypt' in Security and Usability: Designing Secure Systems that People Can Use, eds. L. Cranor and G. Simson. O'Reilly, pp. 679-702. See also: Lee, Timothy B. (2013), 'NSA-proof encryption exists. Why doesn't anyone use it?' http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/14/nsa-proof-encryption-exists-why-doesnt-anyone-use-it/, accessed on 10 October 2014, and CNET (2013) , 'Dark Mail Alliance' looks to create user-friendly e-mail encryption, http://www.cnet.com/news/dark-mail-alliance-looks-to-create-user-friendly-e-mail-encryption/, accessed on 17 October 2014. The Dark Mail Alliance, consisting of the founders of shuttered e-mail services Silent Mail and Lavabit, aims to create encrypted e-mail "easy enough for your grandma to use". See also their website

more than security. "Security is very rarely free," says J. Alex Halderman, a computer science professor at the University of Michigan in the Washington Post. "There are trade-offs between convenience and usability and security." This means that most people currently accept the risks.

Unless more users adopt it, those who currently use encryption will remain a distinct minority. This is especially a problem in countries with censorship and/or human rights issues, where encryption might even be illegal.

A chicken-and-egg problem also occurs: using encryption services becomes useful only if enough people are using it. PGP, DIME/Darkmail or other encrypted e-mail applications offer protection only when communicating with other users with the capability to read and receive encrypted e-mail.

Encryption is only effective if one is certain about the identity of the party one is communicating with. This authentication relies on using the right keys. A 'man in the middle' attack can trick the sender into using the wrong encryption key. To thwart this kind of attack, the sender and recipient need a way to securely exchange and verify each other's encryption keys. Confidentiality therefore depends heavily on authenticity.

Much mass surveillance effort depends on metadata to find the needle in the haystack. For privacy purposes this metadata should also be encrypted, not just the content of communications. However, this is not the case with all E2EE solutions.

A more practical disadvantage of E2EE concerns the consequences of losing a password. Losing a password means losing all data in the user's account, as the service provider has no access to the data, nor to the private key. However, this is a usability issue rather than a privacy issue, although it might deter potential users.

E2EE has to be set up carefully too, in order to be effective. This is one of the reasons why it is deemed less user-friendly. The user may believe the message or call is encrypted, but due to some mistake it might not be.[9]

For the reasons mentioned above, E2EE can also create a false sense of security for users. It does not always offer complete protection, even when used correctly.

More practically, performance loss is the most noticeable issue with encryption. The complexity of implementation (for instance key management) is another challenge for end-users.

Service providers

For commercial service providers, E2EE does not yet offer any specific, substantial advantages. There might be a business opportunity in offering encrypted e-mail as a paid bonus option on (now still) free mail accounts. Fear of reputational damage due to (alleged) cooperation with intelligence agencies can be another driver for service providers. In order to keep their clients, they can adopt E2EE as a generic service.

On the other hand there are substantial challenges. With E2EE, service providers lack access to content. This disrupts their business model, particularly for currently free services ('mining free e-mail' is a source of data for Google, Microsoft and others). *'If you're not paying, you're the product.'*

https://www.darkmail.info/ and, oddly more informative, their contributions on the crowdfunding website Kickstarter: https://www.kickstarter.com/projects/ladar/lavabits-dark-mail-initiative/posts.

[9] Whitten et al (1999).

Other business models are available, such as paying for extra storage and/or per month, but many users are attracted to free services and lose interest when they cease to be free.

Paid options still do not solve the issue that data-enriching options such as indexing, reformatting, filtering of user data are practically impossible with encryption. Providers such as Facebook use this technique to present users with tailor-made timelines, for instance.[10] The overall service level, value and attractiveness for users decrease.

A specific challenge is standardisation of encryption products. Some vendors[11] are trying to solve the underlying interoperability problem between encryption systems with the OASIS Key Management Interoperability Protocol (KMIP).[12] This is intended for streamlining and standardising communications between encryption products.

ISPs

E2EE also offers no direct benefits for ISPs (including telecom providers). Providing E2EE as a standard service increases the costs of operations in a business where margins are already under pressure.

On the security side, E2EE might also hamper spam filtering, depending on the solution used to tackle spam. Other solutions are available, however.

Law enforcement/intelligence

The primary opportunity of E2EE from the law enforcement and national security perspective is the protection of users (and society as a whole) against cybercrime and digital espionage. If content is encrypted, this sets up a serious barrier against malicious actors and prevents crimes and data leakage, or at least lowers the potential impact.

On the other hand, E2EE offers possibilities for criminals and terrorists to hide the nature of their activities from LE and national security agencies.[13] Even with known suspects it might prove to be very difficult to access the content of their communications (and thus intentions, plans and actions).

Troels Oerting from Europol therefore recently stated that: *"The increasing trend towards greater encryption of online communications is not acceptable (...). Imagine in the physical world if you were not able to open the trunk of a car if you had a suspicion that there were weapons or drugs inside... we would never accept this. I think that should also count for the digital world. I hate to talk about backdoors but there has to be a possibility for law enforcement, if they are authorised, to look inside at what you are hiding in your online world."* [14] His underlying statement is that *"privacy cannot equal anonymity"*.[15]

Along the same lines FBI Director James Comey has asked the US Congress to force smartphone developers to build backdoors into all devices for law enforcement surveillance, seemingly in response to

[10] Washington Post, NSA proof encryption exists. Why doesn't anyone use it?, 14 June 2013, http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/14/nsa-proof-encryption-exists-why-doesnt-anyone-use-it/

[11] For instance Dell, IBM, Oracle, SafeNet, Thales e-Security and Vormetric.

[12] Lemos, R. (2014) 'Keypocalypse' another barrier to encryption systems, http://searchsecurity.techtarget.com/feature/Keypocalypse-another-barrier-to-encryption-systems, accessed on 4 November 2014.

[13] See also Part 1 of this study, where it is stated that encryption is among the top 10 Internet challenges for law enforcement (according to the findings of the World Middle East 2014 conference Telestrategies).

[14] BBC.com 'Only 100 cybercrime brains worldwide, says Europol boss, http://www.bbc.com/news/technology-29567782, accessed on 27 October 2014.

[15] See bbc.com (2014) and repeated during a keynote speech at The Grand Conference 2014, 6 November in Rotterdam.

new customer data encryption standards adopted by Apple and Google that could hamper FBI surveillance efforts.[16]

For certain E2EE e-mail tools the service provider does not have the private keys to decrypt data and/or it is not located in a country which has the legal authority to obtain keys and/or user data. Paradoxically this then probably requires the monitoring agency to switch to targeted surveillance and thereby commit a deeper breach of privacy.

However, content that lies with large e-mail providers, even those with encryption facilities, is still within reach of government agencies if the provider also has the private key. A court order would probably be needed in most countries to gain access to the required data.

Finally, the secure e-mail providers Silent Circle and Lavabit both closed down e-mail services after the latter was ordered by a court to hand over the key for user data. This has forced the business to come up with new concepts and a drive to keep its data out of the hands of law enforcement agencies, arguing that they would otherwise lose the trust of those who fund their business.[17] In this way law enforcement successes are also fuelling (inherently legitimate) innovations to better protect E2EE.

Corresponding policy options

Improving adoption of E2EE in all sorts of applications can follow two paths: stimulating individual users and stimulating collective solutions.

Policy options targeted at increasing adoption by individual users:

Stimulate **awareness of the necessity of using encryption** by initiating a campaign, as research shows awareness of privacy risks is fairly low.[18] Also, privacy concerns are not always top of mind or considered acceptable grounds for surveillance (so the need for protection is low).

Stimulate **increased knowledge among end-users** through both individuals and responsible departments in organisations (public and private), by setting up an independent platform where users can find information on tools, implementation, dos and don'ts etc. Note that many tools can currently only be found by insiders and the trustworthiness of websites and tools is hard to guess for most users. Sourceforge is not the first place most users would look, except insiders who are already well informed.

Support independent tests by institutions such as the Electronic Frontier Foundation. These institutions also help users make better-informed choices.[19] Support can be a financial contribution, but also promotion of the work done and its results.

A parallel option is to **stimulate the user-friendliness of E2EE solutions**, for instance by promoting existing user-friendly platforms. We do think that developers are aware of this need in most cases, but, as

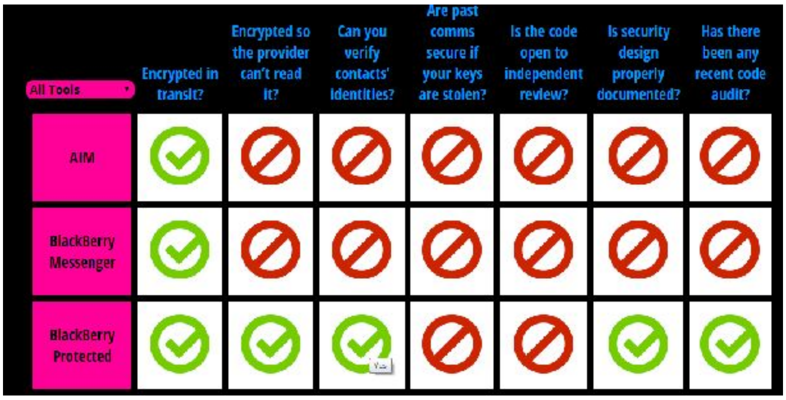
[16] Speech by James B. Comey, Director of Federal Bureau of Investigation, Brookings Institution, Washington, D.C., 16 October 2014, http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course (accessed on 6 November 2014). In the same sense Commissioner Bernard Hogan-Howe of the Metropolitan Police on 6 November 2014, see: http://content.met.police.uk/News/Commissioners-US-visit/1400027598397/1257246745756

[17] Levison, Ladar and Stephen Watt, Dark Mail, presentation on DefCon 22, 10 August 2014, http://www.youtube.com/watch?v=TWzvXaxR6us, accessed on 17 October 2014.

[18] Renaud K. et al., Why Doesn't Jane Protect Her Privacy?, paper for The 14th Privacy Enhancing Technologies Symposium, Amsterdam 2014.

[19] https://www.eff.org/secure-messaging-scorecard (accessed on 12 November 2014).

in all technology projects, they struggle with the balance between performance and usability. Dedicated **funding or participation** in OSS E2EE solutions is also an option to specifically improve user-friendliness.



All Tools	Encrypted in transit?	Encrypted so the provider can't read it?	Can you verify contacts' identities?	Are past comms secure if your keys are stolen?	Is the code open to independent review?	Is security design properly documented?	Has there been any recent code audit?
AIM	✓	⊘	⊘	⊘	⊘	⊘	⊘
BlackBerry Messenger	✓	⊘	⊘	⊘	⊘	⊘	⊘
BlackBerry Protected	✓	✓	✓	⊘	⊘	✓	✓

Figure: part of security test of various communication products (source and full test results at: https://www.eff.org/secure-messaging-scorecard)

However, as the lack of user-friendliness is far from the only reason for slow adoption, it seems to be more promising to invest in awareness, knowledge and independent tests. The latter can of course include user-friendliness; otherwise with a larger (non-specialist) user base, user demand will probably steer requirements towards better user-friendliness.

Policy options targeted at collective adoption

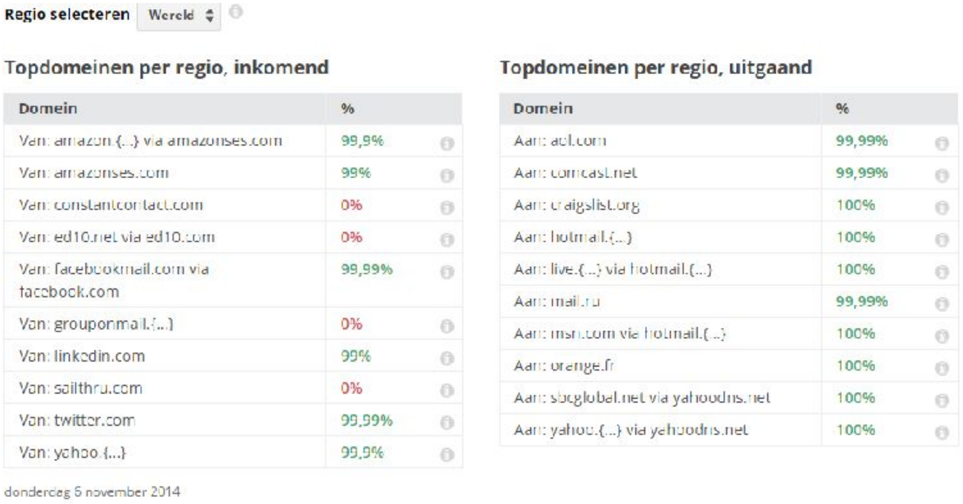
When users are not aware of the need or are not capable of implementing sufficient protection, service providers can offer a 'collective' solution, unburdening the users (who will usually use what is on their computer anyway). Options identified are:

Rely on the market to adopt E2EE solutions under pressure from the Snowden revelations. There are many examples: Google introduced a Chrome extension in 2014, called End-to-End, which uses OpenPGP and can be used by people requiring extra security or for sensitive e-mails. Using the extension, anyone can send and receive end-to-end encrypted e-mail through their existing web-based e-mail provider.[20]

Reports such as that illustrated below (Gmail encrypted mail) also inform the public about many more providers than just Gmail. One of these periodic reports demonstrated that Apple was (quietly) switching to TLS encryption for e-mails in transit from and to its iCloud.[21] Market pressure is apparently working for US service providers, as they fear losing market share in the post-Snowden era.

[20] Rosenblatt, Seth (2014), 'New Chrome extension hopes to demystify encryption', http://www.cnet.com/news/new-chrome-extension-hopes-to-de-mystify-encryption/, accessed on 13 July 2014.

[21] Threatpost, Apple Implements Email Encryption for iCloud, http://threatpost.com/apple-implements-email-encryption-for-icloud/107285, 17 July 2014 (accessed on 12 November 2014).



Regio selecteren Wereld

Topdomeinen per regio, inkomend

Domein	%
Van: amazon.{...} via amazonses.com	99,9%
Van: amazonses.com	99%
Van: constantcontact.com	0%
Van: ed10.net via ed10.com	0%
Van: facebookmail.com via facebook.com	99,99%
Van: groupon mail.{...}	0%
Van: linkedin.com	99%
Van: sailthru.com	0%
Van: twitter.com	99,99%
Van: yahoo.{...}	99,9%

Topdomeinen per regio, uitgaand

Domein	%
Aan: aol.com	99,99%
Aan: comcast.net	99,99%
Aan: craigslist.org	100%
Aan: hotmail.{...}	100%
Aan: live.{...} via hotmail.{...}	100%
Aan: mail.ru	99,99%
Aan: msn.com via hotmail.{...}	100%
Aan: orange.fr	100%
Aan: sbcglobal.net via yahoodns.net	100%
Aan: yahoo.{...} via yahoodns.net	100%

donderdag 6 november 2014

Figure: percentage of encrypted e-mails to and from Gmail (source: http://www.google.com/transparencyreport/saferemail/, Dutch version[22]*). More than 99.99% of all e-mails sent from Gmail to top domains are encrypted (with Transport Layer Security (TLS)*[23]*). E-mail sent to Gmail from major platforms like Twitter and LinkedIn is usually encrypted, although traffic from many top domains is not.*

This 'collective' approach by different service providers does increase protection against cybercrime. It does not eliminate the possibility of mass surveillance entirely, unless the service provider does not have the decryption keys. Otherwise LE authorities can still require access.

If the market does not provide security with E2EE by itself, **regulation** could be considered, obliging service providers and/or ISPs to provide end-to-end protection for data in transit. Given the costs associated with encryption and the lack of a solid business model, this is an option worth considering. An additional benefit of regulation would be a thorough and concrete political discussion on the balance between privacy and law enforcement and national security, at European (EU) and/or national level.

Conclusions

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

On the other hand, collective options are much more promising in terms of numbers of users. E2EE raises the general level of security, although not 100% as authorities can probably request access. However, given the slow adoption by individuals, the collective road is preferable. The invisible hand of the market is already forcing US service providers (such as Google, Apple, Amazon, Facebook, Twitter and LinkedIn) to implement E2EE. Should these market dynamics stall, regulation should be considered. Otherwise stimulate European service providers to follow the examples already available (or lose market share).

[22] As found on http://www.google.com/transparencyreport/saferemail/ (accessed on 7 November 2014).

[23] Basic information and IETF references can be found at http://en.wikipedia.org/wiki/Transport_Layer_Security

2.1.2. Stimulate open-source software life cycle management processes

Development and adoption of open-source software (OSS) is a recurring recommendation in security and privacy discussions.[24] The rapid growth of the Internet has created the prerequisite for numerous OSS communities and widespread use. The collaborative effort of those communities has generated alternatives for almost all proprietary (also known as closed-source) software.

From a security and privacy perspective the attractiveness of OSS lies mainly in the openness of the source code: anyone can review it and propose a fix for any problems encountered. The drive to publish identified vulnerabilities is not hampered by the vendor's reputational fear and in fact publishing is encouraged. Major open-source applications might also have 'owners' with reputations to protect.[25]

According to Anderson[26], vulnerabilities found by a vendor might be withheld from the public because they are disclosed to national governments for exploitation. Only when outsiders (e.g. other governments, cybercriminals) start exploiting the vulnerabilities does the vendor start shipping patches. In this sense, OSS and the way it is supported by communities (code checking/review) can help with finding, removing and even preventing backdoors enabling mass surveillance in widely used software.

Besides this, OSS also has the potential to decrease the EU's technological dependence on especially US vendors, with all the attendant advantages in terms of security and privacy. Investing in European OSS instead of in licences of US vendors could mean billions of euros of stimulus for the European software industry.

Bias, bias and statistics

But how secure is OSS when looking at the facts? Discussions around OSS tend to be determined by the bias of the participants, even if empirical data does not justify their claims.[27] In most studies on this subject, no significant empirical differences in security between open- and closed-source software appear. In some cases, however, the researcher finds empirical results arguing that "compared with closed source software, vulnerabilities in open-source software: (a) have increased risk of exploitation, (b) diffuse sooner and with higher total penetration, and (c) increase the volume of exploitation attempts."[28] The level of vulnerabilities (or their absence) therefore does not seem to be the primary reason to pitch for OSS as a security measure. It is interesting that the discussion is continuing, even though these and other empirical findings are over ten years old.

[24] This includes the LIBE committee report 'on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs'(2013/2188(INI)), published in 2014.

[25] Wheeler, Dick, Secure Programming for Linux and Unix HOWTO. Chapter 2, Is Open Source Good for Security?, 2004.

[26] Anderson, Ross, Security in Open versus Closed Systems. The Dance of Boltzmann, Coase and Moore, Open Source Software: Economics, Law and Policy, Toulouse, France, 20-21 June 2002.

[27] Schryen, G., Security of Open Source and Closed Source Software: An Empirical Comparison of Published Vulnerabilities, AMCIS 2009 Proceedings, Association for Information Systems 2009. Likewise Anderson 2002 and Iyengar, Kishen, A Security Comparison of Open-Source and Closed-Source Operating Systems, 2007.

[28] Ransbotham, S., An Empirical Analysis of Exploitation Attempts based on Vulnerabilities in Open Source Software, Workshop on the Economics of Information Security, June 2010.

Processes are key

It is important to keep in mind that it is not the difference between open and closed source that determines the level of security, but much more the quality of the lifecycle management process.[29] Factors that influence this quality include:

- How rigorous is code reviewing and testing?
- How many versions are currently in the market and supported?
- Are security and privacy key interests of the supporting community?
- And of course the size and level of expertise of the community.

Example of Android vs iOS: open does not necessarily mean more secure[30]

Symantec's 2013 Mobile Threat Report revealed 387 documented vulnerabilities in Apple's iOS software, compared to a mere 13 on Android. However, despite Apple's higher iOS vulnerability score, Android remained the leading mobile operating system in terms of the amount of malware written for it in 2012 because it is more open and less restrictive than Apple's iOS and has a much larger market share.

In fact, while Apple's iOS had the most documented vulnerabilities in 2012, there was only one threat created for it. In the case of Android, although only 13 vulnerabilities were reported, it led all the mobile operating systems in the amount of malware written for the platform. It said 32% of those attacks were hackers attempting to steal information such as e-mail addresses and telephone numbers, showing that a growing number of malware authors are looking to commit some form of identity theft.

The differences in lifecycle management processes play an important role. It appears to be far easier to push infected apps through the Google Play app store than through Apple's App Store.[31] Also, attackers benefit from the fragmented Android ecosystem (lots of current versions) that stops the vast majority of devices receiving new security measures. That leaves users exposed, even to known and documented threats.

The OSS lifecycle management process, with its openness and communities, has its advantages, but also its challenges, for which some level of support might be in order.

Key players involved and challenges and opportunities

The key players for open-source software in general are:

- End-users, who in general do not participate in maintaining the software, although a limited number do and participate in the community. End-users can be individuals or organisations.
- Community members, who support the lifecycle of OSS through different roles (architect, designer, developer, code review or audit etc.)
- Commercial ICT providers who participate or even launch an OSS platform. Their business model financially enables them to support the lifecycle of OSS.

The development and maintenance (lifecycle management process) of OSS meets a number of challenges that need to be addressed:

- The quality of the review process in most cases depends heavily on the abilities (to read and write secure code) and availability of volunteers. These volunteers might work for companies, with OSS support forming part of their job description. Most often, however, they are truly (unpaid)

[29] See amongst others Anderson 2002.

[30] Based on Symantec's Internet Security Threat Report 2013, http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf.

[31] Juniper, Third Annual Mobile Threats Report 2013, 2013.

volunteers, with a dedication to OSS based on their own use of it. Heartbleed and other incidents could be detected earlier by auditing and checking code. TrueCrypt is a typical example of a problem of the commons: worldwide use of software package was probably dependent on two or three developers. The Tor project also relies on very few people to audit its security features: only one.[32]

- OSS in more exotic programming languages, or niche or rarely used applications, might not attract a community large and/or expert enough to maintain the application and its security. Even widely used OSS such as (once) TrueCrypt or OpenSSL have fairly small support communities that require support in terms of extra volunteers or funding to maintain their work.
- Frankly speaking, reviewing and testing code can be boring. For many developers it is much more attractive to (just) fix what annoys them in the software. The position may be slightly different for commercially distributed OSS, where above-average rigorous maintenance processes are deployed because the vendor has a (usually limited) liability for its products and a reputation to protect.
- As mentioned above, an attacker does not necessarily need the code to find vulnerabilities. Like closed source, OSS also benefits from penetration testing.
- Distribution of fixes and feedback to the developers on found vulnerabilities are crucial. Likewise the installation of fixes on end-user devices of course, but this is quite similar to closed source (assuming that the OSS in question has a user-friendly, automatic update mechanism).

Corresponding policy options

Although it is not a universal remedy, OSS is still an important ingredient in an EU strategy for more security and technological independence. The quality of the support processes of OSS is crucial to its security, however, and these support processes face challenges that cannot be solved without outside support.

Support and fund maintenance and/or audit of important OSS platforms: open-source initiatives, some of them widely implemented in very important systems, such as OpenSSL[33], TrueCrypt/Ciphershed[34], GPG[35], Tor[36] , OwnCloud[37] etc. [38] need funding to keep going and be audited (with regard to both code and processes).

Initiate a European OSS Bug Bounty Programme or finance existing ones. Instead of intervening directly with specific OSS programmes, the EU could also set up a 'Bug Bounty' programme for some or all OSS platforms. A Bug Bounty programme is a deal offered by many open- and closed-source vendors of software to individuals who report vulnerabilities in their software. Rewards can range from (sometimes substantial) direct payments to money, T-shirts or inclusion in the Hall of Fame.

[32] https://blog.torproject.org/blog/thoughts-and-concerns-about-operation-onymous#comments

[33] https://www.openssl.org/

[34] www.ciphershed.org. At the time of writing, the first version of CipherShed was in development, "rebranding" the TrueCrypt 7.1a code. TrueCrypt itself was discontinued as of 28 May 2014.

[35] https://www.gnupg.org/

[36] https://www.torproject.org/

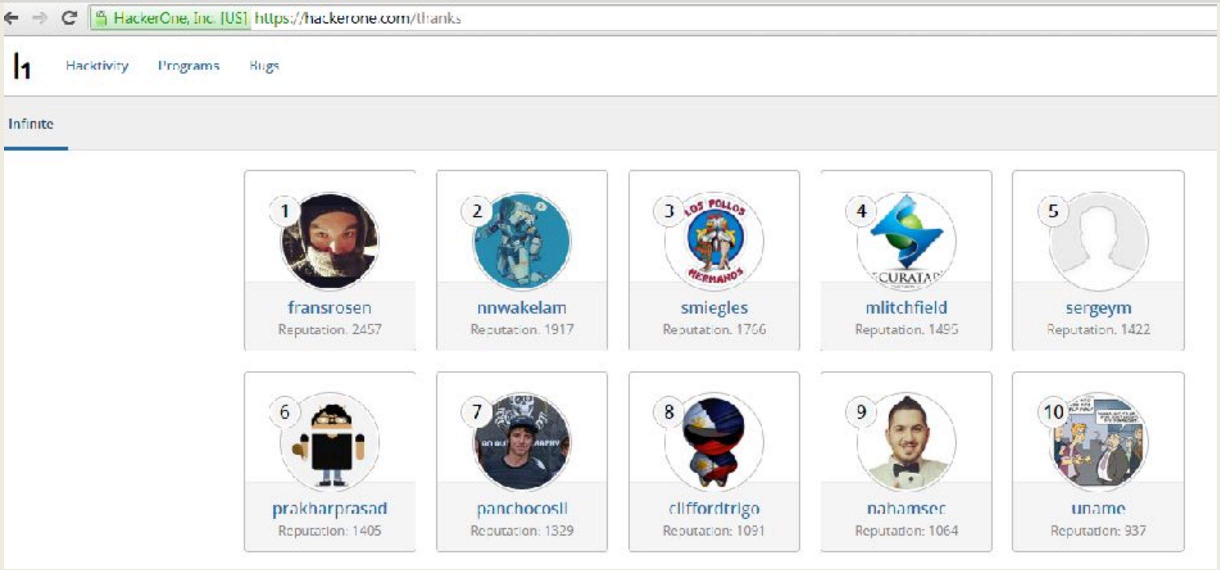
[37] https://owncloud.org/

[38] This list does not mean the research team endorses this or any other OSS specifically, nor does the European Parliament. The list is also incomplete; the names mentioned are just examples. More and better alternatives may be available.

Existing Bug Bounty programmes

Hundreds of bounty programmes are active. These include the programmes of specific vendors/platforms, such as Facebook, Microsoft, Mozilla, 4chan, AirBNB, Adobe, Amazon, Apple, the Internet[39] and others. [40]

In some cases a bug bounty programme is started to remedy a specific issue with specific software or a combination of software.[41]



1 fransrosen Reputation. 2457
2 nnwakelam Reputation. 1917
3 smiegles Reputation. 1766
4 mlitchfield Reputation. 1495
5 sergeym Reputation. 1422
6 prakharprasad Reputation: 1405
7 panchocosil Reputation: 1329
8 cliffordtrigo Reputation: 1091
9 nahamsec Reputation: 1064
10 uname Reputation: 937

Figure: the Hall of Fame - 'thanks' page on Hacker One, status 17 November 2014

Platforms such as Hacker One[42] combine dozens of programmes, to facilitate both bug hunters and software communities. Since its start in 2013 4,719 bugs have been fixed, $1.49 million of bounties paid and 971 hackers thanked in 70 public programmes.

Given the widespread nature of bug bounty programmes, a new program would not be preferable. Financial support (even small) can be enough to keep promising programmes going.

Rather than fixing, it is better to work more securely from the start. **Promoting secure software development guidelines** for all sorts of open and closed software is therefore an option that is very worthwhile considering. This should include distribution (to and from developers and to end-users). Security by design also applies to OSS.

The setting up of certification schemes for specific critical types of OSS, potentially supported by technical tests (e.g. penetration tests), could be considered. A recommendation supporting this would be to set up an agenda of critical OSS for the EU.

[39] https://hackerone.com/internet, accessed on 17 November 2014.

[40] See for instance: http://www.bugsheet.com/bug-bounties and https://bugcrowd.com/list-of-bug-bounty-programs for lists of current Bug Bounty programmes and their rewards.

[41] Example at: https://bitcointalk.org/index.php?PHPSESSID=nklrdn90ip5rq3m3enprac9154&topic=337294.0;all

[42] https://hackerone.com/. This website is sponsored by individuals and organisations such as Microsoft and Facebook.

Conclusion

OSS has many advantages. From a security and privacy perspective the attractiveness of OSS lies mainly in the openness of the source code. However, the mostly volunteer-based lifecycle management processes prove to be vulnerable, especially with regard to security reviews. Even OSS platforms that aim to increase security, such as TrueCrypt or Tor, are vulnerable in that sense. Without financial support or otherwise sponsored manpower for secure lifecycle management and certification, such platforms face substantial risks and cannot guarantee the security and privacy of their users any more than closed-source platforms can.

2.1.3. Promote and/or stimulate European Cloud services: Cloud, social media, search engines

As more and more countries are developing services that can operate (if required) separately from the Internet[43], it is logical to have an EU-wide focus on the question of whether it is desirable to develop specific, European Internet-related services. China leads the race in developing social networking sites as alternatives to US platforms. YouTube, Facebook and Twitter are blocked in China, but their Chinese equivalents are expanding. China is able to produce alternatives for each of the famous US social networks, such as Youku for YouTube, Sina Weibo for Twitter and QZone for Facebook etc. By some measures, the use of Chinese social media is among the most intense in the world. The user base in China has increased so enormously that even if Facebook is allowed in China, it may not prove to be dominant in the current scenario.

What is being proposed?

One of the main Snowden revelations about the NSA is the fact that major American companies are – willingly or unwillingly – the subject of major tapping operations[44]. Moreover, the grounds for this are legal, since the FISA court has approved the actions of the NSA in this regard, especially in the case of non-US residents[45]. The idea of developing own versions of services has been quietly promoted by countries in the form of separate social networks, search engines and the like.

Rank	Name	Registered users	Active user accounts	Date launched	Country of origin	Date of user stat.
1	Facebook	1.6+ billion	1.32 billion	February 2004	United States	June 2014
2	Tencent QQ	1+ billion	829 million	February 1999	China	August 2014
3	Tencent Qzone	712+ million	645 million	2005	China	August 2014
4	WhatsApp	700+ million	600 million	June 2011	United States	August 2014

[44] The Guardian (2014), 'Putin considers plan to unplug Russia from the internet 'in an emergency'', http://www.theguardian.com/world/2014/sep/19/vladimir-putin-plan-unplug-russia-internet-emergency-kremlin-moscow

[44] The Guardian (2014), 'NSA Prism program taps in to user data of Apple, Google and others', http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (accessed on 5 October 2014).

[45] European Parliament (2014), 'The US Surveillance programmes and their impact on EU citizens' universal rights', pp. 16-19 http://www.europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL-LIBE_NT(2013)474405_EN.pdf

Rank	Name	Registered users	Active user accounts	Date launched	Country of origin	Date of user stat.
5	Google+	1+ billion	540 million	June 2011	United States	October 2013
6	WeChat	600+ million	438 million	January 2011	China	August 2014
7	Skype	663+ million	300 million	August 2003	Estonia	March 2014
8	Twitter	500+ million	271 million	March 2006	United States	July 2014
9	Instagram	300+ million	200 million	October 2010	United States	March 2014
10	LINE	490 million	200 million	June 2011	Korea	July 2014
11	Baidu Tieba	1 billion	200 million	December 2003	China	December 2013
12	Sina Weibo	503+ million	156 million	August 2009	China	August 2014
13	Viber	300 million	105 million	December 2010	Israel	February 2014
14	YY	300 million	100 million	December 2010	China	August 2014
15	VK	270 million	100 million	September 2006	Russia	September 2014

Table: list of virtual communities with more than 100 million active users[46]

From the above data, it can be inferred that US and Chinese social networking websites lead the race in the user base when compared around the world. The same applies to Cloud computing services. There are many reasons for this, and security is definitely one of them. Other reasons include user satisfaction and ease of customisation. The user base of these networks is far ahead of other countries.

The idea of European (EU) Cloud services is subject to some differentiation, however: it is not always clear (even from the EC's own Cloud Strategy[47]) if this means specific European services or just a differentiation by which data is only used in the EU. For instance, several commercial service providers which operate worldwide offer European Cloud services, in the sense of localised data. In the context of this paper, European services are described as services operated under European law, and where all the data is stored and used within the EU.

The idea of independent or anonymous services has always been popular in tech circles, where the NSA revelations led to the search for alternative services, such as DuckDuckGo as a search engine and, more recently, Ello as a social network. The use of these alternatives has nevertheless been limited so far. However, the rise of social media such as Yammer, which offers corporate accounts for a Twitter-like medium, suggests that secure applications can be adopted first in a corporate (or government) environment.

[46] Multiple sources, assembled on: http://en.wikipedia.org/wiki/List_of_virtual_communities_with_more_than_100_million_active_users, accessed on 9 October 2014.

[47] European Commission, Unleashing the Potential of Cloud Computing in Europe, 2012, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF, accessed on 2 October 2014.

There are some movements towards open-source cloud solutions, as in services such as OpenStack, an open-source IaaS solution. However, as is demonstrated by the recent acquisition of Eucalyptus, an open-source Cloud provider, by the US firm HP[48], open source is no guarantee of non-US involvement. In the context of this policy option, using open source is seen as one of the ways in which independence from globally operating and integrated services could be achieved. However, the main focus is on developing separate European services.

Why should a European Cloud, social media and search engines be promoted?

From a security standpoint, there is much to be said for operating separate European services.

Rule of Law. EU citizens are considered third parties under US law. In other countries where the rule of law is even less well defined, the position of EU citizens who use services is even less certain. If services are specifically targeted at EU citizens and visitors and data is only collected and stored within the EU, compliance with EU law is more easily enforceable.

Independence. Since the tech world is a highly volatile market with lots of acquisition, the service a user signs up for today may be acquired by a different company tomorrow. Setting up standards for services aimed specifically at the European market would provide a certain measure of independence from these market movements (although agreement will still ensure access by acquired services to the European markets).

Accountability. Basing users and user data in Europe ensures accountability, in the sense that there is no risk of takeovers affecting legal ownership of user data. Offering European Cloud services or a search engine will mean that operations must be based in a European country and thus be compliant with its laws and the European framework of laws and guidelines.

What are the limitations and drawbacks of offering European services?

Market inefficiency. The most obvious drawback of the scenario of developing European social media is that it will create market inefficiencies. Foreign players being unable to operate in Europe or differentiating their service for European users will mean unnecessary hurdles to business and innovation. Moreover, European services being unable to expand beyond their home turf will hamper growth and innovation within the European market.

Lack of demand. The appeal of the currently popular Cloud services, social media and search engines lies in the fact that they are a) the best (or interchangeably the best) service available and b) usually more importantly, widely used.

Problems with use outside Europe. Numerous interoperability problems lie ahead in this scenario, both between devices, but more importantly between countries, once users start moving abroad.

Interdependence of hardware and software. If the idea of developing European services is to be free of foreign meddling, it is highly likely that this goal will be missed, because foreign hardware and software, as well as personnel, is integrated in every operation of major IT business and development. There is a very high likelihood that this is – or will be – equipped with backdoors or simply required to cooperate with local intelligence and law enforcement.

[48] Wired, 'HP Acquires Open Source Cloud Pioneer Eucalyptus', 11 September 2014, http://www.wired.com/2014/09/hp-eucalyptus/

'Balkanisation'. The idea of 'cutting up' the Internet and its services goes against the very ideas that propelled the Internet and have fuelled EU policy towards a 'free, open and secure' Internet.

Installed base. Many companies and consumers have adopted US-based Cloud services for their business, communication or leisure. It would take a substantial effort to transfer their data, social networks etc. to a different platform.

Limited effect against mass surveillance. In the case of Google and Yahoo, public reports indicate that the NSA tapped directly into communication links to gain access to user information, including that passing to and from overseas data centres.[49] Only protecting European datasets in Europe or implementing strictly European Cloud services does not provide any guarantee against such practices, especially when European intelligence agencies cooperate with foreign agencies.[50]

Key players involved

In the context of the European Cloud Strategy, the European Commission spoke with many key players. (CloudSigma, Microsoft, ATOS, IBM, Alcatel-Lucent, SAP). Although some of these players are US-based, there is an established European IT market, as well as a booming startup culture in parts of Europe. A report released by the European Commission in 2014 maps the EU's top ICT hubs[51] and suggests healthy prospects for both business and R&D. In this sense, finding parties to develop these services should not be too hard – although its development should be a top priority. In fact, being able to develop services within the European market might help counter the monopolising nature of current market trends by encouraging the development of competing services without them being bought or crushed by their competitor.

Another group of key players consists of the incumbent Cloud services providers, such as Microsoft, Google, Facebook, LinkedIn, Amazon, eBay, AliBaba and others. They have a stake in maintaining the status quo. The US-based service providers feel the market pressure in the sense of loss of trust due to the Snowden revelations. Their fear is a loss of market share caused by government actions and some are urging their legislators to ensure more transparency[52] and more protection for (US) citizens.[53]

Corresponding policy options

Because of the reasons mentioned above, developing a purely consumer-market-oriented approach to European social media and Cloud services seems a desirable option to explore. Although a completely separate market seems highly unlikely, stimulating the development of European services is at least desirable from a security perspective. There are several ways to encourage this:

Support further development of EU ICT Hubs. Identifying ICT Hubs can be seen as a useful way to develop instruments for stimulating ICT development in products such as apps or software, as well as

[49] The Guardian (2014), 'NSA Prism program taps in to user data of Apple, Google and others', http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (accessed on 5 October 2014).

[50] See for instance: Süddeutsche Zeitung, BND leitete Telefondaten an NSA weiter, 24 June 2014, http://www.sueddeutsche.de/digital/geheimdienste-bnd-leitete-telefondaten-an-nsa-weiter-1.2016504

[51] European Union (2014), EU Atlas of ICT Hot Spots, http://is.jrc.ec.europa.eu/pages/ISG/eipe/atlas.html, press release at http://europa.eu/rapid/press-release_IP-14-435_en.htm

[52] AOL et al., USA Freedom Act Letter, 31 October 2013, http://sensenbrenner.house.gov/uploadedfiles/usa_freedom_act_letter_10-31-13.pdf

[53] Fedscoop, Microsoft champions Internet privacy, calls on Congress to act, 24 June 2014, http://fedscoop.com/microsoft-calls-congress-act-privacy/

research capacity. Developing a funding programme for research and development of small business and innovative research in top ICT spots aimed at European services has a high likelihood of success, due to the encouraging environment.

Develop governmental blueprints and initiatives for using European-based Cloud services, social media or search engines within governmental agencies. The European Cloud Strategy and the *Cloud for Europe* projects are prime examples of the EU pioneering the adoption and use of services within EU institutions and stimulating EU-wide use. Stimulating the adoption of other European services and accompanying policies for data protection within the EU will stimulate wider use within the EU.

Conclusion

In the EU context, developing Europe-only services for the Cloud, social media and search seems unlikely. Due to the EU's own regulatory priorities and Member States' proclivities, there is no prospect of fostering an ecosystem separate from the world economy. However, by encouraging the development of an industry that is at least partially independent of foreign regulation, the most excessive mass surveillance practices could be mitigated. By encouraging EU ICT hubs to develop further and by encouraging the adoption of EU-based technology, some steps can be taken towards making the IT industry more independent and accountable.

2.1.4. Promote secure software development

In essence, the opportunity for cybercrime, digital espionage and illegitimate surveillance has its origin in flaws in software. Software is defined broadly here to include Internet protocols, firmware, encryption standards, operating systems, browsers, business applications, social media and Cloud platforms. On this basis, no vulnerabilities in software means no cyber attacks.

In an intriguing presentation, professor Daniel Bernstein pointed out that despite this fundamental truth, efforts to achieve secure software are distracted by all kinds of other security initiatives focused mainly on detection and reducing impact.[54] In his thought experiment, he constructs a way in which software stays insecure by distracting managers and system administrators with controls such as virus scanners, security management frameworks, risk assessments, intrusion detection systems, awareness and others. Likewise, programmers can be distracted with low-latency software updates and marketing ('new version is more secure!'). Researchers are distracted from fixing vulnerabilities by demanding the actual damage ('how bad is this really?'). And ultimately, security professionals discourage insecurity by stating that there is no such thing as 100% security. Combined with the assertion that security is hard to define (thus discouraging the programmer), this leads to acceptance of software vulnerabilities.

All these activities and discouragements take away funding, time and attention from the basic source of insecurity.

In this study, at least three specific challenges for secure software are described:

- Backdoors in encryption standards;
- Internet protocols that do not meet confidentiality needs;
- Shortage of skills or capacity in OSS communities for security reviews.

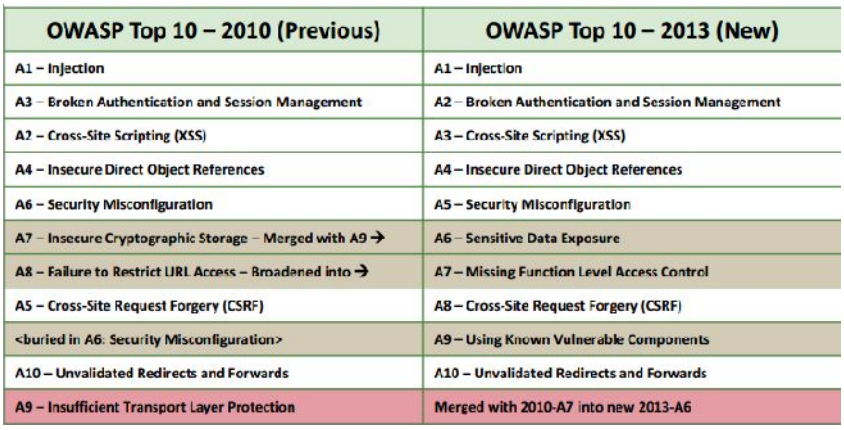
These challenges have their own specific solutions and options. This paragraph focuses on the overarching problem of insecure software.

[54] Bernstein, D.J., Money is not spent on more secure software, presentation on 10 July 2014.

Key players for security in the Software Development Lifecycle (SDLC)

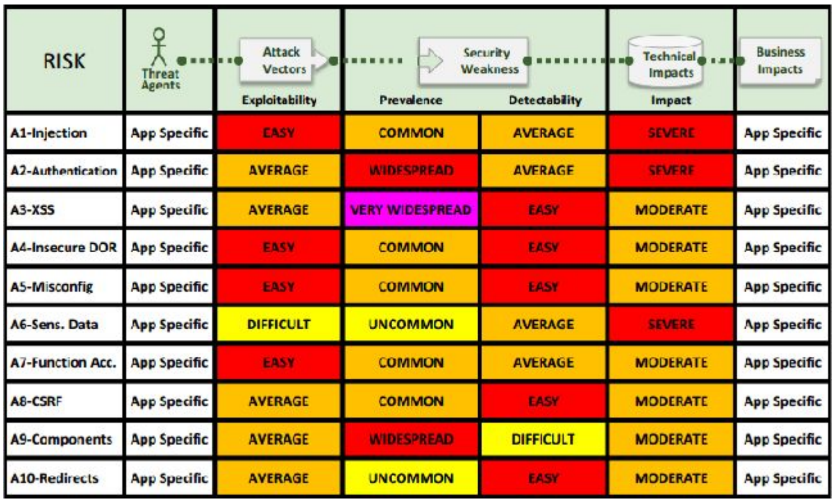
Security is a serious topic which should be given proper attention during the entire SDLC, 'right from the beginning'.[55] The question is how. Often software budgets are tight and requirements numerous. Security knowledge is also lower than desired, in our personal observation.

There are guidelines available for the most common problems. A good example is the so-called **OWASP** (Open Web Application Security Project) top 10[56] for secure web applications, which is periodically updated. This list describes the most vulnerable spots in web applications, based on attack patterns.



OWASP Top 10 – 2010 (Previous)	OWASP Top 10 – 2013 (New)
A1 – Injection	A1 – Injection
A3 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References	A4 – Insecure Direct Object References
A6 – Security Misconfiguration	A5 – Security Misconfiguration
A7 – Insecure Cryptographic Storage – Merged with A9 →	A6 – Sensitive Data Exposure
A8 – Failure to Restrict URL Access – Broadened into →	A7 – Missing Function Level Access Control
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
<buried in A6: Security Misconfiguration>	A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards	A10 – Unvalidated Redirects and Forwards
A9 – Insufficient Transport Layer Protection	Merged with 2010-A7 into new 2013-A6

Figure: OWASP top 10 – 2010 and 2013[57]



RISK	Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
		Exploitability	Prevalence	Detectability	Impact	
A1-Injection	App Specific	EASY	COMMON	AVERAGE	SEVERE	App Specific
A2-Authentication	App Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App Specific
A3-XSS	App Specific	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	App Specific
A4-Insecure DOR	App Specific	EASY	COMMON	EASY	MODERATE	App Specific
A5-Misconfig	App Specific	EASY	COMMON	EASY	MODERATE	App Specific
A6-Sens. Data	App Specific	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	App Specific
A7-Function Acc.	App Specific	EASY	COMMON	AVERAGE	MODERATE	App Specific
A8-CSRF	App Specific	AVERAGE	COMMON	EASY	MODERATE	App Specific
A9-Components	App Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App Specific
A10-Redirects	App Specific	AVERAGE	UNCOMMON	EASY	MODERATE	App Specific

Figure: OWASP Top 10 Risk Factors[58]

[55] Banerjee, C; S. K. Pandey, Software Security Rules: SDLC Perspective, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 1, 2009. Authors describe 21 rules for secure software.

[56] https://www.owasp.org/index.php/Top_10_2013-Top_10

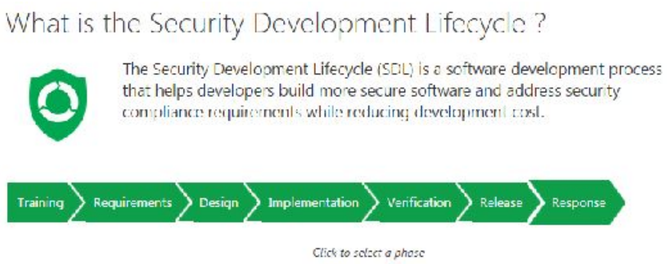
[57] OWASP, OWASP Top 10. The Ten Most Critical Web Application Security Risks, 2014.

[58] OWASP, OWASP Top 10. The Ten Most Critical Web Application Security Risks, 2014.

Well-informed lists such as the OWASP Top 10 help **programmers** to quickly define key risks and take appropriate action to make their software more secure, in this case web applications.

The current dominant practice, however, is still to identify issues by performing a security assessment of applications ***after*** they are developed and to fix these issues afterwards. Patching software in this way can help, but it is a costlier approach to address the issues than fixing them from the start.

The good news is that over the last few years security has made it to the programmer's desk. For instance, **major software developers** such as Microsoft[59] have improved their software development processes to address security concerns. This is largely due to the changing threat landscape and criticism of major players for security deficiencies.



What is the Security Development Lifecycle ?

The Security Development Lifecycle (SDL) is a software development process that helps developers build more secure software and address security compliance requirements while reducing development cost.

Figure: example of Security Development Lifecycle by Microsoft

Pressure from clients supports more secure software

In some cases, threats or publicity do not trigger more secure software, but client pressure. For instance, a group of Dutch government agencies devised guidelines for secure software development.[60] These guidelines derived from a need to have their own bespoke systems developed and maintained in a more secure way. **Software contractors** were consulted in that process to ensure feasibility. With the same purpose but for a broader public, OWASP is working on a Secure SDLC Cheat Sheet.[61]

This is an important step, because in the case of bespoke software the **client** is responsible for security, as he prescribes the requirements and budget. Prior to the guidelines, most clients did not recognise security as a subject at all, struggled with the requirements or left the issue entirely to contractors, expecting them to deliver secure software without agreement on what that should be (and without the budget to match security needs).

In the case of standard software, a slightly different situation applies. Here the **vendor** determines the specifications and budgets for security. See the Microsoft example.

Corresponding policy options

Stimulate the **use of existing guidelines** for secure software development, for example through the OWASP Top 10. Security is a job not just for 'Security', but for all staff involved in designing, developing, maintaining and exiting software.

[59] http://www.microsoft.com/security/sdl/default.aspx

[60] CIP Overheid, Grip op secure software development (SSD), 2014 (Dutch).

[61] https://www.owasp.org/index.php/Secure_SDLC_Cheat_Sheet

Stimulate the **wider distribution of guidelines or propose a European set of guidelines** for secure software development, drafted with the software industry.

Challenge **software suppliers in the EU** to adhere to secure software development guidelines, leveraging the buying power of the EU institutions. **Certification of software** as an ultimate challenge is also a policy option, but given the magnitude of software circulating and under development, this should probably start with a very specific focus. For instance browsers, operating systems and mobile apps.

The next step could be urging **product liability for software** to protect users from risks resulting from insecure software, risks they themselves can usually neither assess nor mitigate.

Conclusions

Secure software – in the widest sense – is key, but unfortunately (still) utopian. There is simply too much software; the amount is growing every day and an astounding number of vulnerabilities are involved.

The EU can stimulate secure software in general both by promoting guidelines and by leveraging its buying power. This will probably contribute to a shift in the mindset and an overall movement towards more secure software, more secure protocols and more secure encryption standards.

2.2. Build confidence: measures to improve trust between Member States

2.2.1. Security baselines

A security baseline defines a set of basic security objectives, which are pragmatic and complete but do not impose any technical (or other) means. The details of the fulfilment of these objectives are determined by the owner of a specific (IT) environment and depend on the characteristics of that environment. Derogations are usually possible and expected (but preferably explicitly).[62] Baselines do not cover strategy or public regulations, but offer guidance for tactical and operational measures in terms of people, process and technology.

Security baselines are well-known instruments for designing security in single organisations and industries (including the public sector). The objectives of baselines consist of topics (indicators, the 'what'), norms (standards, the level) and metrics (the 'how much' and 'how do we know/measure'). Such baselines usually build on market standards such as ISO2700x, which is considered best practice. ENISA drafted a shortlist of such information security standards in 2012.[63] Over the past two years, this list has grown significantly across the EU, with ISO2700x being transposed into national or industry standards.

Security baselines are considered a policy option for security in Europe

Given that networks and systems are interconnected and influence each other, fragmented approaches to security hinder the creation of trust among peers, which is a prerequisite for cooperation and information sharing. According to the draft NIS Directive (July 2013), there *"currently is no effective mechanism at EU level for effective cooperation and collaboration. (...) this may result in uncoordinated regulatory interventions,*

[62] Based on: https://security.web.cern.ch/security/rules/en/baselines.shtml

[63] ENISA, Shortlisting network and information security standards and good practices, Version 1.0, January 2012 https://resilience.enisa.europa.eu/article-13/shortlist-of-networks-and-information-security-standards

incoherent strategies and divergent standards. Internal Market barriers may also rise, by increased compliance costs for cross-border operating businesses".[64]

Earlier EU studies had already covered the subject of security baselines, as an option to improve e-government and e-health services, for instance: *"The development of such a baseline starts by outlining a security strategy on a political level that presents a roadmap of security measures for Europe. Implementing a security check list could be the short-term measure to start improving the level of security of eGovernment services. In the mid-term perspective it would be relevant to start looking at policy options that can achieve Security by Design of crucial components. In the long term, policy measures that push for highly secure entire IT systems become relevant."*[65]

This idea takes the idea of security baselines much further: from a true baseline with objectives to secure components to secure IT systems. The focus shifts from standardisation to certification, becoming much more detailed, much more compulsory.

This paragraph is restricted to the initial step, the checklist/standards as a confidence-building measure within organisations, between organisations in an industry or supply chain (or in an e-government context) or between Member States.

A good example of such a baseline as a confidence-building measure in a supply chain is the PCI-DSS standard[66], which defines security objectives for different actors in the chain of card payments (Point of Sale (device), merchant, service provider, acquirer). This helps establish secure transactions even if multiple different businesses are involved.

The draft NIS Directive is less far-reaching in its ambitions. Article 14(1) prescribes a risk-based approach for selecting appropriate measures, but the draft Directive does not refer to a specific set of measures or a specific standard. Using standards is encouraged, but the choice is left open:

"Article 16

Standardisation

1. To ensure convergent implementation of Article 14(1), Member States shall encourage the use of standards and/or specifications relevant to networks and information security.

2. The Commission shall draw up, by means of implementing acts, a list of the standards referred to in paragraph 1. The list shall be published in the Official Journal of the European Union."[67]

The open question in this case is whether this big step forward (harmonisation of security baselines across the EU) would provide more safeguards for privacy and security against unlawful mass surveillance.

EU security baselines do not necessarily offer protection against mass surveillance

As mentioned, a common EU security baseline aims to raise the general level of security in Europe, and several slightly more specific aims have been attached to the concept. Not all of these, however,

[64] For example ISO2700x has been translated in the Netherlands into separate security baselines for the central government (BIR), municipalities (BIG) and water authorities (BIWA).

[65] STOA, Security of eGovernment Systems - Conference Report, July 2013, http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/513510/IPOL-JOIN_ET(2013)513510(ANN02)_EN.pdf

[66] Payment Card Industry (PCI), Data Security Standard. Requirements and Security Assessment Procedures, Version 3.0, November 2013.

[67] European Commission, proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, 2013.

necessarily and specifically include mitigating mass surveillance risks; whether this is the case depends on the scope and objectives in the baseline.

The main benefits of security baselines would at least be improved co-operation across borders through a common understanding and language, better protection of 'weakest links' and easier (more uniform) auditing or other supervision.[68] By raising the overall level of protection, EU Member States and their citizens should become less attractive for attackers than less-protected countries. This is because the costs of surveillance, cybercrime or other attacks will rise. However, to genuinely offer more security and privacy against mass surveillance targeting the EU, specific objectives will have to be set and the accompanying controls rigorously implemented. Incorporating those specific objectives will probably be greeted with political discussion.

Market standards offer a good starting point for a generic EU security baseline

An earlier ENISA study pointed out that EU-wide security good practices (or baselines) should be based on ISO 27001/27002 standards, and if business continuity requirements are included, those could be based on BS 25999. The idea of different sets of requirements for different kinds of businesses can be adopted from PCI-DSS[69], although some of the implementation-enforcing mechanisms in the card payment industry are not available or not as strong in other sectors. Regulation is probably needed where the market system will not lead to spontaneous adoption of baselines.

For generic baselines the content will not be the main hurdle for implementation. That is partly because, according to the aforementioned study, ISO2700x is used extensively across the EU. The scope of this study did not, however, include a detailed comparison of all national and industry standards/baselines.

The scope of an EU security baseline is mainly a political challenge

Scoping is one of the first issues to tackle with baselines: what/who do the EU security baselines cover? Critical information infrastructure, including the Internet and other telecom backbone infrastructure? E-government systems? Financial services? All services providers for EU citizens? The broader the scope, the more stakeholders will be involved, the more complex decision-making will be. This scope would ideally match that of the NIS Directive[70], which was still under debate at the time of writing. The *current* regulatory framework only covers telecommunication companies.

In the end this is not a technical discussion, but a political one. In some cases facilities should be included to help mitigate the risks of mass surveillance. These include fixed and mobile telecommunications and Internet backbone facilities, but also ICT hardware and software, social media and (other) Cloud services. These are the services used extensively for producing, sharing, processing and storing massive amounts of personal data.

The digital world is dynamic, so baseline implementations should be too

Looking at the swift pace of developments in both technology and attack mechanisms, security can only be successful as an ongoing process, with continuous iterations to adapt to new circumstances. Any framework, standard or baseline should be able to be high-level enough to leave room for swift operational adjustments. This is the current practice with the standards mentioned earlier, which describe

[68] Based on ENISA 2012.

[69] ENISA (2012).

[70] European Commission, proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, 2013.

objectives. Organisations implementing the standard as their baseline put in the details and can adjust these according to a scheme that fits their needs (or possibilities). That scheme can range from years to months. The standards themselves are also periodically evaluated and adjusted to new times. ISO2700x, for instance, was revised between 2005 and 2013.

Following this train of thought, an EU security baseline needs to be both descriptive and high-level enough to give organisations room for manoeuvre and adjust to new threats. The EU baseline also needs to be periodically evaluated.

Compliance with baselines requires an accepted level of monitoring

A measure designed to achieve trust can only be trusted if it can be seen and checked. Earlier studies[71] therefore recommend that there should be some form of supervision and oversight of implementation at EU and Member State level. Performance metrics (for a common KPI dashboard) should be mandatory in Europe for benchmarking purposes. Different institutional set-ups of such supervision are possible and need to be evaluated. These set-ups are out of scope for this study, but the idea of oversight and supervision should be embraced. It is advisable to combine this role with participating in evaluation of the baseline itself, as the supervising authority or authorities will have a good overview of the workings of the baseline.

Beyond baselines: certification for ICT hardware

In general security baselines do not prescribe detailed security requirements for hardware and software. This would require a different instrument, which will be much more costly to implement and maintain. Certification of hardware and software is such an instrument.[72] In theory, the use of certified product evaluations or certified development processes could be made mandatory, but it will be very hard to enforce if components are produced outside the EU.

This latter statement is especially true for software. It can be ordered on the web, downloaded and installed with ease. Modern coding, programming and assembling tools allow millions of software producers, large and very small, to publish millions of lines of code on a daily basis. It is difficult to envision a situation where all (major) software in use within the EU is certified.

In the case of ICT hardware, the position is substantially different. It is much harder to design, produce and distribute hardware on a large scale. Importing and exporting hardware is also a physical process, with more opportunities for supervision and enforcement of regulations. We see a parallel with the automotive industry, where all new car models are examined and approved before going onto EU roads. In this process, approval by an authority or institute in one EU country leads to approval for all EU countries. This experience could be reused and adopted for the context of cyber security. Lastly, in order to ensure a level playing field and maximum security, certification should be implemented for ICT hardware, whether produced in or outside the EU.

[71] ENISA 2012, STOA 2013.

[72] STOA 2013

Key players involved

The corresponding key players for security baselines can be divided into three groups:

- Regulatory bodies or international standards bodies
  - National and supranational governmental agencies
  - Private bodies, such as ISO-IEC or national standardisation agencies
- Supervisory bodies (id.)
  - Governmental agencies (mostly national)
  - Independent (private) auditing and certifying organisations
- Implementing parties
  - Industries
  - Individual organisations
  - Consultancy firms

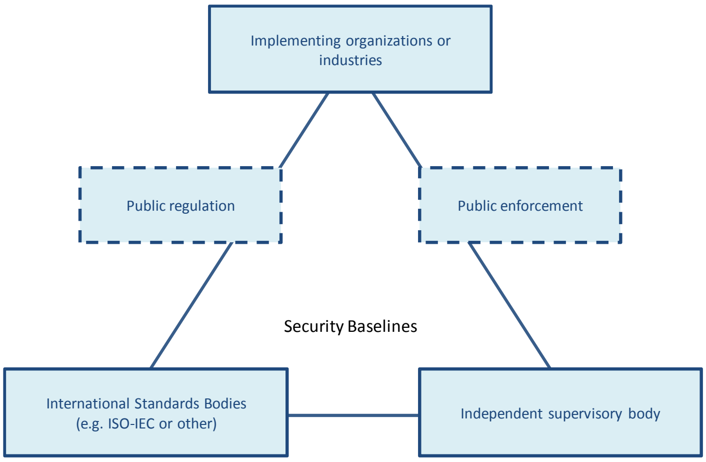

Implementing organizations or industries
Public regulation
Public enforcement
Security Baselines
International Standards Bodies (e.g. ISO-IEC or other)
Independent supervisory body

Figure: key players in security baselines

Their specific opportunities, challenges and barriers for implementation are described above.

The supply chain and battle of the baselines

One specific point of interest is the **supply chain**. In recent years, more security-mature organisations have started to impose security demands on their suppliers. An older example is the PCI-DSS baseline for payments, but in our observation single organisations such as oil and gas companies, defence ministries and financial institutions are also turning to the next weakest link in their defence after solving their own.

In itself this is a positive development, as many sophisticated data breaches show that suppliers are the primary targets for attackers. In a way the same actually applies to operators of mass surveillance.

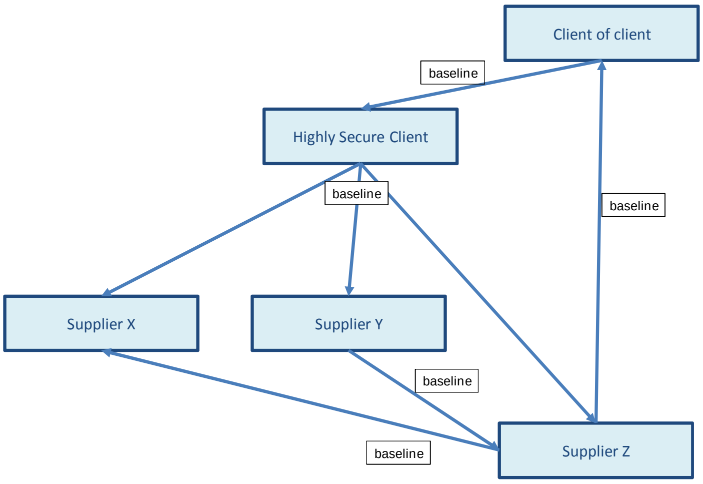


Figure: battle of the baselines

A complication arises when a supplier works for multiple clients (which most commercial firms do) and/or has its own security baseline. In the current network economy, this is a clear risk. A 'battle of the baselines' could emerge as a result, which is especially burdensome when baselines have non-matching or even conflicting demands. In the long run business will benefit from a more uniform set of baseline rules.

Corresponding policy options

Implement an **EU Security Baseline regulation** to build confidence by ensuring that a minimum level of security measures are implemented**.** To match interests between these three groups of key players, different policy arrangements can be implemented. The key question is how far public intervention should reach. Current baselines (including cross-sector ones such as PCI-DSS) are designed, implemented, maintained and supervised by private organisations, with very limited public intervention. But on both the regulating side (should we have security baselines and if so, which ones?) and the supervising side (are we sure relevant industries comply?), options for intervention exist. Various options are also available in terms of scope (which industries?). Both subjects could well be part of the discussions about the NIS Directive.

Conclusion

Security baselines are a foresight option in the sense that implementation is a long-term project. EU security baselines do not necessarily make the world a more secure place, but they do improve transparency between Member States and with regard to specific vulnerable industries. Thus security baselines are more about confidence-building between nations. But depending on the measures prescribed and the standards applying to each measure, baselines can raise the overall level of security, including against cybercrime threats.

Implementing baselines requires detailed discussions, however, on scope (what industries etc.), security measures to be covered and standards applying to each measure, but this is not completely new or innovative. The challenge is mainly a political one: an EU security baseline needs to be both concrete and high-level enough to serve all relevant industries and to adjust to technology dynamics. The Internet of Things, for instance, will dramatically change the scope of objects to be secured.

2.2.2. EU Coordinated Disclosure

Few organisations realise the potential of volunteers looking for software vulnerabilities. Mitigating existing vulnerabilities in information systems starts with finding them. Many people who are looking for vulnerabilities have good intentions and report them to the owner. Many organisations, however, do not know how to respond to these reports, or fixing vulnerabilities takes too long. Sometimes a report on a vulnerability even leads to legal action or threats towards the reporter. Some of these reporters can easily trespass legal boundaries, even though their intentions are good. This can lead to a situation where those with knowledge of vulnerabilities are unwilling to report them, which means they are not fixed. Not fixing vulnerabilities leaves the information in these systems at risk.

In the corporate world, the practice of coordinated disclosure has been in use for several years.[73] ISO standards have even been developed: ISO/IEC 29147 Vulnerability Disclosure[74] and ISO/IEC 30111 Vulnerability Handling Processes[75]. In the Netherlands, experience has been gained with a formal, government-sponsored procedure. The Dutch government realised the advantages of fixing the vulnerability to improve systems and prevent misuse. It published a guideline for both organisations and reporters of vulnerabilities.[76] The guideline encourages vulnerability reporters and organisations to work together on making information systems secure. Organisations should refrain from legal action against the reporter, and the reporter should report the vulnerability as soon as possible and not try to abuse the vulnerability.

Sometimes coordinated disclosure can fail to satisfy researchers, for example those who expect to get high financial compensation. Organisations such as Google offer high rewards for reporting vulnerabilities, up to €20,000[77], but this is not always the case. Reporting vulnerabilities with the expectation of high compensation might be viewed as extortion. Besides, researchers might be prosecuted or sued. This has been the case in some disclosures. An example of a coordinated disclosure comes from Radboud University Nijmegen, which broke the security of the MIFARE Classic cards in 2008.[78]

Although coordinated disclosure has existed for many years, the Dutch government's approach has been very successful. While in the past vulnerability reporters complained about being sued, they now complain that the reward is too low.

The most important topics to be addressed in a coordinated disclosure guideline are:

Organisation	Reporter
Promises not to take legal action.	Reports vulnerability as soon as possible and only to the organisation.
Offers reward to vulnerability reporter.	Accesses as little information as possible from the organisation.
Allows anonymous reporting.	Reports to a coordinating body when the organisation does not respond or is unwilling to cooperate.
Follows standardised procedure to make it easier to report.	

[73] See for instance: https://forms.cert.org/VulReport/, http://www.gpwebsolutions.co.uk/responsible-disclosure-policy/; https://www.braintreepayments.com/developers/disclosure; http://www.symantec.com/en/uk/security/ and https://www.airbnb.co.uk/help/article/550

[74] http://www.iso.org/iso/catalogue_detail.htm?csnumber=45170

[75] http://www.iso.org/iso/catalogue_detail.htm?csnumber=53231

[76] https://www.ncsc.nl/english/current-topics/news/responsible-disclosure-guideline.html

[77] http://www.google.com/about/appsecurity/reward-program/

[78] Radboud University of Nijmegen, Dismantling contactless smartcards, press release of 12 March 2008.

Key players involved

- European organisations, such as ENISA, to make guidelines for coordinated disclosure;
- National coordinators, which can act as an intermediary between the reporter and the organisation with a vulnerable system. The national coordinator can make sure that the vulnerability is addressed;
- All organisations that are using IT systems, to implement the guidelines for coordinated disclosure;
- The hacking community, to understand and apply the rules for coordinated disclosure.

Barriers to implementation can be the unwillingness of organisations to implement a coordinated disclosure guideline, e.g. because they are afraid they will attract hackers. To overcome this, organisations should be well informed about the guidelines and organisations that have implemented them successfully should convince others to do the same.

Corresponding policy options

EU **rules or guidelines for facilitating a process of 'coordinated disclosure'** would help discover and fix more software vulnerabilities, whilst protecting those disclosing within the rules. This would lead to more secure information systems and more secure information.

To implement this **an EU guideline on Coordinated Disclosure** should be published. To really make the guideline successful, it should be implemented by both public and private parties. Potential vulnerability reporters should be taught how to make a coordinated disclosure. A (trusted) coordinating body should ensure that reported vulnerabilities are fixed.

Conclusion

European coordinated disclosure is an interesting policy option that can be implemented easily, is very cost-effective and can quickly contribute to safeguarding the information of European citizens and organisations.

2.3. Disrupt(ive innovation): increasing EU technological independence

Two long-term options were identified that help mitigate structural risks deriving from European dependence on (for instance) American or Chinese hardware and software or communications. First, a better understanding of exactly what hardware and software is being shipped and validation that no backdoors have been installed. Second, creating an Internet Subnet, which in theory provides more control over what happens with communicated EU data. Both options tackle different issues and can be pursued independently from each other.

2.3.1. EU certification schemes

Encryption standards, hardware and software can all contain backdoors that facilitate mass surveillance. Currently no independent European (EU) institution inspects these technologies or sets technological standards for them. By comparison, in the automotive industry, the EU set up a solid framework for homologation decades ago: no car goes onto EU roads before approval. This approval only comes after extensive technical tests. Could this approach be used for encryption, hardware and software?

Independent encryption standardisation is necessary and feasible

For encryption, standardisation is paramount for open-market platforms. Encryption can only contribute to security if enough users actually trust and use the encryption standard. Currently most encryption standards are coordinated by the National Institute for Standards & Technology (NIST). But NIST is a federal agency within the US Department of Commerce, with a mission to promote US innovation and industrial competitiveness. Its security advice is primarily aimed at the US Federal Government, not the world. Furthermore, the NIST has admitted that it worked closely with the NSA in the development of cryptography standards.[79] Credibility has become an issue.

Several experts have therefore been very critical of the role and independence of the NIST in the recent past[80] and backdoors in encryption standards have been revealed.[81] These experts note that many communities blindly pass their security leadership to the NIST. This can lead to conflicts in the process if the NIST is focusing on specific things and other experts are not looking at all.

It should be noted that the NIST is currently in the process of redesigning its way of working with regard to encryption standardisation, in response to public concerns about the security of NIST cryptographic standards and guidelines. A proposal for the *Cryptographic Standards and Guidelines Development Process* (NISTIR 7977) was drafted, which has received both positive and negative appraisals.

The EU currently does not have an independent evaluator similar to the NIST. EU countries and organisations therefore often rely on the evaluations of the NIST, even though the EU has top cryptography researchers and research institutes.

As described in the next paragraph, there are advantages and disadvantages connected to EU encryption standardisation, but it is feasible and, given the domination of US interest in current standards, also necessary.

Hardware homologation is probably effective, but not feasible

Even for open hardware, it is very hard to prove that hardware has only the designed functions and that no malicious functions (like backdoors) have been added. To ensure this, the design and manufacturing processes and logistics are all required to be secure. In general, and certainly for mass production, this is almost impossible to do.

In theory, computer hardware types can be inspected and approved for use in the EU prior to import, just like cars.[82] Hardware homologation would raise the barrier for standard hardware for mass surveillance and require more targeted attacks, thus raising the costs and risk of detection.

This would not be a 100% barrier, as specific features of a type of hardware can be altered during transport to their – apparently critical – destination. Firmware can also be updated later, even online and in real time. After all, it is just software. The resulting homologation efforts to keep track of all hardware

[79] National Institute for Standards and Technology, NISTIR 7977 NIST Cryptographic Standards and Guidelines Development Process (Draft), 2014.

[80] Good examples can be found in NIST, Public Comments Received on NISTIR 7977: NIST Cryptographic Standards and Guidelines Development Process (Draft), 2014.

[81] New York Times, Secret Documents Reveal N.S.A. Campaign Against Encryption, 5 September 2013, http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?_r=1& (accessed on 20 November 2014) and The Register, NIST denies it weakened its encryption standard to please the NSA, http://www.theregister.co.uk/2013/09/11/nist_denies_that_the_nsa_weakened_its_encryption_standard/ (accessed on 20 November 2014).

[82] Not regarding any possibly existing legal obstructions (like trade agreements) for such an approval process.

and its corresponding firmware would be huge and frequent, raising market entrance barriers considerably. Inspection of hardware also requires scarce expertise. At this stage we therefore do not recommend a separate homologation process for computer hardware.

Software homologation is ineffective and not feasible

The import and export of software is much harder to regulate. Software flows in and out of the EU uncontrollably via the Internet. An approval process as suggested for hardware will not function for software, partly because almost every piece of software that is not end-of-lifecycle is (regularly) updated or patched. Frequencies and impacts may differ, but each change and each new release requires a new check. The sheer volume is considerable. All in all, approval of all software used in the EU is very impractical.

A focus on open-source software, where the code can be reviewed, and support of the code review process for critical platforms would be more advisable. See paragraph 2.1.2.

Process requirements for encryption standardisation[83]

Back to encryption standardisation: how could this be drafted to work and be credible? Based on the review conducted by the NIST and learning from comments on its draft document, the process for standardisation of encryption should be **systematic**, **open**, **transparent**, committed to well-defined **principles and processes**, and **responsive** to international or even global concerns.

Openness refers to the fact that anyone can participate in the process. Key stakeholders such as industry experts and academics should be invited. **Quality of review** is obviously a key component. Putting together one good standard, SHA-3, involved 200 cryptographers from around the world and took years of sustained public effort. Size does indeed matter; the cryptographic community has confidence in AES and SHA-3, thanks to the focused competitions that produced these standards. It is strongly recommended to wait for conclusive evidence of adequate public review, and abort standardisation if the public review does not produce a solid consensus.

Transparency of the process means, for instance, that cryptographic competitions are open, and evaluation criteria and their assessment are also clear. A security proof for standards should always be available when a standard is sent out for public comment.[84] Recording and immediately publishing all communication between the standardisation body and ALL external stakeholders would also improve transparency. This would reduce the risk of one-on-one input by intelligence services, especially when giving names and affiliations.[85]

Any changes to proposed algorithms or standard parameters should be fair and transparent, with check-ins with the larger community and a clear, documented rationale for the changes grounded in technical merit. The recent case of SHA-3's post-competition standardisation is an example of changes to algorithm parameters that proved problematic to a number of people in the cryptographic community.[86]

[83] Partially based on NIST, Public Comments Received on NISTIR 7977: NIST Cryptographic Standards and Guidelines Development Process (Draft), 2014.

[84] Access Now et al. in: NIST, Public Comments Received on NISTIR 7977: NIST Cryptographic Standards and Guidelines Development Process (Draft), 2014.

[85] Tanja Lange and also IEEE in: NIST, Public Comments Received on NISTIR 7977: NIST Cryptographic Standards and Guidelines Development Process (Draft), 2014.

[86] Joseph Lorenzo Hall, "What the heck is going on with NIST's cryptographic standard, SHA-3?," Center for Democracy & Technology (24 September 2012), available at: https://cdt.org/what-the-heck-is-going-on-with-nist%E2%80%99s-cryptographic-standard-sha-3/

This transparency is unending for security standards. The standardisation body should always be open to comments showing vulnerabilities in the published standards and commit to responding to such comments in public.[87]

Due process requires fair treatment of all stakeholders throughout the standards process, ensuring there are adequate opportunities for stakeholders to object to or amend certain decisions and that no stakeholder or set of stakeholders is disadvantaged or privileged throughout the process.

A standardisation body for encryption must also engage explicitly with **global interest**s, as these standards are the building blocks of security online and in digital environments. Even an EU standardisation body cannot prioritise EU interests without the risk of being blamed for the same things the NIST has been blamed for.

Standards and guidelines should be evaluated on the basis of **technical merit,** clearly and specifically defined, including the anticipated use model (mobile, server) as it drastically affects the technical merits.

Finally, the standardisation process itself has to be **secure** too, in the sense that it cannot be intentionally maliciously manipulated by outsiders.[88]

Key players involved

As encryption is a widely used security method, standardisation touches many stakeholders. A regional standardisation body is also a disruptive development. It changes the way security on the Internet is organised, shifting and/or fracturing encryption and the larger **security community**, including the **academic encryption community**. Instead of focusing on one informal world leader (NIST), they would have to split their attention or focus on one.

The **US Government** (and the NIST in particular) would not favour such a European (EU) regional development, although **US industry leaders** have warned that this could happen as the credibility of the NIST is dented.[89]

Fracturing cryptographic standards into different regional or national domains leads to negative effects on interoperability, according to Microsoft. This is a valid point, unless standards set by one regional body are also recognised by the other, under clear criteria. Different standards can exist side by side and need not derive from the same process owner. It is, however, a threat to US industry, as it would have to comply with non-US encryption standards as well. This could be potentially beneficial for **EU industry**, although both the threat to US Industry and benefits for EU industry are topics for further research.

To set up a systematic, transparent, open and technically solid process, the **EU and its Member States** should consider focused investments in setting up an **EU standardisation body** with sufficient expertise and capacity and an excellent network in the academic world and industry. Ideally such an EU standardisation body would align with the NIST and other national agencies on a process level (way of working) and principles, to avoid negative effects of regionalisation.

The role of **security and law enforcement agencies** is one to consider carefully. Experience in the US has shown that in order to balance the needs of intelligence gathering, substantial cooperation took place. In the end, this damaged the credibility of the (resulting) encryption standards, with the exception of those reviewed extensively in public (AES, SHA-3).

[87] Tanja Lange in: NIST 2014.

[88] D.J. Bernstein in: NIST, Public Comments Received on NISTIR 7977: NIST Cryptographic Standards and Guidelines Development Process (Draft), 2014.

[89] Microsoft and INTEL independently in: NIST 2014

Firstly, a thorough ***policy discussion on backdoors*** in encryption standards in Europe is required to define the principles. Secondly (but only after that discussion), participation of law enforcement and intelligence in defining standards is more than welcome. Encryption is not just a barrier in the fight against crime and terrorism; it also remains the best line of defence available against cybercrime and digital espionage. Solid encryption standards are therefore in the interest of these agencies too.

Corresponding policy option

The key policy option with regard to encryption schemes is to establish an **EU standardisation body or certification authority for encryption standards**. This organisation should have sufficient expertise and capacity and an excellent network in the academic world and industry. It should also operate on the basis of a systematic, transparent, open and technically solid process.

Ideally, such a European standardisation body would **cooperate internationally** with the NIST and other national agencies on a process level (way of working) and principles, to avoid the negative effects of regionalisation. A European standard should not raise barriers in international trade and should comply (if applicable) with the WTO code of good practice on standardisation.[90]

A thorough ***policy discussion on backdoors*** in encryption standards in the EU is required to maintain credibility when cooperating with law enforcement and intelligence agencies. This cooperation is desirable, but only with clearly defined principles based on the outcome of the policy discussion.

Conclusion

Fragmentation of standards is never a desirable thing. But in the case of encryption standards the reasonable doubts concerning the role of the US government justify the exploration of a European standardisation body. Such an EU body should be adequately equipped and learn from the good (and less than good) practices of the NIST and other (non-IT) standardisation bodies. International cooperation is also paramount to prevent negative effects of fragmentation.

Given an open and transparent process including the large encryption community, an EU standard will better protect EU interests, as implementation of backdoors would be seriously impeded.

2.3.2. European Internet Subnet

In the digital world, there are many ways for third parties to intercept traffic that is not addressed to them, legally or illegally. However, analysing in detail these huge volumes of digital data flowing permanently through IP networks worldwide is practically impossible. Interceptors need indications to filter potential valuable data packages from the large volumes of irrelevant data. This is more specifically relevant when data is encrypted, as decryption consumes time and processing power, even for highly specialised interceptors. But metadata is also relevant for legal reasons, because most lawful interceptors need metadata to justify to formal, responsible authorities the need to access the data content itself.[91]

[90] World Trade Organization, Agreement on Technical Barriers to Trade, Annex 3: Code of good practice for the preparation, adoption and application of standards, http://www.wto.org/english/res_e/booksp_e/analytic_index_e/tbt_02_e.htm#ann_3. If this code of good practice is applicable as a legal judgment, which was not part of this study.

[91] See for instance: https://www.aivd.nl/publicaties/@3033/interception/

Weaknesses in Internet routing

As stated above, there are many vulnerabilities in the architecture of the Internet in general and the design of the TCP/IP protocol more specifically. For this report the relevant weaknesses are the uncovered content of the data packets flowing openly through the network and the design of the routing principle, requiring that each router needs to read the destination address and check it with the routing table to find the next link for the packet. Each router is more or less independent. There is no global supervisor governing the network of routers. Any router in an upstream network therefore has access to the metadata within it, and in principle anyone can insert a router in a network and manipulate the routing tables to attract relevant data traffic[92].

To solve this weakness, there are basically two conceivable approaches: (physically) separating the EU trusted network as a subnet of the Internet or protecting the EU data packets within the Internet.

Approach 1: The European Internet Subnet, physically separating the EU network

The effective physical separation of an EU network means in the first place that connections to and from the EU environment should be well guarded, by deeply analysing the content of all passing traffic (DPI, deep packet investigation) and taking appropriate action. This could mean formal control of a state-governed or other, independent body. Furthermore, there needs to be an effective surveillance method to monitor the presence of illegal separate external connections. Also, an effective European Identity Management process (distributed or centralised) is required to prevent illegal access inside the EU network by non-EU citizens. This has its drawbacks, such as the sheer size of this effort and the varying approaches to digital identities among Member States. There is also a real possibility of identity mules (people who offer their digital identity in exchange for something else, usually money).

One of the strongest measures against personal data extraction is prohibiting the export of personal data to non-EU data processors. In a thought experiment, this would mean seriously investing in gateway technology and monitoring, similar to the *Great Firewall of China*. It would limit market access, especially for US Cloud providers, even if they had their own data centres on EU soil. This would no doubt be very unpopular with the general public. The main economic difference in the Chinese situation is of course that China's is a much larger and less fragmented market, where Chinese substitutes were initiated years ago for popular American services such as Google, eBay, Twitter et al. Despite being censored, these platforms attract many millions of users.[93]

It is good to notice too that besides the impact on EU citizens, a physical segmentation in combination with strong data protection rules could also result in severe economic disputes, such as claims for the lost investments in facilities in the EU.

Finally, the consequence of a physically separated Internet implies that the physical network, the fibre cables stretching across the EU, should also be protected (at the lowest OSI level). Eavesdropping on fibre cables is relatively easy and, using current technology, practically undetectable. Eavesdropping on submerged cables has been done for decades, with improved data collection technology providing ever more advanced and easily obtainable results. In the current situation, tapping physical networks, not necessarily underwater, seems to be very effective, as the revelations on the Tempora project from the

[92] Michael Mimoso, Threatpost.com , Internet-traffic-following-malicious-detours-via-route-injection-attacks, 20 November 2013, http://threatpost.com/ (accessed on 24 November 2014)

[93] http://readwrite.com/2010/03/03/china_top_3_social_network_sites, see also Annex 5.

Snowden files indicate.[94] Analysts conclude that for these reasons the old-fashioned technology for submarine data collection seems to be disappearing.[95]

Approach 2: Protecting EU data packets on the Internet

The second way of protecting EU metadata is to mask the information in such a way that unauthorised persons or systems cannot understand the content, i.e. cryptography. The options for protection and encryption of data packets are twofold. First the content should be protected and second the routing data should be protected to prevent it being diverted outside the EU. The first option, end-to-end encryption of data, is discussed extensively in other annexes.

For many years encrypted route control products have been available on the market.[96] This technology enables ISPs to manage the routing paths for their outgoing traffic.[97] This technology is relevant to ISPs in providing optimised Internet connectivity and, at the same time, decreases the cost of bandwidth. Theoretically one can imagine a situation in which all EU ISPs are able to route traffic only on predefined safe routes in order to keep all EU data inside the EU (by managing routing tables accordingly).

Effectively, however, the challenges are the same as those described in the last paragraph on physical separation of the network. First, there will be many users legitimately requiring unauthorised external routes. This traffic has to be investigated deeply by a reliable agent with a suitable mandate, rules and equipment. Second, this method assumes that all inside users are trusted and that no other illegal and non-surveilled connections with non-EU domains elsewhere are in place.

If centralised or semi-centralised encryption of meta and content data is not possible for practical reasons, the encryption of metadata could alternatively be delegated to the user community itself. The EU governments would then provide the knowledge and facilities to the user community. An example of this concept is onion routing.

Hiding routing information

A number of other options are available to hide routing information. Some of these options are based on the concept of **mix networks**[98]. Mix networks are routing protocols that create hard-to-trace communications by using a chain of proxy servers known as mixes which take in messages from multiple senders, shuffle them and send them back out in random order to the next destination. Applications based on this concept include **onion routing** and **anonymous remailers**.

An alternative that does not add an extra layer of complexity is replacing the network routing layer (layer 3) with another that does not reveal a global identity. **Dovetail**[99] is an example of such a proposal. Dovetail combines ideas from **source-controlled routing** and low-latency anonymity systems.

[94] The Guardian, GCHQ taps fibre-optic cables for secret access to world's communications, 21 June 2013, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

[95] Reuters, The Navy’s underwater eavesdropper, 19 July 2013, http://blogs.reuters.com/great-debate/2013/07/18/the-navys-underwater-eavesdropper/ (accessed on 24 November 2014)

[96] http://www.techopedia.com/definition/2532/route-control

[97] Ballani, H., Off by Default!, http://www.eecs.berkeley.edu/~sylvia/papers/ballani-defoff-camera.pdf

[98] http://en.wikipedia.org/wiki/Mix_network

[99] Sankey, J. and M. Wright, Dovetail: Stronger Anonymity in Next-Generation Internet Routing, PET symposium 2014 papers, 2014.

Key players involved

Several **Member States** are already investigating the possibilities of a subnet. Germany specifically has indicated interest in this regard.

A critical mass of **companies** and **ISPs** would have to indicate a willingness to work within this structure. In fact, demand from several large multinational corporations for the establishment of such a network to ensure the protection of their intellectual property and economic interests could provide a strong accelerator for such a path.

Demand from **law enforcement and intelligence** agencies for more secure routing of information within the EU is imaginable, due to their legitimate interest in keeping sensitive data – either their own or that of critical infrastructures – out of the hands of other nations or individuals.

Corresponding policy option

To prevent network routing information from being intercepted for metadata analysis purposes by a third party, the EU could in theory **physically or logically separate the network** from the rest of the world. The economic and practical impacts of both of these options on the community would be enormous, however, as the material and technical prerequisites to develop these concepts are costly. Finally the effectiveness of the concept is limited, in part because the European Subnet would still be vulnerable from the inside.

More effort should be put into researching options for the protection of data packet routing data, in order to prevent it from being diverted outside the EU. The concept of **encouraging advanced onion routing mechanisms** and other options is attractive, but not currently scalable enough to be used for the EU as a whole.

Conclusion

The introduction of a separate European Subnet seems generally to be more of a political idea than a technologically driven solution to current problems. Also, in a technical way, it does not seem to offer actual fixes for the current problems of mass surveillance, and none of the experts surveyed have suggested this as a good solution to current mass surveillance problems. However, if current developments continue and more and more parties develop their own infrastructure that can in part be cut off from the traditional world wide web, it could be that EU countries will be forced to develop a strategy for a European Subnet.

2.4. Innovate: the smart fixes to mitigate structural technological vulnerabilities

2.4.1. Stimulate R&D on reduced trackability/traceability of mobile and fixed devices

Many electronic devices emit some kind of electronic signals that make it possible to track them. Some even call this Digital Exhaust. Equipment transmitting radio signals such as Wi-Fi, NFC/RFID, Bluetooth and mobile telephony signals (2G, 3G, 4G) in particular make it easy to track users. Mobile phones even contain functions that make it possible to determine the exact location of the phone. Software such as browsers also leaves fingerprints that make it possible to identify and, over a longer period of time, trace users. Most people are not even aware that these possibilities exist. It has not been a requirement for protocol and systems designers and has received relatively little attention.

It is not only mobile devices that have these properties; many fixed devices such as video cameras and Automatic Number Plate Recognition (ANPR) also make it possible to track humans – e.g. by combining data with facial recognition – or the vehicles they use for transport. A rough estimate is that there are one million video cameras in the Netherlands.[100] With the expected growth of (personal) devices – the Internet of Things – tracing people will become a bigger issue, especially when this is done without the user's consent.

Key players involved

Universities can play an important role in designing improvements in protocols and (personal) equipment that make it harder to trace people. **Telecom equipment** and **mobile phone manufacturers** are important because they need to make adaptations to their products. The open hardware and software community can also play an important role, because they can serve as an example. **Telecom operators** and **ISPs** are among the organisations that need to implement changes.

A barrier to implementation is the huge installed base. There are billions of mobile phones and devices communicating with the mobile phones.

Corresponding policy options

Let the EU set up a dedicated research project to **design or redesign Internet protocols** to minimise the trackability of users. **Regulate** to implement an option in **consumer devices to block** the sending of messages that reveal the location of the user (with an opt-in for users).

Fund **open-source tools** that enhance privacy/block traceability. **Impose** an obligation (in cases where it is not possible to avoid traceability) to show a **message to users warning** them that they can be traced. Or even stronger: **impose non-traceability as a requirement** as part of security by design for personal and/or mobile devices.

Conclusion

Many users now take for granted the fact that they or their actions can easily be traced, especially with mobile devices. At present that can be countered only by removing the battery from the device. Traceability should not be an inherent property of this type of device.

[100] http://sargasso.nl/cameratoezicht-in-nederland-hoeveel-cameras-zijn-er-eigenlijk/

2.4.2. Fix the Internet – promote improvement of inherently insecure protocols

Internet traffic exists due to a stack of Internet protocols, sometimes called the TCP/IP stack. Secure Internet traffic also means having secure Internet protocols. This is not self-evident, however.

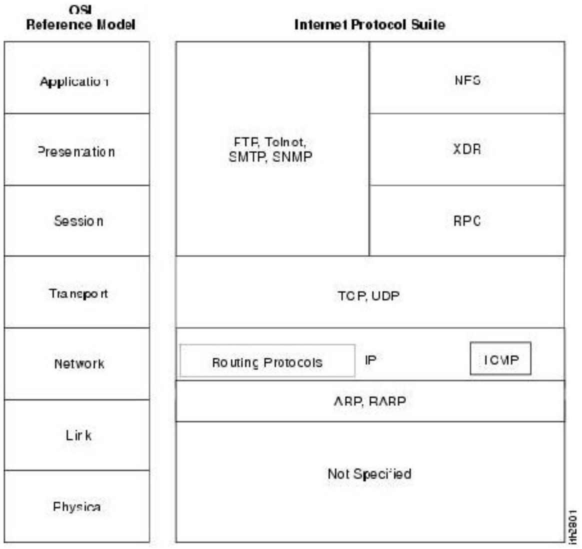


Figure: Internet protocol suite, source: http://docwiki.cisco.com/wiki/Internet_Protocols

All protocols were primarily designed for availability (and integrity), with very limited attention initially paid to confidentiality. Most protocols have vulnerabilities, and to mitigate or resolve these many new versions were released or alternatives designed. See the table below for an (incomplete) overview of examples.

Protocol	Known vulnerabilities	Open-standard solutions
File Transfer Protocol (FTP) is a standard network protocol used to transfer data from one host to another host over a TCP-based network, such as the Internet.	Passwords and file contents are sent unprotected and in clear text. Usernames, passwords, commands and data can be read by anyone able to perform packet capture (sniffing) on the network.	The SSH File Transfer Protocol (SFTP) has the ability to encrypt authentication information and data in transit. Specific software is necessary. Explicit FTPS (FTP over SSH) is an extension to the FTP standard that allows clients to request that the FTP session be encrypted. This is done by sending the "AUTH TLS" command. The server has the option of allowing or denying connections that do not request it.
Transmission Control Protocol (TCP). One of the basic protocols of the Internet, it provides reliable, ordered and error-checked delivery.	Has been modified many times, but remains vulnerable to DDoS and ICMP attacks (pinging).	Several TCP improvements have been designed and implemented.
Internet Protocol (IP)	IP addresses can be spoofed.	IPsec authenticates and encrypts each IP packet of a communication

Protocol	Known vulnerabilities	Open-standard solutions
		session. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption) and replay protection.
Hyper Text Transfer Protocol (HTTP)	Data is sent in clear text.	HTTPS offers encryption through SSL-TLS HTTP2 offers opportunistic encryption (see Annex B, chapter 1).
Secure Socket Layer (SSL) was designed to provide data confidentiality and data integrity between two communicating applications.	Many vulnerabilities in SSL have surfaced. The Heartbleed Bug, a serious vulnerability in the OpenSSL cryptographic software library, allows theft of protected information. Poodle did something similar for SSLv3. SSLv3 is an older protocol that has been replaced in many client and server configurations with TLS (Transport Layer Security), but many browser clients and web servers that use TLS for connections still support SSLv3.	Transport Layer Security (TLS) is the successor to SSL. It has a variety of security measures. Several versions with varying degrees of security of both protocols are in widespread use.
Domain Name Server (DNS) provides mapping from host names to IP addresses.	Traffic can be spoofed (via DNS cache poisoning and DNS Forgery) to facilitate a man-in-the-middle attack rerouting traffic.	DNSSec provides authentication and integrity to DNS, tackling the majority of security issues related to DNS .
Border Gateway Protocol (BGP) is a protocol for exchanging routing and reachability (AS) on the Internet. Version 4 of BGP has been in use on the Internet since 1994.	Faulty, misconfigured, or deliberately malicious sources can disrupt overall Internet behaviour by injecting bogus routing information into the BGP-distributed routing database (by modifying, forging or replaying BGP packets).	New BGP versions and BGPSec.

Table: examples of (lack of) security of Internet Protocols[101]

[101] Based on: Hemant. K et al., Security Problems and Their Defenses in TCP/IP Protocol Suite, in Journal of Scientific and Research Publications, Vol. 2 Issue 12, December 2012. Bellovin, S.M., Security problems in the TCP/IP Protocol suite, Computer Communications Review; Cisco, Internet Protocols, http://docwiki.cisco.com/wiki/Internet_Protocols, undated, Accessed on 26 November 2014. Bansal, P., TCP Vulnerabilities and IP Spoofing: Current Challenges and Future Prospects, October 2012. Network Working Group of The Internet Society, RFC 4272 BGP Security Vulnerabilities Analysis, 2006. Mateti, P., Security Issues in the TCP/IP Suite, World Scientific Review Volume – 9, 21 November 2006. Related Wikipedia pages and IETF standards were also used to check facts and definitions.

Key players involved

Usually a technical solution is feasible to improve the security of Internet Protocols. The **Internet Engineering Task Force (IETF)** is doing just that. Its mission is '*to make the Internet work better by producing high-quality, relevant technical documents that influence the way people design, use, and manage the Internet*.' The IETF is organised in working groups which define new (or renewed) open standards in an open, transparent review process.

In most cases standards – being open – are used by very many devices (both on the server (mostly **ISPs and other telco companies**) and on the client side **(end-users)**). Adoption and implementation therefore requires time. In some cases, such as IPv4 and IPv6, old and new standards have to operate side by side for an unspecified period of time.

For **ISPs and telcos** new standards often add very little concrete business benefit, but often require very concrete investments in installing new protocols or buying new hardware.

Despite the open and transparent nature of the open standard design process, there are still risks of (state-sponsored) backdoors, possibly exposing **end-users**. Allegations of backdoors in open Internet standards were made during discussions surrounding the Snowden revelations.[102]

For the **EU and its Member States, other countries and organisations such as the ITU**, interventions go to the heart of the debate on Internet governance. This is an ongoing political discussion. Under current Western policies, the free-market vision dominates the Internet debate and intervention is therefore supposed to be limited; the Internet should not be governed by a supranational body. Influencing open standards should therefore be low-key.

Corresponding policy option

For the EU, **stimulating more secure open standards** for Internet protocols by either supporting **individual contributions** or setting up a **dedicated long-term research programme** in cooperation with the academic world, ISPs and IETF others to research and co-develop open standards.

A point to consider is the incorporation of these open standards into **certification schemes** as proposed elsewhere in this study, on top of the open process provided by the IETF. This would offer more guarantees against backdoors.

Finally, if protocols are considered to be insecure and a cure is not easily obtained, then **depreciation of that protocol** is in order, ultimately by **regulation**.

Conclusion

Promoting more secure open standards for Internet protocols is a key policy option for the EU, as any online security depends on those standards. The level of intervention is politically driven for the most part. In our opinion the EU should take a long-term interest in this topic.

[102] New York Times, "Secret Documents Reveal N.S.A. Campaign Against Encryption", 5 September 2013, accessed on 25 November 2014. John Gilmore in the cryptography mailing list: "Re: [Cryptography] Opening Discussion: Speculation on 'BULLRUN'", http://www.mail-archive.com/cryptography@metzdowd.com/msg12325.html, accessed on 25 November 2014 .

2.4.3. Data-centric security

A completely different and promising way of protecting digital content is using the concept of data-centric security. This concept focuses on securing information instead of protecting applications, assets such as computers and networks. Data-centric security is based on deperimeterisation as a fundamental idea, in this case on the data level.

The key thought is that as long as data is secure, it does not matter where it is stored. This is especially important because much information flows outside the organisation's perimeter because of Software as a Service (SaaS), Cloud computing, e-mail, instant messaging, social networking activities, laptops, smartphones, tablets and Google Glass.

The self-protection of data requires intelligence be put into the data itself. It needs to be self-describing and defending, regardless of its environment. Data needs to be encrypted and supplemented with a usage policy. When accessed, data should consult its policy and attempt to recreate a secure environment using virtualisation and reveal itself only if the environment is verified as trustworthy.[103]

The concept of data-centric security was introduced at the beginning of this millennium and fostered by the Jericho Forum, later the Jericho Work Group[104] within the Security Forum of the Open Group. Ten years later very few organisations have implemented it on any significant scale. One of the reasons is that the security market has so far failed to offer data-centric audit and protection (DCAP) products to operate across all silos within organisations.[105]

The interest in data-centric security has increased over the last few years and more software companies are creating products that are compliant with this model. The data-centric security model was designed for the protection of business information but can also be applied to a consumer situation.[106]

As with many security solutions, the security level depends on its weakest link, so great care should be taken in selecting the right (open-source?) packages to support this concept. As mentioned, these are not yet widely available.

Attribute-based access

A related development is that of attribute-based access, instead of role-based access. In attribute-based access, the authority to read, write or delete data is not based on the role someone has (user, administrator, super-user etc.). Instead, the context determines the user rights (usually in combination with high-level rules on roles and rights). Context can include things like what device the data is accessed from, from where and when it is accessed. For instance, a bank client can effect more payment transactions for higher values when operating from his desktop computer at home during the evening when he normally does his e-banking work than from his mobile device, abroad, in the middle of the night.

Key players involved

As more research is required into the possibilities and constraints of data-centric security, **universities** are key players to be involved.

[103] Chow, R. et al., Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control, 2009.

[104] https://collaboration.opengroup.org/jericho/index.php

[105] Gartner, Gartner Says Big Data Needs a Data-Centric Security Focus, press release of 4 June 2014.

[106] Future consumer mobile phone security: a case study using the data-centric security model, André van Cleeff, University of Twente.

Vendors have so far shown limited interest in developing and launching ready-to-use concepts for private and public organisations, let alone individuals. Although the **end-user** is facilitated, ease of implementation for **organisations** is still far away. Early implementations show that the consequences for technology and business processes are far-reaching.[107] However, data-centric security does offer huge advantages for working securely within Cloud facilities or BYOD.

The **open-source software community** might fill the niche, to develop products that contribute to data-centric security. Cooperation with universities should be encouraged.

Corresponding policy option

Stimulate and finance research & development on data-centric security, especially implementation concepts and more specifically those for individual users (consumers). Cooperation between the academic world and the open-source community should also be encouraged.

Conclusion

Data-centric security is a promising model for securing information, especially for working with the Cloud and BYOD. More research is required, especially in the area of consumer applications.

2.5. Closing thoughts

The key question in this chapter was how to achieve a balance over the long term (within the next 10 years), from a technological and organisational foresight perspective, between the need for individual privacy and the needs of the organisations legally in charge of law enforcement and/or national security.

Looking back at the described technology and organisational options in both this main report and the annexes, four headlines appear:

- encryption (E2EE adoption, certification schemes etc.)
- (de-)perimeterisation (at data, application (SDP) and network (SubNet) level)
- (secure) open-source software
- fixing structural problems of the Internet (more confidentiality through improved protocols).

These options provide a higher level of privacy protection for EU citizens, but all have their disadvantages, of which cost and ease of use are important ones. The complex governance of the Internet is also a point to consider. Furthermore, the widespread adoption of encryption in particular seems to pose a threat to legitimate surveillance for law enforcement and intelligence.

In the final paragraphs of this chapter we address some other overarching subjects that have not yet been touched on: certificates as a single point of failure, secure software in general and detection of surveillance as an aspect of privacy protection. We would also like to highlight some additional challenges, such as the Internet of Things and the Big Data that is behind it.

2.5.1. Certificates as a single point of failure?

Encryption is one of the main themes in this study. Many technology options discussed rely on cryptokeys which are ultimately verified by a certifying authority (CA). In the current situation this means that one root CA verifies all underlying certificates in a pyramid model.

This is a workable but also unsatisfactory situation for (at least) two reasons:

[107] This is based on experience of the authors.

1. Breaches in the past (such as Diginotar, Comodo and RSA) have demonstrated that root CAs can also be compromised and that the consequences can be very serious.
2. The HTTPS market is highly concentrated and depends largely on a small number of US providers. About 75% of all root certificates are provided by the three largest CAs: Symantec[108], GoDaddy and Comodo. They are *too big to fail*: the failure of a single CA would impact the whole ecosystem. They are also '*too big to want to adjust'* to market conditions (such as price competition, but also desired improvements to the system). [109]

Several options for intervention arise, each having advantages and disadvantages.

First there are regulatory solutions. The HTTPS authentication model is more or less unregulated in both the US and the EU, although the industry is covered by the NIS Directive. The current existing regulatory regime in the EU and auditing obligations worldwide have proved ineffective on the basis of numerous incidents. The proposed directive on Electronic Identification and Trust Services Regulation (June 2012, amended by the European Parliament in April 2014) focuses on availability to boost trust in e-commerce, neglecting confidentiality and integrity concerns. The proposal and amendments take limited account of privacy concerns or the Snowden revelations, although there was good reason to do so. Security requirements will be elaborated by the European Commission at a later stage. Some authors[110] are concerned that the industry has far too much influence, which is given the '*too big to want to adjust'* observation a serious concern from the security point of view.

The second angle is to approach a more fundamental issue. Why ultimately depend on only one CA that can be compromised? From a conceptual point of view it would make sense to demand two verifications for every certificate or key. This would reduce the risk of a single point of failure. However, this option will also raise costs for users (two certificates instead of one) and under current market conditions prices would probably not drop dramatically with this rise in demand. Furthermore, it remains to be seen whether large CAs will favour such a construction, as it may undermine their position.

2.5.2. Stimulate R&D on the detection of surveillance

Instead of – or in addition – to preventing surveillance, detecting it also provides a certain level of privacy protection. The surveillance 'value chain' offers multiple detection points: profiling, initial intrusion, infection with malware, command and control, harvesting data and possibly the exit and erasing of evidence.

For instance, in order to become usable, a program that is secretly harvesting information must be able to forward this data to the recipient. Depending on the technical capacities of the user, the external flow may be monitored and even intercepted. Nevertheless, if the mechanism is sophisticated enough to embed the stolen information in legitimate flows, such as credible software updates, the attack may remain essentially unnoticed.

Neither part of this study covers the detection of mass surveillance extensively, but it seems a valuable angle to follow. In recent periods, increased attention from activists and human rights organisations has been focused on finding ways to counteract surveillance. In November 2014 Amnesty International, the Electronic Frontier Foundation (EFF) and privacy investigators launched Detekt, a tool designed to scan

[108] Symantec owns multiple brands, including Verisign, GeoTrust, Thawte, RapidSSL and TC TrustCenter.

[109] Based on: Arnbak, A.M., et al. Security Collapse in the HTTPS Market, October 2014, Vol. 57 No. 10, Communications of the ACM.

[110] Arnbak, A.M., et al. Security Collapse in the HTTPS Market, October 2014, Vol. 57 No. 10, Communications of the ACM.

computers for traces of known surveillance spyware. Detekt is apparently able to detect at least FinFisher, software known to be widely used by governments of all stripes, including repressive regimes. The underlying thought behind this and similar tooling is that knowing that one is under surveillance can make one more conscious of one's privacy. Obviously, the fact that this encompasses 'known' spyware already entails a caveat, apart from the fact that there has been no time to evaluate the operation of the tooling. There is also, however, another major downside to this kind of tooling: the first parties to learn how to detect surveillance are probably malicious actors, such as criminals and spies. Their interests in preventing surveillance are much higher than those of normal, everyday citizens.

2.5.3. Additional challenges

This study on technology foresight options was written from the perspective of today. However, in the environment of mass surveillance and privacy protection, several challenging developments are under way that might change the point of view for the reader.

We referred earlier to quantum computing, for instance. If that becomes operational, then almost every encryption-based option in this study becomes obsolete overnight. But there are other developments to take into account.

Internet of Things

The Internet of Things (IoT) is one of the hot topics of today. It is notable that the key business driver for IoT is not the thing (the price for the device), nor the Internet (connectivity); it is the Big Data that the billions of expected devices will generate. Devices range from personal weather stations and televisions to cars, wearable devices (glasses, watches), medical devices and clothes. The data those devices generate provides information for marketeers and security agencies alike on uniquely identifiable people and the conditions they are in, the things they own, their locations and what they are physically doing or watching. This offers huge data collection and analysis opportunities.

From a privacy point of view this poses an even greater threat than collecting metadata of (deliberate) communications by citizens. With IoT, the citizen ultimately has very few options when deciding whether or not to use the device (and hence whether or not to send data). This requires vigilance on the part of regulators and Data Protection Authorities alike.

A policy option would be to devise a policy on the Internet of Things, balancing all sorts of benefits (economic, health, social etc.) and privacy impacts. This policy would ideally be based on a public discussion on the advantages and disadvantages of IoT and would include the role of Big Data and marketing.

Technical developments in surveillance require a political discussion

This study is focused on mitigating the risks of *known* mass surveillance techniques, as described in part 1. However, given the considerable budgets the major powers are investing in their cyber intelligence capabilities, we cannot exclude the possibility that much more is possible already. In addition, new targeted or collective surveillance options may already be under development.

The policy consequence is that rather than technology, it is the legal framework, authorities and accountability that should be regulated.

The reverse is true too. Encryption can pose a serious hindrance to (targeted) crime investigations. On the other hand, operations such as Onymous demonstrate the ingenuity of law enforcement agencies across the globe. Even the Tor network is not 100% secure.

This balance requires a solid political discussion on what is reasonable from a law enforcement perspective in comparison to privacy and protection against other cyber threats. Without a conclusive discussion it will remain a cat-and-mouse game from a technological perspective.

3. POLICY OPTIONS

The main objective of this study is to provide the European Parliament and specifically the LIBE Committee with more technological background information and possible policy options based on technology foresight, regarding the protection of the European information society against mass surveillance from the perspective of technology and organisational foresight. Four scenarios, each with two to four technology options, were developed in this study.

3.1. Policy options for the 'Promote Adoption' scenario

3.1.1. Promote E2EE

Stimulate **awareness of the necessity of using encryption** by initiating a campaign, as awareness of privacy risks is fairly low.

Increase the **knowledge level of end-users**, both individuals and responsible departments in organisations (public and private), by setting up an **independent platform** where users can find information on tools, implementation, *do's and don'ts* etc.

Support product security tests by independent institutions such as the Electronic Frontier Foundation that help users make better-informed choices. Support can be a financial contribution, but also promotion of the results. Alternatively the EU can set up its **own regular product security test programme**.

A parallel option is to **stimulate the user-friendliness of E2EE solutions**, for instance by promoting existing user-friendly E2EE solutions for e-mail, messaging, chat etc. Dedicated **funding or participation** in OSS E2EE solutions is also an option to specifically improve user-friendliness.

If the market does not provide security with E2EE by itself, **regulation** should be considered, obliging service providers and/or ISPs to provide end-to-end protection as standard for data in transit. An additional benefit of regulation would be a **concrete political discussion on the balance** between privacy and law enforcement and national security, at European and/or national level. The outcome of this debate should be translated to national legislation.

3.1.2. Promote open-source software

Although it is not a universal remedy, open-source software (OSS) is still an important ingredient in an EU strategy for more security and technological independence. The **quality of the lifecycle processes** of OSS is crucial for its security, more than technology.

Support and fund maintenance and/or audit of important OSS: open-source initiatives, some of them widely implemented in very important systems, such as OpenSSL, TrueCrypt/Ciphershed, GPG, Tor, OwnCloud, etc., need funding to keep going and be audited (with regard to both code and processes).

Initiate a European "OSS Bug Bounty Programme" or finance existing programmes, as an alternative to intervening directly with specific OSS programmes.

Set up certification schemes for a limited set of critical types of OSS, implemented by technical tests (e.g. penetration tests, code reviews). Supporting this, the EU should draft and maintain an **agenda of critical OSS** for its citizens and companies.

3.1.3. Promote and stimulate EU ICT services: Cloud, social media, search engines

A consumer-market-oriented approach to European social media, Cloud services and search engines is a desirable option, although not the easiest, since the European market is open and fragmented and major platforms are available for all *current* service categories.

We therefore propose stronger **legal limits on exporting personal data** than those offered by the forthcoming Data Protection regulation (mainly transparency with regard to location, informed consent by individual). This would give European ICT players the time and legal space necessary to create demand for specific EU solutions. **Liability and substantial fines** for non-compliance will also provide a strong stimulus for action.

3.1.4. Promote secure software development

Promote the **use of existing guidelines** for secure software development, such as the OWASP Top 10. Security is a job not just for 'Security', but for all staff involved in designing, developing, maintaining and exiting software. Draft **EU guidelines** for secure software development, with the software industry. Challenge software suppliers to adhere to secure software development guidelines, **leveraging the buying power** of the EU institutions.

Certification of software is also a policy option, but given the magnitude of software circulating and under development, this should start with a very specific focus. For instance (OSS) browsers, operating systems and mobile apps. The next step could be **product liability for (some) software** to protect users from risks resulting from insecure software, risks they themselves can usually neither assess nor mitigate.

3.2. Policy options for the 'Build Confidence' scenario

3.2.1. Security baselines

Implement an **EU Security Baseline regulation** to build confidence by ensuring a minimum level of security measures for Critical Information Infrastructure elements in the EU.

3.2.2. EU Coordinated Disclosure

EU **rules or guidelines for facilitating a process of 'coordinated disclosure'** help discover and fix more software vulnerabilities, whilst protecting those disclosing within the rules. An **EU guideline on Coordinated Disclosure** should be issued. **A (trusted) national coordinator** should monitor to ensure that reported vulnerabilities are fixed.

3.3. Policy options for the 'Disrupt(ive Innovation)' scenario

3.3.1. Certification schemes

The key policy option with regard to encryption schemes is to establish an **EU standardisation body or certification authority for encryption standards**. Such a certification scheme should be complemented by a **legal framework that imposes liability** on non-compliant ISPs, for instance. Ideally such an EU standardisation body would **cooperate internationally** with the NIST and other national agencies around the world on the process level (way of working) and principles, to avoid negative effects of regionalisation.

3.3.2. European Internet Subnet

To prevent network routing information from being intercepted for metadata analysis purposes by a third party, the EU could in theory **physically or logically separate the network** from the rest of the world. This is not the way forward. Other approaches such as **deperimeterisation**, at data and application level, must be implemented instead.

Regulation on certified hardware and software for major Internet access points in the EU would raise the overall security of the European part of the Internet.

3.4. Policy options for the 'Innovate' scenario

3.4.1. Stimulate R&D into reduced trackability/traceability and detection of surveillance

Let the EU set up a dedicated research project to **design or redesign Internet protocols** to minimise the trackability of users. **Regulate** to implement an option in **consumer devices to block** the sending of messages that reveal the location of the user (with an opt-in for users).

Fund **open-source tools** that enhance privacy/block traceability. **Impose** an obligation (in cases where it is not possible to avoid traceability) to show a **message to users warning** them that they can be traced. Or even stronger: **impose non-traceability as a requirement** as part of security by design for (personal and/or or mobile) devices.

3.4.2. 'Fix the Internet' – promote improvement of inherently insecure protocols

More secure open standards for Internet protocols in the EU could be **stimulated** by supporting **individual contributions** and setting up a **dedicated long-term R&D effort** in cooperation with the academic world, ISPs, the IETF and others to research and co-develop open standards.

Finally, if protocols are considered to be insecure (which most are) and a cure is not easily obtained, then **depreciation of that protocol** is in order, ultimately by public **regulation**.

3.4.3. Data-centric Security

Set up a specific EU **Research & Development programme** on data-centric security, especially implementation concepts and more specifically those for individual users.

3.5. Overall conclusions

Despite the many technology foresight options, there is no single technological solution to help citizens better manage their privacy risks in the light of mass surveillance and other threats against their privacy. Work needs to be done on a number of technologies to achieve a robust security posture, and this work should start now.

Given the open nature and general technological state of the Internet and local ICT environments, the technology-based policy options to pursue in combination are:

- **End-to-end encryption** is one of the strongest ways to protect data during communication, but ease of use and (proactive collective) implementation must be pursued to achieve sufficient scale in terms of the number of users. Furthermore, Europe should set up its own **certification schemes** for encryption standards, to mitigate the risk of backdoors. Bear in mind that should **quantum computing** become available, this and other encryption options should be deemed obsolete immediately.

- **Deperimeterisation at data and application** level, not network level, to protect access to critical data. Data-centric approaches and software-designed parameters offer much more flexible application, regardless of the underlying (Internet) infrastructure.
- Increase EU technological independence through **verifiably Secure Open-Source Software ("SOSS")**. Improving the quality of lifecycle management processes of key OSS platforms is essential, as is certification of these OSS platforms. The EU should invest in code review and certification schemes and facilities for OSS.
- The EU should increase its efforts to fix structural security problems with Internet protocols, which undermine security against all sorts of cyber threats.
- And finally the EU should set up an independent institute for **certification** of encryption standards and key OSS platforms.

These technology options should be accompanied and supported by legal, financial and promotional arrangements. A tougher posture than that currently proposed in the forthcoming **Data Protection regulation** on personal data export, for instance, would create the breathing space that European (OSS) ICT needs to build up a substantial market position and enough scale to survive independently.

Product liability and leveraging the **purchasing power of the EU and its Member States** are other ways to stimulate the market to produce more secure ICT, fit for secure use in the EU.

Several developments will challenge the technologies described. Quantum computing was mentioned, but undoubtedly (other) **surveillance technologies** are under development as well. The **Internet of Things** (IoT) will dramatically widen the possibilities for surveillance and will pose new security and privacy risks as well. With IoT the average citizen will have even less influence on what data he or she shares, when and with whom. The privacy and security aspects of IoT are barely discussed at present.

The **Big Data** that the Internet of Things generates is of specific interest for **marketing** too, providing valuable data on consumer behaviour and well-being. The focus on privacy with regard to mass surveillance should not steer attention away from other intrusions.

Finally it is not technology, but **political debate** that determines where the balance should be between privacy and law enforcement, intelligence and marketing. Leaving the balance up to technological and market forces will most probably be unsatisfactory for all sides.

Annex A. Sources

Documents

Acquisti, A., Grossklags, J., *Privacy and rationality in individual decision making*. IEEE, Security & Privacy 2, 24–30, 2005.

Aite, *End-to-End Encryption in Card Payments: An Introduction*, 2010, http://www.aitegroup.com/report/end-end-encryption-card-payments-introduction, accessed on 10 October 2014.

Anderson, Ross (2002), *Security in Open versus Closed Systems. The Dance of Boltzmann, Coase and Moore*, in: Open Source Software: Economics, Law and Policy, http://www.net-security.org/dl/articles/toulouse.pdf, accessed on 12 May 2014.

AOL et al., *USA Freedom Act Letter*, 31 October 2013, http://sensenbrenner.house.gov/uploadedfiles/usa_freedom_act_letter_10-31-13.pdf, accessed on 9 October 2014.

Arnbak, A.M. et al., *Security Collapse in the HTTPS Market*, October 2014, Vol. 57 No. 10, Communications of the ACM.

Ars Technica, *How the NSA (may have) put a backdoor in RSA's cryptography: A technical primer*, http://arstechnica.com/security/2014/01/how-the-nsa-may-have-put-a-backdoor-in-rsas-cryptography-a-technical-primer/, accessed on 31 July 2014.

Asghari H., M.J.G. van Eeten, A.M. Arnbak, N.A.N.M. van Eijk, *Security Economics in the HTTPS Value Chain*, WEIS 2013 paper, 2013.

Axe, D., '*The Navy's underwater eavesdropper*', 19 July 2013, Reuters, http://blogs.reuters.com/great-debate/2013/07/18/the-navys-underwater-eavesdropper/, accessed on 24 November 2014.

Babcock, C., '*HP Warns Of IoT Security Risks*', Information Week, 29 July 2014, http://www.informationweek.com/cloud/software-as-a-service/hp-warns-of-iot-security-risks/d/d-id/1297617, accessed on 3 October 2014.

Ballani, H., *Off by Default!*, http://www.eecs.berkeley.edu/~sylvia/papers/ballani-defoff-camera.pdf, accessed on 25 November 2014.

Banerjee, C; S. K. Pandey, *Software Security Rules: SDLC Perspective*, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 1, 2009.

Bansal, P., *TCP Vulnerabilities and IP Spoofing: Current Challenges and Future Prospects*, October 2012.

Bell, L., '*Intel claims IoT encryption tool will make payment transactions more secure*', The Inquirer, October 16, 2014 http://www.theinquirer.net/inquirer/news/2376030/intel-claims-iot-encryption-tool-will-make-payment-transactions-more-secure, accessed 27 October 2014

Bernstein, D.J., *Money is not spent on more secure software*, presentation on 10 July 2014.

Bienfang, J., *Truly Random Numbers -- But not by Chance*, 2013, http://www.nist.gov/pml/div684/random_numbers_bell_test.cfm, accessed on 4 August 2014.

Bos, J.W. et al., '*Fast Cryptography in Genus 2*,' Microsoft Research Workshop on Elliptic Curve Cryptography, 2013 https://www.cosic.esat.kuleuven.be/ecc2013/files/joppe.pdf, accessed on 10 August 2014.

Breaking Defense, *DARPA's CRASH Program Reinvents The Computer For Better Security*, 2012 http://breakingdefense.com/2012/12/darpa-crash-program-seeks-to-reinvent-computers-for-better-secur/, accessed on 3 August 2014.

Bugcrowd, *The Bug Bounty List*, undated https://bugcrowd.com/list-of-bug-bounty-programs

Bugsheet, *List of Bug Bounties & Disclosure Programs*, http://www.bugsheet.com/bug-bounties

Caudill, A., '*On Opportunistic Encryption*', 25 February 2014, https://adamcaudill.com/2014/02/25/on-opportunistic-encryption/, accessed on 21 July 2014.

Centrum voor Informatiebeveiliging en Privacy, *Grip op Secure Software Development (SSD) - SIVA Beveiligingseisen voor (web)applicaties*, 2014.

Cern Computer Security, *Mandatory Security Baselines*, 2010 https://security.web.cern.ch/security/rules/en/baselines.shtml, accessed on 10 August 2014.

Cern Computer Security, *Mandatory Security Baselines*, 2010 https://security.web.cern.ch/security/rules/en/baselines.shtml, accessed on 10 August 2014.

Chow, R. et al., *Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control*, 2009.

Cisco, *Internet Protocols*, undated, http://docwiki.cisco.com/wiki/Internet_Protocols, accessed on 26 November 2014.

Cloud Security Alliance – Software Defined Perimeter Working Group, *Software Defined Perimeter*, December 2013.

Cloud Security Alliance – Software Defined Perimeter Working Group, *SDP Specification 1.0*, April 2014.

Cloud Security Alliance – Software Defined Perimeter Working Group, *SDP Hackathon Whitepaper*, April 2014.

Cloud Security Alliance, *Hackathon On! Cloud Security Alliance Challenges Hackers To Break Its Software Defined Perimeter (SDP) At CSA Congress 2014*, https://cloudsecurityalliance.org/media/news/hackathon-on-cloud-security-alliance-challenges-hackers-to-break-its-software-defined-perimeter-sdp-at-csa-congress-2014/, accessed on 17 November 2014.

Cloud Security Alliance, *Software Defined Perimeter Yet to be Hacked. Full Attack Analysis Coming Soon!*, https://hacksdp.com/, accessed on 17 November 2014.

Comey, J., '*Going dark: are technology privacy and public safety on a collision course?*', Brookings Institution, Washington, D.C., 16 October 2014, http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course accessed on 6 November 2014.

Computerworld, *Cloud computing 2014: Moving to a zero-trust security model*, 2013, http://www.computerworld.com/s/article/9244959/Cloud_computing_2014_Moving_to_a_zero_trust_security_model, accessed on 4 August 2014.

Computerworld, *IBM touts encryption innovation*, 2009, http://www.computerworld.com/s/article/9134823/IBM_touts_encryption_innovation?taxonomyId=152&intsrc=kc_top&taxonomyName=compliance, accessed on 4 August 2014.

Court of Justice of the European Union, *Judgment in Joined Cases C-293/12 and C-594/12*, 8 April 2014.

CTOVision.com, *Software Defined Perimeter, Cloud Security Alliance: Coca-Cola Case Study*, 28 October 2014, https://ctovision.com/2014/10/software-defined-perimeter-cloud-security-alliance-coca-cola-case-study/, accessed on 18 November 2014.

Daily Caller, *FBI Asks Congress For Backdoor Access To All Cellphones For Surveillance*, 20 October 2014, http://dailycaller.com/2014/10/20/fbi-asks-congress-for-backdoor-access-to-all-cellphones-for-surveillance/, accessed on 6 November 2014.

DARPA, *CRASH program*, http://www.darpa.mil/Our_Work/I2O/Programs/Clean-slate_design_of_Resilient_Adaptive_Secure_Hosts_(CRASH).aspx, accessed on 3 August 2014.

DARPA, *High-Assurance Cyber Military Systems (HACMS)*, 2012 http://www.darpa.mil/Our_Work/I2O/Programs/High-Assurance_Cyber_Military_Systems_(HACMS).aspx, accessed on 10 August 2014.

DARPA, *Mission-oriented Resilient Clouds (MRC)*, 2011, http://www.darpa.mil/Our_Work/I2O/Programs/Mission-oriented_Resilient_Clouds_(MRC).aspx, accessed on 10 August 2014.

Deutsche Welle, "I expect Merkel's actions to follow her words", http://www.dw.de/i-expect-merkels-actions-to-follow-her-words/a-17438783, 17 February 2014, accessed on 23 September 2014.

Dingledine, Roger et al., *Tor: The Second-Generation Onion Router (draft version 1)*, 2014, http://www.cl.cam.ac.uk/~sjm217/papers/tor14design.pdf, accessed on 1 November 2014.

Dourado, Eli, *Let's Build a More Secure Internet,* http://www.nytimes.com/2013/10/09/opinion/lets-build-a-more-secure-internet.html?ref=international&_r=1&, 8 October 2013, accessed on 10 October 2014.

Dunkelberger, Philipp, *The Future of Encryption*, 2004, 'http://www.ttivanguard.com/austinreconn/encrypt.pdf, accessed on 20 August 2014.

Encryptics, *Securing Valuable Corporate Intellectual Property,* undated, https://www.encryptics.com/case_studies/Oil_Energy.pdf, accessed on 10 October 2014.

ENISA, *Algorithms, Key Sizes and Parameters Report*, 2013.

ENISA, *eID Authentication methods in e-Finance and e-Payment services*, 2014.

ENISA, *Shortlisting network and information security standards and good practices, Version 1.0,* January 2012.

ENISA, *Shortlisting network and information security standards and good practices,* January 2012, https://resilience.enisa.europa.eu/article-13/shortlist-of-networks-and-information-security-standards

Erkonnen, Henrik and Jonas Larsson, *Anonymous Networks: Onion Routing with TOR, Garlic Routing with I2P*, http://www.cse.chalmers.se/~tsigas/Courses/DCDSeminar/Files/onion_routing.pdf, accessed on 4 August 2014.

European Central Bank, *Recommendations for the security of internet payments*, 2013, available at http://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf , accessed on 3 October 2014.

European Commission, *Privacy Enhancing Technologies (PETs),* 2007, http://europa.eu/rapid/press-release_MEMO-07-159_en.htm, accessed on 10 August 2014.

European Commission, *proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union*, 2013.

European Parliament, *Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs* (2013/2188(INI)), 2014, accessed on 10 August 2014.

European Parliament, *The US Surveillance programmes and their impact on EU citizens' universal rights*, http://www.europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL-LIBE_NT(2013)474405_EN.pdf, accessed on 5 October 2014.

European Union, *EU Atlas of ICT Hot Spots*, 2014, http://is.jrc.ec.europa.eu/pages/ISG/eipe/atlas.html, accessed on 9 October 2014.

FedBizzOps, *Security And Privacy Assurance Research (SPAR) Program Broad Agency Announcement (BAA)*, 2011, https://www.fbo.gov/index?s=opportunity&mode=form&id=c55e38dbde30cb668f687897d8f01e69&tab=core&_cview=1, accessed on 10 August 2014.

Fedscoop, *Microsoft champions Internet privacy, calls on Congress to act*, 24 June 2014, http://fedscoop.com/microsoft-calls-congress-act-privacy/, accessed on 10 August 2014.

Ferreira, Edy and Stoyan Tanev, *How Companies Make Money Through Involvement in Open Source Hardware Projects,* 2009, http://timreview.ca/article/228, accessed on 20 August 2014.

Finley, K. *'HP Acquires Open Source Cloud Pioneer Eucalyptus'*, 11 September 2014, Wired, http://www.wired.com/2014/09/hp-eucalyptus/, accessed on 9 October 2014.

First Data, *Data Encryption and Tokenization: An Innovative One-Two Punch to Increase Data Security and Reduce the Challenges of PCI DSS Compliance*, 2009, https://www.firstdata.com/downloads/thought-leadership/fd_encrypt_token_pci_whitepaper.pdf, accessed on 10 October 2014.

Fisher, D., *'Apple Implements Email Encryption for iCloud'*, 17 July 2014, Threatpost, http://threatpost.com/apple-implements-email-encryption-for-icloud/107285, 17 July 2014, accessed on 12 November 2014.

Forbes, *IBM's Blindfolded Calculator*, 2009 http://www.forbes.com/forbes/2009/0713/breakthroughs-privacy-super-secret-encryption.html, accessed on 5 August 2014.

G. Pallis, D. Zeinalipour-Yazti and M. Dikaiakos, *Online social networks: Status and trends,* 2011, in: New Directions in Web Data Management 1, volume 331, Studies in Computational Intelligence, pages 213–234, Springer Berlin Heidelberg.

Gallagher, Ryan, *Meet the "Dark Mail Alliance" Planning to Keep the NSA Out of Your Inbox*, 2013 http://www.slate.com/blogs/future_tense/2013/10/30/dark_mail_alliance_lavabit_silent_circle_team_up_to_create_surveillance.html, accessed on 17 October 2014.

Gartner, *Gartner Says Big Data Needs a Data-Centric Security Focus*, press release of 4 June 2014.

Gentry, Craig (2009), *A fully Homomorphic Encryption Scheme*, http://crypto.stanford.edu/craig/craig-thesis.pdf, accessed on 3 August 2014.

Gonsalves, Antone, *Researcher argues for open hardware to defend against NSA spying*, 2013 http://www.csoonline.com/article/2134047/network-security/researcher-argues-for-open-hardware-to-defend-against- nsa-spying.html, accessed on 21 September 2014.

Google, *Email encryption in transit.* http://www.google.com/transparencyreport/saferemail/

GOVCERT.NL, *'FACT SHEET FS 2009-05 Eavesdropping on GSM-communications'*, 2010 https://www.ncsc.nl/binaries/en/services/expertise-advice/knowledge-sharing/factsheets/factsheet-regarding-eavesdropping-on-gsm-communications/1/Factsheet%2BEavesdropping%2Bon%2BGSM%2Bcommunications.pdf, accessed on 13 July 2014.

Greenberg, A., *Global Web Crackdown Arrests 17, Seizes Hundreds Of Dark Net Domains*, 11 July 2014, www.wired.com, accessed on 24 November 2014.

Greenwald G. and MacAskill E., *'NSA Prism program taps in to user data of Apple, Google and others'*, 7 June 2014, The Guardian, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, accessed on 5 October 2014.

Greenwald, Glen, *No Place to Hide*, 2014.

GSM SecureVoice, *Secure VOIP Solution for Everyone.* Undated http://www.securevoicegsm.com/encrypted-voip-calls/, accessed on 13 July 2014.

Harding, L., *'Putin considers plan to unplug Russia from the internet 'in an emergency'*, The Guardian, 29 September 2014, http://www.theguardian.com/world/2014/sep/19/vladimir-putin-plan-unplug-russia-internet-emergency-kremlin-moscow, accessed on 5 October 2014.

Hemant. K et al., *Security Problems and Their Defenses in TCP/IP Protocol Suite*, in: Journal of Scientific and Research Publications, Vol. 2 Issue 12, December 2012. Bellovin, S.M., Security problems in the TCP/IP Protocol suite, Computer Communications Review.

Hoffman, Chris, *Why Most Web Services Don't Use End-to-End Encryption*, 2013, http://www.howtogeek.com/166507/why-most-web-services-dont-use-end-to-end-encryption/, accessed on 10 October 2014.

Homepage 'Project: AN.ON - Anonymity.Online', http://jap.inf.tu-dresden.de/index_en.html, accessed on 4 July 2014.

HP Security Research, *HP Research Reveals Nine out of 10 Mobile Applications Vulnerable to Attack*, 2013, http://www8.hp.com/us/en/hp-news/press-release.html?id=1528865#.U9lyJfldVPp, accessed on 15 October 2014.

http://curvecp.org/, accessed on 10 September 2014.

http://en.wikipedia.org/wiki/Hardware_security_module, accessed on 1 November 2014.

http://en.wikipedia.org/wiki/List_of_virtual_communities_with_more_than_100_million_active_users, accessed on 9 October 2014.

http://en.wikipedia.org/wiki/Transport_Layer_Security

http://projectmeshnet.org/, accessed on 10 August 2014.

http://www.cryptophone.de/en/company/, accessed on 13 July 2014.

http://www.nist.gov/

https://cryptech.is/, accessed on 4 July 2014.

https://en.wikipedia.org/wiki/Software_Defined_Perimeter

https://owncloud.org/, accessed on 8 July 2014.

https://wiki.projectmeshnet.org/FAQ, accessed on 4 July 2014.

https://wp.cryptech.is/organization/, accessed on 4 July 2014.

https://www.gnupg.org/, accessed on 8 July 2014.

https://www.libreswan.org/, accessed on 21 July 2014.

https://www.openssl.org/, accessed on 25 August 2014.

https://www.torproject.org/, accessed on 8 July 2014.

https://www.torproject.org/about/overview, accessed on 4 August 2014.

IETF, '*Opportunistic Encryption for HTTP URIs*', draft-ietf-httpbis-http2-encryption-00, expires 14 December 2014, http://tools.ietf.org/html/draft-nottingham-http2-encryption-03, accessed 21 July 2014.

IETF, '*HTTP Strict Transport Security (HSTS)*', final, November 2012, http://tools.ietf.org/html/rfc6797, accessed on 31 July 2014.

IETF, '*SMTP Service Extension for Secure SMTP over Transport LayerSecurity*', undated http://tools.ietf.org/html/rfc3207, accessed 21 July 2014.

Infosec Institute, '*Defending the Internet with Project Meshnet*', 2012 http://resources.infosecinstitute.com/project-meshnet/, accessed on 10 August 2014.

Iyengar, Kishen, '*A Security Comparison of Open-Source and Closed-Source Operating Systems*', 2007 http://www.swdsi.org/swdsi07/2007_proceedings/papers/236.pdf, accessed on 12 August 2014.

Jacobi, A. et al., *Security of eGovernment Systems,* July 2013 http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/513510/IPOL-JOIN_ET(2013)513510(ANN02)_EN.pdf, accessed on 31 July 2014.

Jacobi, A. et al., *Security of eGovernment Systems*', http://www.europarl.europa.eu/stoa/cms/cache/offonce/home/publications/studies;jsessionid=064C72F4A6DC5DEAC8CBE544E382B31F?reference=IPOL-JOIN_ET%282013%29513510, accessed on 4 July 2014.

Jankowski, K. et al., '*Intel Polynomial Multiplication Instruction and its Usage for Elliptic Curve Cryptography*' http://www.intel.co.kr/content/dam/www/public/us/en/documents/white-papers/polynomial-multiplication-instructions-paper.pdf, 2012, accessed on 10 August 2014.

Jankowski, K. et al., '*Multiplication Instruction and its Usage for Elliptic Curve Cryptography*', 2012 http://www.intel.com/content/www/us/en/intelligent-systems/wireless-infrastructure/polynomial-multiplication-instructions-paper.html, accessed on 5 October 2014.

John Gilmore in the cryptography mailing list: "*Re: [Cryptography] Opening Discussion: Speculation on 'BULLRU'*", http://www.mail-archive.com/cryptography@metzdowd.com/msg12325.html, accessed on 25 November 2014.

Juniper, '*Third Annual Mobile Threats Report 2013*', 2013, http://www.juniper.net/us/en/forms/mobile-threats-report/, accessed on 12 August 2014.

Klanke, D. et al., '*Elliptic curves and public key cryptography*', 2013 https://www.projectrhea.org/rhea/index.php/Walther453Fall13_Topic13_paper, accessed on 4 August 2014.

Kulkarni, Mandar M. et al., '*Encryption Algorithm Addressing GSM Security Issues - A Review*', International Journal of Latest Trends in Engineering and Technology (IJLTET) Vol. 2.

Lee, Timothy B., ‘*NSA-proof encryption exists. Why doesn't anyone use it?*’ http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/14/nsa-proof-encryption-exists-why-doesnt-anyone-use-it/, accessed on 10 October 2014.

Lemos, R., '*Keypocalypse' another barrier to encryption systems*', 2014 http://searchsecurity.techtarget.com/feature/Keypocalypse-another-barrier-to-encryption-systems, accessed on 4 November 2014.

Lemos, R., ‘*Keypocalypse' another barrier to encryption systems,* September 2014, http://searchsecurity.techtarget.com/feature/Keypocalypse-another-barrier-to-encryption-systems

Lemos, R., '*Keypocalypse' another barrier to encryption systems*', 2014, http://searchsecurity.techtarget.com/feature/Keypocalypse-another-barrier-to-encryption-systems, accessed on 4 November 2014.

Leong, Khoo Boo, ‘*Why end-to-end encryption holds the key to trusted clouds*’, 2014 http://www.networksasia.net/article/why-end-end-encryption-holds-key-trusted-clouds.1404869534, accessed on 10 October 2014.

Leong, Koo Boo, ‘*Why end-to-end encryption holds the key to trusted clouds*’, 2014 http://www.networksasia.net/article/why-end-end-encryption-holds-key-trusted-clouds.1404869534, accessed on 10 October 2014.

Limer, E., ‘*Mega's Clever Encryption Will Protect You, But Mostly Kim Dotcom*’, 19 January 2013, Gizmodo http://gizmodo.com/5977265/how-megas-encryption-will-protect-you-but-mostly-kim-dotcom, accessed on 15 October 2014.

Lynch, L., ‘*The Black Box Paradox – How to Trust a Secret on Today's Internet*’, 2014, http://www.internetsociety.org/blog/tech-matters/2014/07/black-box-paradox-%E2%80%93-how-trust-secret-todays-internet, accessed on 4 July 2014.

Martin, L., ‘*Key recovery vs. key escrow*’, 2010 http://www.voltage.com/blog/crypto/key-recovery-vs-key-escrow/, accessed on 13 July 2014.

Mateti, P., ‘*Security Issues in the TCP/IP Suite*’, 21 November 2006, World Scientific Review Volume 9.

Mattsson, J., ‘*Is Opportunistic Encryption the Answer? Practical Benefits And Disadvantages*’, 2014 https://www.w3.org/2014/strint/papers/27.pdf, accessed on 21 July 2014.

McLachlan, J. et al., ‘*Scalable onion routing with torsk*’ in Proceedings of the 16th ACM conference on computer and communications security, ser. CCS ’09. New York, NY, USA: ACM, 2009, pp. 590–599.

Mendonca, M. et al., ‘*A Flexible In-Network IP Anonymization Service*’, 2012 http://yuba.stanford.edu/~srini/papers/icc-sdn12.pdf , accessed on 4 August 2014.

Metropolitan Police, ‘*press release of Commissioner Bernard Hogan-Howe of the Metropolitan Police*’, 6 November 2014, see: http://content.met.police.uk/News/Commissioners-US-visit/1400027598397/1257246745756

Microsoft, *What is the Security Development Lifecycle?*, undated, http://www.microsoft.com/security/sdl/default.aspx

Mimoso, M., ‘*Internet-traffic-following-malicious-detours-via-route-injection-attacks*’, 20 November 2013, Threatpost.com http://threatpost.com/, accessed on 24 November 2014.

Mozilla Developer Network, ‘*HTTP Strict Transport Security*’, 2012 https://developer.mozilla.org/en-US/docs/Web/Security/HTTP_strict_transport_security, accessed on 31 July 2014.

National Institute for Standards and Technology, '*NISTIR 7977 NIST Cryptographic Standards and Guidelines Development Process (Draft'*), 2014.

Neal, R., '*PRISM-Proof Your Smartphone: 10 Apps To Keep The NSA Out Of Your Phone*', 2013 http://www.ibtimes.com/prism-proof-your-smartphone-10-apps-keep-nsa-out-your-phone-1321085, accessed on 13 July 2014.

Network Working Group of The Internet Society, '*BGP Security Vulnerabilities Analysis*', 2006.

New York Times, '*No Morsel Too Minuscule for All-Consuming N.S.A.*', 2 November 2013, http://www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html?_r=1&&pagewanted=all, accessed on 24 November 2014.

New York Times, '*Secret Documents Reveal N.S.A. Campaign Against Encryption*', 5 September 2013, accessed on 25 November 2014.

New York Times, '*Secret Documents Reveal N.S.A. Campaign Against Encryption*', 5 September 2013, http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?_r=1&, accessed on 20 November 2014.

NIST, '*Public Comments Received on NISTIR 7977: NIST Cryptographic Standards and Guidelines Development Process (Draft)*', 2014.

NIST, '*Recommendation for Key Management – Part 1: General (Revision 3)*', 2012, NIST Special Publication 800-57.

NIST, '*Security Requirements For Cryptographic Modules*', 2001, FIPS PUB 140-2.

NSA, '*The Case for Elliptic Curve Cryptography*', 15 January 2009, http://www.nsa.gov/business/programs/elliptic_curve.shtml, accessed on 4 August 2014.

Oltheanu, Alexandra and Guillaume Pierre, '*Towards Robust and Scalable Peer-to-Peer Social Networks*', 2012, ACM, http://reconcile.pjwstk.edu.pl/AppData/Files/SNS12_Alexandra_Olteanu_authors_version.pdf, accessed on 3 October 2014.

OSHWA, '*Open Source Hardware (OSHW) Statement of Principles 1.0*', http://www.oshwa.org/definition/, accessed on 4 August 2014.

osmocom.org, accessed on 1 November 2014.

OWASP, *Secure SDLC Cheat Sheet*, undated https://www.owasp.org/index.php/Secure_SDLC_Cheat_Sheet

Payment Card Industry, '*Data Security Standard. Requirements and Security Assessment Procedures, Version 3.0*', 2013, https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0 , accessed on 31 July 2014.

Peterson A., '*Yahoo to roll out end-to-end encryption option for all Yahoo Mail users in 2015*', 7 August 2014, Washington Post, http://www.washingtonpost.com/blogs/the-switch/wp/2014/08/07/yahoo-to-role-out-end-to-end-encryption-option-for-all-yahoo-mail-users-in-2015/ , accessed on 20 August 2014.

Ponemon, Global Encryption Trends Study, 2014.

Ransbotham, S., '*An Empirical Analysis of Exploitation Attempts based on Vulnerabilities in Open Source Software*', 2010, Workshop On The Economics Of Information Security, http://weis2010.econinfosec.org/papers/session6/weis2010_ransbotham.pdf , accessed on 20 May 2014.

Renaud K. et al., '*Why Doesn't Jane Protect Her Privacy?*', paper for the 14th Privacy Enhancing Technologies Symposium, 2014.

Richardson, R., '*Open source needs some sort of body that promotes secure architectural design and coding*', 2011, Open source needs more than the Open Crypto Audit Project, http://searchsecurity.techtarget.com/opinion/Open-source-needs-more-than-the-Open-Crypto-Audit-Project, accessed on 4 November 2014.

Robachevsky, A. et al., '*The Danger of the New Internet Choke Points*', 2014 http://www.internetsociety.org/sites/default/files/The%20Danger%20of%20the%20New%20Internet%20Choke%20Points_0.pdf, accessed on 20 August 2014.

Roberts, P., '*Pervasive Internet Surveillance – The Technical Community's Response (So Far)*', 2014 http://www.internetsociety.org/blog/tech-matters/2014/06/pervasive-internet-surveillance-technical-community-response-so-far , accessed on 4 July 2014.

Roberts, P., '*Pervasive Internet Surveillance – The Technical Community's Response (So Far)*', 2014 http://www.internetsociety.org/blog/tech-matters/2014/06/pervasive-internet-surveillance-technical-community-response-so-far, accessed on 4 July 2014.

Rockman, S., '*Vodafone Germany looks to provide end-to-end encryption with SIM signatures*', 11 March 2014, The Register http://www.theregister.co.uk/2014/03/11/vodafone_germany_takes_g_and_d_secure_sim/, accessed on 13 July 2014.

Rosenblatt, S., '*New Chrome extension hopes to demystify encryption*', 2014 http://www.cnet.com/news/new-chrome-extension-hopes-to-de-mystify-encryption/, accessed on 13 July 2014.

Rouse, M., *Elliptical curve cryptography (ECC)*, undated, http://searchsecurity.techtarget.com/definition/elliptical-curve-cryptography, accessed on 4 August 2014.

RSA Laboratories, '*4.1.2.1 What Key Size Should Be Used?*', undated, http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/key-size.htm, accessed on 20 November 2014.

RT, '*Spy agencies seek to store Aussies' web-browsing histories, end encryption*', 2014 http://rt.com/news/australia-nsa-snowden-surveillance-510/, accessed on 13 July 2014.

Sakr, S., '*Back off, NSA: Blackphone promises to be the first privacy-focused smartphone*', 2014 http://www.engadget.com/2014/01/15/blackphone-privacy-and-security-android-smartphone/, accessed on 10 August 2014.

Sankey, J. and Wright, M., '*Dovetail: Stronger Anonymity in Next-Generation Internet Routing*', PET symposium 2014 papers, 2014.

SANS Institute, '*An Overview of Hardware Security Modules*', 2002, http://www.sans.org/reading-room/whitepapers/vpns/overview-hardware-security-modules-757

Scarfone, K. et al., '*Guide to Storage Encryption Technologies for End User Devices*', 2007 http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist800111.pdf, accessed on 20 August 2014.

Schneier, B., *'Homomorphic Encryption Breakthrough'*, 2009, https://www.schneier.com/blog/archives/2009/07/homomorphic_enc.html, accessed on 5 August 2014.

Schneier, B., *'The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption'*, 1998 https://www.schneier.com/paper-key-escrow.html, accessed on 13 July 2014.

Schryen, G., *'Security of Open Source and Closed Source Software: An Empirical Comparison of Published Vulnerabilities'*, 2009 http://www.bibsonomy.org/bibtex/b72580b5932700da4873fe1ba70134aa, accessed on 12 August 2014.

Skorobogatov, S. and C. Woods, *'Breakthrough silicon scanning discovers backdoor in military chip'*, 2012.

Soghoian, C., *'Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era'*, 8 Journal on Telecommunications and High Technology Law 359; Berkman Center Research Publication No. 2009-07, http://www.jthtl.org/content/articles/V8I2/JTHTLv8i2_Soghoian.PDF, accessed on 13 July 2014.

Somogy, S., *'Making end-to-end encryption easier to use'*, 2014 http://googleonlinesecurity.blogspot.in/2014/06/making-end-to-end-encryption-easier-to.html, accessed on 20 August 2014.

Stackexchange, *'Are phone calls on a GSM network encrypted?'*, 2013 http://security.stackexchange.com/questions/35376/are-phone-calls-on-a-gsm-network-encrypted

Stanford, *'Encryption Backdoors'*, undated, http://cs.stanford.edu/people/eroberts/cs201/projects/ethics-of-surveillance/tech_encryptionbackdoors.html , accessed on 31 July 2014.

STOA, *'Security of eGovernment Systems - Conference Report'*, 2014.

Süddeutsche Zeitung, *'BND leitete Telefondaten an NSA weiter'*, 24 June 2014, http://www.sueddeutsche.de/digital/geheimdienste-bnd-leitete-telefondaten-an-nsa-weiter-1.2016504, accessed on 9 October 2014.

Symantec, *'Internet Security THREAT REPORT 2013'*, 2013 http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf, accessed on 12 August 2014.

Taylor, S. and Wexler, J., *'The pros and cons of IPSec'*, 11 November 2004, accessed on 26 November 2014.

Tech Republic, *'Corporate espionage or fearmongering? The facts about hardware-level backdoors'*, 2013 http://www.techrepublic.com/blog/it-security/corporate-espionage-or-fearmongering-the-facts-about-hardware-level-backdoors/, accessed on 20 August 2014.

The Guardian, *GCHQ taps fibre-optic cables for secret access to world's communications*, 21 June 2013, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

Thomson, I. *'NIST denies it weakened its encryption standard to please the NSA'*, 11 September 2013, The Register, http://www.theregister.co.uk/2013/09/11/nist_denies_that_the_nsa_weakened_its_encryption_standard/, accessed on 20 November 2014.

Trustwave, *'Trustwave Unveils End-to-End Encryption Software Solution'*, 2010, Trustwave, https://www.trustwave.com/Company/Newsroom/News/Trustwave-Unveils-End-to-End-Encryption-Software-Solution/, accessed on 10 October 2014.

University of Maryland, *'Random, but not by chance: A quantum random-number generator for encryption, security'*, 19 April 2010, ScienceDaily www.sciencedaily.com/releases/2010/04/100414134542.htm, accessed on 4 August 2014.

US Department of Defense, '*Global Information Grid Architectural Vision*', 2007.

VPN Services Reviews, *'Advantages and Disadvantages of IPsec'*, undated, http://vpn-services.bestreviews.net/advantages-and-disadvantages-of-ipsec/, accessed on 26 November 2014.

Wagenseil, P., *'HTTP Must Die, Security Experts Tell Hackers'*, 18 July 2014, Tom's Guide http://www.tomsguide.com/us/http-must-die,news-19188.html, accessed on 21 July 2014.

Waldrop, M., *'DARPA and the Internet Revolution'*, 2008, http://www.darpa.mil/WorkArea/DownloadAsset.aspx?id=2554, accessed on 3 August 2014.

Weinstein, L., *'No, I Don't Trust You! – One of the Most Alarming Internet Proposals I've Ever Seen'*, 22 February 2014, Vortex http://lauren.vortex.com/archive/001076.html, accessed on 31 July 2014.

Wheeler, D., *'Secure Programming for Linux and Unix HOWTO, Chapter 2, Is Open Source Good for Security?'*, 22 August 2004, http://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO/index.html , accessed on 12 August 2014.

Whitten, A. and Tygar, J., *'Why Johnny Can't Encrypt'*, Security and Usability: Designing Secure Systems that People Can Use, eds. L. Cranor and G. Simson. O'Reilly, pp. 679-702, 1999.

Willis, N., *'Should the IETF ship or skip HTTP 2.0?'*, LWN.net *http://lwn.net/Articles/600525/* , accessed on 31 July 2014.

www.ciphershed.org, accessed on 8 July 2014.

Yeung, C. et al., *'Decentralization: The Future of Online Social Networking'*, 2008 http://www.w3.org/2008/09/msnws/papers/decentralization.pdf, accessed on 3 October 2014.

Zhang, M., *'A Censorship-Free Alternative to the Global Internet?'*, 2012, https://opennet.net/blog/2012/08/censorship-free-alternative-global-internet, accessed on 10 August 2014.

Interviews

The following experts were interviewed:

Mr Axel Arnbak, University of Amsterdam (NL)

Mr Brent Bilger, Vice-President Solutions Architecture at Vidder (USA)

Mr Caspar Bowden, independent privacy researcher (UK)

Dr Christian Doerr, University of Delft (NL)

Mr Rickey Gevers, forensic investigator at Digital Investigations (NL)

Ms Monika Maglione, Mr Michael Palmer and Ms Cecilia-Joanna Verkleij (EC-DG Home)

Mr Gopal Padinjaruveetil, Chief Security and Compliance Architect, Capgemini US (USA)

Mr Rejo Zenger and Mr Hans de Zwart, Bits of Freedom (NL)

Capgemini Cyber Security Community of Practice: *Mr Jule Hintzbergen, Mr Cees de Kuijer, Mr Guido Voorendt, Mr Jan Willem de Vries and Mr Jack van 't Wout.*

Annex B. Technology themes

This annex is in a separate document.

Annex C. List of abbreviations

AES	Advanced Encryption Standard
ANPR	Automatic Number Plate Recognition
ANSI	American National Standards Institute
AppB	Application Binding
ARP	Address Resolution Protocol
AS	Autonomous System
BGP	Border Gateway Protocol
BS	British Standard
BYOD	Bring Your Own Device
CA	Certificate Authority
CRASH	Clean-slate design of Resilient, Adaptive, Secure Hosts
CRL	Certificate Revocation List
DARPA	Defense Advanced Research Projects Agency
DCAP	Data Centric Audit and Protection
DDoS	Distributed Denial of Service attack
DIME	Dark Internet Mail Environment
DISA	Defense Information Systems Agency
DIY	do-it-yourself
DNS	Domain Name System
DNSSEC	DNS Security Extensions
DoD	(US) Department of Defense
DPA	Differential Power Analysis
DPI	Deep Packet Inspection
DSA	Digital Signature Algorithm
DV	Device Validation
E2EE	End-to-End Encryption
ECC	Elliptic Curve Cryptography
EDA	Electronic Design Automation
EFF	Electronic Frontier Foundation
ENISA	European Union Agency for Network and Information Security
EU	European Union
FDE	full disk encryption
FIPS	Federal Information Processing Standard
FIRE	Future Internet Research & Experimentation
FISA	Foreign Intelligence Surveillance Act
FPGA	Field-programmable gate array
GCHQ	Government Communications Headquarters
GPG	GNU Privacy Guard
GSM	Global System for Mobile Communications
HACMS	High-Assurance Cyber Military Systems
HDL	Hardware Description Language
HMAC	Keyed-Hash Message Authentication Code specified in [FIPS198]
HSM	Hardware Security Module
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol

HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
IARPA	Intelligence Advanced Research Projects Activity
ICMP	Internet Control Message Protocol
ICT	Information & Communication Technology
IDRP	ICMP Router-Discovery Protocol
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IoT	Internet of Things
IP	Internet Protocol
ISO	International Standards Organization
ISP	Internet Service Provider
IT	Information Technology
IXP	Internet Exchange Point
KMIP	Key Management Interoperability Protocol
LAN	Local Area Network
LIBE	Committee on Civil Liberties, Justice and Home Affairs
MAC	Message Authentication Code
MNO	mobile network operators
MRC	Mission-Oriented Resilient Clouds
mTLS	mutual transport layer security
NAP	Network Access Points
NAT	Network Address Translation
NATO	North Atlantic Treaty Organization
NFS	Network File System
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OS	Operating System
OSH	Open-Source Hardware
OSI	Open Systems Interconnection
OSS	Open-Source Software
OTR	Off The Record
OWASP	Open Web Application Security Project
P2P	Peer to Peer
PAR	Positive Acknowledgment and Retransmission
PCI-DSS	Payment Card Industry - Data Security Standard
PCLMULQDQ	PC Carry-Less Multiplication Quadword
PCSM	Personal Computer Security Module
PKI	Public-Key Infrastructure
PROCEED	Programming Computation on Encrypted Data
PSTN	Public Switched Telephony Network
R&D	Research & Development
RA	Registration Authority
RFC	Request For Comments (IETF)
RNC	Radio Network Controller
RPC	Remote Procedure Call

RPKI	Resource Public Key Infrastructure
RSA	Rivest, Shamir, Adelman (an algorithm)
SaaS	Software as a Service
SAM	Secure Application Module
SAML	Security Assertion Markup Language
SCADA	Supervisory control and data acquisition
SCIP	Secure Communications Interoperability Protocol
SDN	Software Defined Networks
SDP	Software Defined Perimeters
SHA	Secure Hash Algorithm
SIGINT	Signals Intelligence
SMTP	Simple Mail Transfer Protocol
SMTP	Simple Mail Transfer Protocol
SPA	Single Packet Authorisation
SPAR	Security and Privacy Assurance Research
SSH	Secure Shell
SSL	Secure Socket Layer
STOA	Science and Technology Options Assessment
SUNET	Swedish University Network
TCP	Transmission Control Protocol
TDEA	Triple Data Encryption Algorithm; Triple DEA
TLS	Transport Layer Security
Tor	The Onion Router
TPM	Trusted Platform Module
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
USB	Universal Serial Bus
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
XAUTH	Extended Authentication
XRD	External Data Representation

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