Mass Surveillance : Technology foresight, options for longer term security and privacy improvements

The purpose of this policy brief is to provide the Members of the European Parliament with technology oriented policy options, regarding the protection of the European Information Society against mass surveillance. Four main themes have been identified corresponding to eleven different policy options.

Theme I: "Promote adoption of existing good practices"

1. End to End encryption (E2EE)

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

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

Support product security tests by independent institutions like 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 regular **own product security test program**.

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

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

2. Open Source Software (OSS)

Despite the fact that it is not a universal remedy, Open Source Software (OSS) still is an important ingredient in a 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, like OpenSSL, TrueCrypt/Ciphershed, GPG, Tor, OwnCloud, et cetera need funding to keep going and be audited (both on code and processes).

Initiate an European "OSS Bug Bounty Program" or finance existing programs, as alternative for intervening directly with specific OSS programs.

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. 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, though not the easiest one since the European market is open, fragmented and major platforms are already available for all *current* services categories.

A stronger **legal limits on exporting personal data** than what the coming Data Protection regulation will provide European ICT players the time and legal space necessarily to create a demand for specific EU solutions. **Liability and substantial fines** for non-compliance will also provide a strong stimulus for action.

4. Secure software development

Encourage the **use of existing guidelines** for secure software development, like the OWASP Top 10. Security is not just a job 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 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 usually cannot assess nor mitigate.

Theme II: Build Confidence among users

5. Security baselines

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

6. 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.

Theme III: Consider implementation of more disruptive initiatives

7. EU Certification schemes

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

8. EU Internet Subnet

To prevent network routing information from being intercepted for meta-data 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 best way forward, other approaches such as **deperimeterization** at the data and application level should be considered 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.

Theme IV: Enable longer term innovation

9. Stimulate R&D into reduced track/traceability of users and better detection of surveillance

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

Fund **open source tools** that enhance privacy/block traceability. **Regulate a**n obligation (for 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: **regulate no-traceability as requirement** as part of security by design for (personal and or mobile) devices.

10. 'Fix the Internet' – promote improvement of inherent insecure protocols

The EU can be **stimulating more secure open standards** for Internet protocols by supporting **individual contributions** and by setting-up **dedicated long term R&D efforts** in cooperation with the academic world, ISPs, the IETF and other organizations involved with the research and co-development of open standards.

Finally, for protocols that are considered to be insecure (and most are), when a cure can-not be easily obtained, **depreciation of that protocol** should be considered by public **regulation**.

11. Data Centric Security

Set up a specific EU **Research & Development program** 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 is 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 while communicated, but ease of use and (proactive collective) implementation must to be pursued to achieve sufficient scale in terms of number of users. Europe should furthermore set up its own **certification schemes** for encryption standards, to mitigate the risk of backdoors. Mind that should **quantum computing** become available, this and other encryption options should be reconsidered obsolete immediately.
- **Deperimeterization 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. EU should invest in code review and certification schemes and facilities for OSS.
- The EU should increase its efforts in fixing 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 currently proposed in the coming **Data Protection regulation** on personal data export would for instance create the breathing space the European (OSS) ICT needs to build up a substantial market position and enough scale to survive independently.

Also **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 widen the possibilities for surveillance dramatically 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 currently.

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 regards 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 unsatisfying for all sides.

Based on a STOA study by the same title published in December 2014 (PE 527.410).

Editor:
Capgemini Consulting, part of Capgemini Netherlands BV.

Authors:
M. van den Berg, P. de Graaf, P.O. Kwant, T. Slewe

For further information, please contact:
Peter Ide Kostic, Scientific Foresight (STOA) Unit
Directorate for Impact Assessment and European Added Value
Directorate-General for Parliamentary Research Services
European Parliament
Rue Wiertz 60 - SQM 02Y014, B-1047 Brussels
E-mail: stoa@europarl.europa.eu