Committee on Civil Liberties, Justice and Home Affairs
Science and Technology Options Assessment Panel
The Luxembourg Presidency of the EU Council
(co-chaired by the Committee on Internal Market and Consumer Protection
and the Committee on Industry, Research and Energy)

High-Level Conference

Protecting Online Privacy by enhancing IT Security and strengthening EU IT Capabilities

Tuesday 8 December 2015, 15.00 - 18.00
Wednesday 9 December 2015, 09.00 - 13.15
Brussels

"Top-3" policy recommendations

Twitter: #EUdataP

Eric Filiol

Theme I

-Making mandatory the use of end-to-end encryption for EU and commercial services

-Develop the EU industry and market of secure, encrypted phone available for every EU citizens

-Adopt stronger legal regulations (jail/fine) in case of prosecuted people do not accept to provide cryptographic keys to investigation judges/police

Theme II

-Establishing a binding policy for software publishers and hardware manufacturers in terms of software/hardware security including criminal and civil penalties.

-Make illegal any kind of intended backdoor

-Adopt a European Internet (infrastructure/protocols/software) which is interoperable with the existing Internet but totally under control of the EU

Theme III

-Include the inalienable right to privacy and data security for EU citizens in the European Constitution

-Give Europe a statute to protect the alert launchers (whistle-blowers) and give them official status

-Forbid any security technology that is non designed, non-implemented in the EU by EU state members and EU industry (excluding external companies' subsidiaries/affiliates branches located in the EU)

***

Melle van den Berg

-PETS: stimulate development of user-friendly encryption, dramatically increase security of mobile communication, stimulate research on how people actually use technology

-Soft- and hardware: stimulate certification schemes, incentivize better security (introduce liability for bad soft/hardware), pay for upkeep of essential Internet infrastructure

-Euro IT industry: Invest in education, prioritize hubs and incentivize (low rents, high-speed broadband), put a premium on using EU products (see certification recommendation in 2)

***

Richard Clayton

-A binding statement of intent from the EU that the long term requirement to promote and maintain trust in cyber-infrastructure should always outweigh subverting that infrastructure for any short- term gain, however laudable the particular motive might be, however up-standing the users of the backdoor might be, or however awful the event that reopened the debate.

-Legislation to make all software developers liable for gross negligence by 2020 and for all consequences of their product development by 2030.

-Removing all requirements to notify anyone of the loss of data when it was encrypted to a formally agreed standard and there was clear evidence that the keying material required to decode the data had not been, and would not in the future be, compromised.

Christian Grothoff

Theme I

-Horizion 2020 stresses way too much the need for solutions for which there is a business model. Already the formulation in the question "lab-to-market" is leading in the wrong direction: Most quality privacy enhancing technology that is actually used by citizens is not sold, but instead made freely available (Tor, GnuPG, SSL, hard drive encryption, etc.) as free software. Looking for sustainable business models is thus counterproductive, as it eliminates one good way for the government to fund privacy enhancing technologies that would have the biggest impact. This even applies to commercial exploitation, as often SMEs do build their systems on top of existing free software tools and libraries. However, those users are typically not easily identified during the proposal phase and would also not allow reviewers to identify a "sustainable" business model, even though the software enables industry. The EU should revise this rule and evaluate projects on how they will impact society at large, and specifically recognize that free software is more likely to have a bigger positive social impact than commercially successful products. Thus, EU should prefer funding free software over funding commercializable software, especially for privacy enhancing technologies as here the ability to verify the sources and to address problems is critical for quality, sustainable solutions.

-Key escrow and other methods that weaken security of all citizens merely to make it easier for the police to catch criminals is not a good solution. The EU needs to recognize that we must not create insecure systems supporting totalitarian control to save the EU from criminal, totalitarian threats. Of course criminals use transportation, communication and payment systems -like all other citizens. Locking down transportation, disabling communication ("Internet Kill Switch") or denying access to basic financial services is virtually always going to make the situation worse. Instead, targeted measures that focus on the criminal activity need to be used. The police can still place bugs in the perpetrators environment (like the US did in EU embassies), or track the shipment of contraband (weapons, illegal drugs, etc.). Such targeted measures also have the advantage that the funds are guaranteed to be spend well, and that the police will pay attention to the information that they acquire. Today, information overload is a major problem; police ignoring credible warnings they receive will not be addressed by providing them with even more information.

-Future mobile phone standards should require location privacy (to be disabled if and only if a person calls an emergency number). Carriers may claim that this is technically not feasible, but if we stop to use subscriber information numbers and switch to zero-knowledge authorization schemes instead of authentification for access control, we could technically provide very good location privacy in 5G, which would also protect our citizens in a hypothetical future drone war that the US, Russians or Chinese may wage against us: When the Pakistani and Afghans deployed 2G, they also could not conceive that this decision would kill tens of thousands of their innocent citizens.

Theme II

-Administrators of BGP and DNS are a threat to the stability and availability of the Internet, both because they wield significant power and because this makes them high-profile targets for attacks (see the NSA's intrusion of Stellar). However, neither securing BGP nor DNSSEC addresses this problem. Instead, we need to move towards self-organizing systems where administrators are eliminated. In a self-organizing system where routers pick the shortest uncongested path, the only way to hijack a route is to build a faster connection, which is expensive and in case of existing local links in fact impossible. Similarly, we have alternatives to DNSSEC like NameCoin and the GNU Name System for self-organizing name systems (replacing DNS) where administrators can no longer hijack or censor names. Thus, the EU should prioritize self-organizing decentralized systems over half-baked problematic security "enhancements" like DNSSEC or DNS-over-TLS (aka confidential DNS), which add excessive complexity to an already complex system and also introduce additional vulnerabilities.

-To secure software, we do should treat it as any other good without special rules or special exceptions. Liability for software should be subject to the same rules as any other product. A major issue today is that anyone discovering bugs and trying to practice responsible disclosure is facing legal uncertainty: by disclosing that a vulnerability was found, one risks being prosecuted under various hacking laws. Here, a clear regulation that indemnifies anyone who discloses vulnerabilities in a responsible way would be beneficial. The rules should require (1) a serious attempt to contact the vendor or author of the software (who may then fix the vulnerability), (2) if the vulnerability is not fixed in a timely fashion, escalation to an information security escalation contact (such as a CERT), followed by (3) publication of the details of the exploit to the general public. The legislation should then indemnify anyone who proceeds from (0) finding the vulnerability through steps (1)-(3) within say 2-4 weeks intervals, and who did not deliberately or by gross negligence cause significant harm during step (0).

-To avoid IoT technologies from sending every tiny bit of information about EU citizens to the US, the EU should eliminate US Safe Harbor status and force US Internet companies to create legally separate entities for the EU where the entire business is hosted, operated and taxed in the EU. Today corporations that have any business in the US fall under US laws, which require these corporations to violate EU data protection laws. This can only be resolved under the rule of law by forcing these corporations to split. This will also be beneficial for the EU as tax evasion will become less of an issue, and more of the value creation will happen within the EU. (Naturally, I do not expect the EU/EC to adopt this stance, as it is unbecoming for a wholy owned subsidiary. However, we will see that China will do quite well with this approach.).

Theme III

-If the EU can overcome its fear of terrorism, it might become a hotbed for privacy enhancing technologies, as especially the German technical community is quite competitive in this regard. Key supportive regulation in this domain would be the universal deployment of IPv6. The EU should mandate all ISPs to offer at least 1024 global IPv6 addresses to each subscriber by 2020. Non-compliant companies should loose their license to operate a communication service. Strict enforcement of this rule would enable both certain privacy enhancing technologies and IoT development, and prevent the broadening of a black market for IPv4 addresses.

-Privacy-enhancing payment systems based on Chaum's blind signatures have the potential for opening up entirely new online business models that are NOT driven by advertising. Today, online publishers suffer because neither sales nor advertising provide sufficient revenue. OTOH, existing payment processes with credit cards take too long to be executed for simply reading an online article. A modern system, similar to Chaum's DigiCash from 1990 but implemented as an open standard to be compatible with the modern Web, would enable online businesses to obtain micropayments and thereby enable business models beyond Big Data and advertising, opening market opportunities and improving privacy at the same time. The EU should thus ensure that its regulation enables reasonable alternative privacy-preserving payment systems (which of course must still provide sufficient transparency to ensure that the merchants offer legal services and not enable black markets or tax evasion).

-Meta projects tend to create mega failures, or at least create significant cost overruns or underdeliver on the promises. Projects like the "Human Brain Project" are not going to deliver on a fraction of the initial promise, and significantly less than what could have been achieved -- and will naturally still be celebrated as a great success, as acknowledging that the EU wasted EUR 2 billion would be too embarrassing. However, that does not mean that doing more mega-projects would be productive. In fact, it might be better to cap the maximum number of participants in any Horizon 2020 project to 4-6 to create focused teams and reduce management overheads. Other metrics to improve the value obtained from EU projects would be to fund software maintenance as follow-up projects, as many projects fail to transition from research prototypes into practice because funding the necessary maintenance work for free software is virtually impossible under the current regime. As a result, many prototypes that may benefit society are never allowed to reach the necessary maturity. Here, funding for software engineers to work at universities to maintain free software would be helpful.

Evangelos Markatos

-Support Research in the area of Privacy and Data Transparency. Currently there is very little transparency on the web today. Users are asked for their data but do not know which data exactly will be collected and what will they be used for. This research will allow users to get real control of their data and will create a healthy open market where trackers will be able to transparently use the data provided by the users.

-Require web sites to provide service even to users that refuse to accept third-party cookies or any other third-party tracking information. Currently, if users do not consent to accept the provided cookies, they receive very poor service, if any at all. Such poor service would not be tolerated in real life situations. For example, most of the services we take for granted (e.g. hotels, restaurants, stores, etc.) in real life cannot refuse their services unless they have a very good reason. Maybe what we take for granted in real life should also be enjoyed by all citizens in cyber space as well.

***

Björn Rupp

-Enforce the highest, peer-reviewed standards in IT security

-Invest in trustworthy, pan-European certification processes

-Do not succumb to dangerous demands from some national governments to weaken encryption

***

Paul Syverson

Theme I

-Policies stimulating adoption of privacy enhancing technologies including End to End encryption and anonymization tools.

-Encourage communication technologies that minimize the creation of non-ephemeral metadata (metadata existing substantially longer than needed to successfully complete a given communication).

-Require government service and information sites to offer .onion addresses bound to the registered domains for their sites to provide stronger site authentication and stronger communication protection for users of government services.

-Encourage technologies that diversify trust: in agencies, countries, companies, etc. for both data and metadata, in particular avoid single points of trust not under user control.

Theme II

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

-Encourage development and deployment of technologies that cryptographically protect the confidentiality and authentication of routing information and other metadata, as well as permit confirmation of these for specific communications by the communicants.

-Compelled technical access (e.g., mandated back doors) is recognized as an increase in attack surface and weakening of technical security by all leading scientific experts in the field. Thus, in the interest of citizens, but also of national security for individual countries and security at a regional level, create an EU policy that clearly states strong encryption is essential for securing devices and networks and that neither EU nor national security is compatible with any form of compelled technical access.

-Encourage nations to adopt requirements that purchasers of equipment or software must give informed consent for any and all settings or intentional access mechanisms in purchased systems that would give access to others than the purchaser or those the purchaser designates. Requirements should include or be accompanied by penalties adequate to discourage violations. For example, if the purchaser is a government, exclusion of the seller from contracts or sales to any EU government for an appropriate period.

***

Aral Balkan

-Champion Ethical Design (see https://ind.ie/ethical-design) in technology

-Encourage and support the creation of organisations to build decentralised, peer-to-peer, zero-knowledge communication platforms

-Effectively regulate the human rights abuses of technology companies like Google, Facebook, etc., whose core business model is to track and farm people.

***

Steven J. Murdoch

-Focus should be on who has control and responsibility over data, rather than the physical location of data or where it is processed

-Strengthen security technologies and encourage wider use, rather than proposing restrictions on security

-Support good engineering, including proper consideration of human behaviour. This will help security as well as improving IT more generally.

***

Bart Preneel

-Foster highly distributed and robust security and privacy architectures where data stays under local control, where there is no single point of failure, and where there is end-to-end protection. The architectures can be reviewed by a board of top level experts (who can also develop model solutions); adoption should be driven by increasing liability for centralized architectures.

-Stimulate the development and deployment of open software and hardware solutions by creating an eco-system that supports development and reviews (integrated governance). The market could be driven by liability regimes and by public procurement.

-Create a multidimensional approach towards the open evaluation and certification of security and privacy solutions by supporting training for architects and developers, the creation of open tools for security and privacy evaluation, bounty programs, and audits. Encourage adoption through public procurement programs and through reducing liability according to the number and depth of elements present in the certifications.

***

Stephan Lechner

-Ban, tax or penalise weak technologies ("0000"-Passwords, sensitive data transmission without encryption, systems that require root access for all, etc.).

-Create a general but dynamic European Security label for software, hardware and IT services. The label should differ between the two dimensions of security and privacy, and could be based on community knowledge about bugs and features in IT products and services, therefore change dynamically like a credit rating. (Do not re-invent the Common Criteria or the BS7799 / ISO 27000 series!).

-Create an obligation for IT vendors to fix known bugs within a 3-6 month timeframe (and provide the bugfixes as downloads for free and without any access restrictions).

***

Susan Landau

As our society moves into the Big Data world, we are in a situation of ubiquitous collection.

-Begin a serious discussion on requirement for controlling use of data and on publication of information on data retention. For example, automatic toll collection on highways involves collecting and storing information on cars that do not have the appropriate pass. How long is the data retained? Where is it stored? Who has access to it?

-Have a public discussion to develop binding rules for government revelation of vulnerabilities in cyber infrastructure. Note that this allows for subtleties in the policy, and does not say all vulnerabilities must be revealed upon discovery.

-Starting with software used in regulated industries, develop a comprehensive plan for introducing a regime of liability for software. This would include timetables for when regulations into effect, in which industries, and for which level of failure - as well as a plan to expand past the regulated industries.

***

Aggelos Kiayias

Theme I

-Enforce user-facing aspects of EU privacy directives to be implemented in uniform and unified way across industry (e.g., notice and consent should be given in a unified way, accessing the data should be provided in a unified way). In this way the users within EU will be able to better manage their private data across different providers as they will be operating a familiar interface. This may be achieved by a combination of legal enforcement (e.g., industry should conform to given precise specifications in the user interface) and

technological innovation and development (e.g., by providing a platform / framework that should interoperate with all systems via an API).

-EU services should emphasize and support decentralization in all aspects and layers. Single points of failure in the security and trust model should be identified and eliminated through R&D as needed.

R&D projects (H2020 etc.) that aim in improving privacy should have a de-emphasised connection with specific business cases. Privacy tools should be made freely available for testing, experimentation and adoption.

-Lawful access and interception should be facilitated only at the end-points of communication and not along the communication route. The infrastructure of the latter should be content and meta-data oblivious and developing such infrastructure can be an R&D priority.

-Provisions for EU wide whistle-blower protection and facilitation of it at the technical level should be made.

-Systematization of privacy aspects of EULAs so that they are readily parsed by all end-users without requiring to understand legal text can be helpful. For instance, the EULA may just point to one of a handful of types of data collection and processing profiles that conforms to the product.

Theme II

-Open source software systems that are adopted by the EU public services should also have access to bug finding and bug bounty programmes (the infrastructure for this may be funded by the public but not the bounties themselves – except for special cases for software that has been considered very thoroughly vetted).

-Suitable privacy-preserving overlays reduce content and metadata available in the Internet. While changing infrastructure may be difficult identifying and making suitable amendments so that overlays are more efficiently carried by the underlying network would facilitate more widespread use of privacy-preserving systems on EU grounds. Supporting such privacy-preserving overlays can be a priority.

Theme III

-Systematization of EU privacy directives and their implementation as suggested above (in theme-I) can allow advertising the related technology to an international audience and its adoption by service providers outside EU. Europe can be a leader in the export of privacy-preserving services and an EU privacy stamp can become associated with a high level assurance in terms of data protection.

-An alternative goal of Europe being autonomous could be that services offered in Europe's grounds are upheld to higher standards of data protection even though they share basic infrastructure with components / elements outside EU that are untrusted. This is a technological challenge that should be pursued and recognizes that many times the enemy is "from within." Developing complete autonomy in a global interconnected world may be unrealistic.

-Developing services that meaningfully and uniformly encode privacy and data protection directives can be a "grand challenge" for the EU R&D sector.

***

Arne Babenhauserheide

Theme I

-PGP/GPG is proven: Bind vendors to ship compatible software with every system. Solves part of the chicken-egg problem. Allows using PGP/GPG against spam.

-Different tools for different use cases.

-Forbid pressure to give up keys. By basic principles of law no one has to incriminate him- or herself and people must be deemed innocent unless proven otherwise. If we want computers to be extensions of ourselves and we want people to trust their tools, this has to apply to the tools, too. Forbid retroactive surveillance.

-Bind data in services to need: Must only store what is needed to provide the service.

-Freenet provides confidential communication between friends, pseudonymous publishing and spam-resistant pseudonymous communication. All three are needed to have digital communication on par with analogue communication. Freenet still needs work on usability and scaling the decentralized spam resistance.

-Tageted surveillance must not be so cheap that it can be used en masse. Physical surveillance is always possible, and physical access enables full digital surveillance.

Theme II

-Security must not break down in case of temporary corruption of any given institution.

-Free open source software does not guarantee security, but there can be no security without free and open source code.

-Distributed or federated systems: Cannot expect every freezer to run GNU DNS, but can expect every ISP to run one in every city.

-The ongoing security of critical infrastructure must not depend on foreign entities.

-Any method which can keep some traffic in EU can be used to push other traffic outside. Net neutrality is needed.

Theme III

-For the users, users first.

-Foster cooperation between SMEs with common needs. For example fund free software development via subsidized cooperatives. Releasing their work as Free Software makes it useful for all European citizens.

-Self-sufficient IT: towards a complete PC and software from top to bottom using purely free hardware and free software developed with European participation (so the know-how is in the EU) and infrastructure. Currently the only similar project comes from China.

Nicola Jentzsch

Theme I

-Fund within the H2020 Programme research on market failure problems in markets for de-personalization and privacy-enhancing technologies. Require this research to focus on advanced regulatory solutions that remedy market failure or market frictions identified.

Theme II

-Fund within the H2020 Programme research on economic options to destroy/insert frictions in data black markets, markets for zero-day exploits and similar trading activities. Encourage cross-disciplinary partnership and public-private partnership in this research.

Theme III

-Strive for vertical independence in securing cyber supply chains that lead into critical infrastructure organizations. The focus hereby should be on the most important CIOs that uphold the security of public security.

***

Jacob Appelbaum

These policies should extend to all people and their computers regardless of nationality or citizenship status:

-Cryptography policies must respect the right to silence as recognized by the European Declaration of Human Rights. No penalty such a fine or jail time should be given to people who refuse to disclose cryptographic keys or for people who use systems that do not have long term keys.

-No cryptographic backdoors or compelled access should be permitted. Rather we should work toward the deployment of ephemerally encrypted systems when possible; we should fund, implement and deploy secure infrastructure, secure end user software and with the goal of a secure internet. Compelled technical access (e.g., mandated back doors) is recognized as an increase in attack surface and weakening of technical security by all leading scientific experts in the field. Thus, in the interest of citizens, but also of national security for individual countries and security at a regional level, create an EU policy that clearly states strong encryption is essential for securing devices and networks and that neither EU nor national security is compatible with any form of compelled technical access.

-The EU should fund, implement, research and improve core internet infrastructure as Free Libre Open Source Software (FLOSS) that implements Privacy by Design in a distributed, decentralized manner whenever possible. This allows for resilience, reproducibility and verifiability for a baseline set of services, platforms and software that respects, upholds and expands human rights.

***

George Danezis

1) Total disentanglement of institutions relating to IT security and assurance from those in charge of interception, signals intelligence and “offensive” operations, to prevent irreconcilable conflicts of interest.

One of the key public policy challenge of our time is that a number of nations hosting large parts of the IT industry, conflate the institutions in charge of domestic assurance, and those in charge of foreign and

national security signals intelligence (eg. GCHQ/CESG, NSA/ NCSC). Even beyond the realm of sigint, and much more widely, there is a systemic confusion within national bodies (police, CIP, …) in charge of quality engineering and assurance, and those in charge of the investigatory and offensive side of things. Yet, the conflits of interest between those two entirely different missions are irreconcilable: attackers' jobs become easier by weakening widely deployed infrastructures (particularly those used by the public in case of LE, or foreign nations in case of SIGINT), while those in assurance always aim to build system that could not be compromised even by themselves. Conflating those two roles into single institutions, in particular those that put the emphasis on offense, creates incentives to subvert any assurance process and make it subservient to the offensive goals. This includes participation in standardization, advice to industry, briefing the press, parliament of the executive, and advice on legislative changes.

It is therefore imperative, to strongly separate IT offense and defence institutions and create an effective "Chinese wall" between the two functions of states. Spies can spy and hack – that is the sovereign right of states. However, the same people and organizations should have no influence on the standards, research funding, incubation funding, procurement, design advice, and any other activities involved in IT assurance. Assurance activities should proceed as if that part of the state did not exist, even if that means that offensive operations may become harder (which is usually the goal of assurance). Defensive institutions should be fully civilian, open, and have working and hiring practices in-line with the rest of the global IT industry. They should be geared towards global open cooperation, as well as open cooperation with the IT industry and academia.

There are a couple of objections to this policy that I would like to discuss. First, there is a fallacious argument that those best in offense are also the best in defence, and therefore it "makes sense" to have the same institutions responsible. While, this may have been true at some point, today the open security community is extremely apt in both attack and defence, and there are no special "dark arts" that are the mere prerogative of the state. In fact a lot of offensive know-how in government comes from private contractors. Thus defenders have ample information and opportunities for training (including in offense), and can coordinate widely amongst themselves -- something that is not possible if their roles also involve offensive operations against each other. A similar argument is that talent is limited, and thus one has to conflate the roles: however, the shortage of talent to work on offence is compounded by the needs to keep national secrets, while defensive institutions can align their hiring practices (and all other practices) with the hiring practices of state of the art security teams in academia and industry – without nationality restrictions or burdensome clearance requirements. Finally, the job of defence against all attack is significantly different than the job of offence, when one weaponises and keep secret a small number of attacks.

2) Mechanisms for the establishment of enforceable or consequential, open, public, and peer-reviewed engineering norms in IT security and privacy based on evidence.

Since IT is taking an increasingly important social role, and security problems are likely to affect life very soon, it is high time to apply to it models of engineering excellence regulation as those seen in the construction, aviation, automotive, health or other industries. However, due to its high specialty and complexity it is imperative that IT security is regulated in ways that are effective to foster excellence and not in fact detrimental to it – for example innovation in the adoption of better techniques should not be inadvertently slowed-down.

One key model that a large part of the IT world has adopted is to use "openness" as a means to achieve excellence in design, architecture and implementation: open standards that all can see, open competitions to decide on ciphers, open source code, and nowadays even high-integrity systems that make operational data open such as bitcoin and certificate transparency. Given the complexity of certification, and the dynamic nature of software, only such radical openness can guarantee high-assurance in the long term. Note however, that even though the designs and artefacts may be open it may be prudent to protect the IP rights of their owners: thus to truly embrace openness state institutions may wish to provide IP protections – in the same spirit that the parent system used to provide protections for publishing inventions (even though this specific model is inappropriate for IT).

In line with openness as an assurance mechanisms, policy makers may wish to establish a number of rights to support it: first in a high-tech world more and more devices are opaque to their users and call upon third services to be useful. It should be established as a right that if a customer or citizen may be affected by a technological artefact that have the right to know what it does and how it works. This is in effect the high-tech equivalent of saying "people have the right to study physics" – yet the right to fully understand ones technical surroundings is in fact not protected, and threatened by inappropriate IP provisions. This right is particularly important if a technology has the potential to impact the security, safety or privacy of a person. Secondly, it should be established, and enforced that security is not enhanced by secrecy, but in fact that secrecy of the mechanisms (but not some operational details like keys) usually weakens assurance.

3) Public promotion and use by public bodies of architectures that embody PETS, and that provide security and privacy guarantees even if those public bodies become compromised.

Public bodies should embrace technologies that protect privacy and integrity in a very strong sense, even by themselves. A key reason computer security is in a dire state is the wide spread use of a model by which organizations are "crunchy on the outside, and soft on the inside": namely once an attacker manages to get "inside" they have free reign to exfiltrate or change information. Instead modern security systems emphasize a "defence in depth" approach, that ensure no single partly or system, or small coalitions thereof, can compromise privacy or integrity.

Public bodies should lead the way in adopting such systems: for example citizens should be allowed to discuss matters with government services through end-to-end encrypted channels, and anonymous access to on-line services (where appropriate) should be supported; selective disclosure credentials should be used for government authentication and authorization; high-integrity distributed cryptographic ledgers should be used to keep information safe.

All these technologies ensure that single component failure or compromise has little effect on the service and citizen security, strengthening our infrastructure against foreign (and domestic) powerful adversaries. Their acquisition is likely to stimulate an EU industry to become fluent in the engineering of such systems providing it with a competitive advantage over other IT industries.

***

Joanna Rutkowska

-We need to treat the infrastructure (backbone, data centers, etc) as_untrusted_. This implies END-TO-END CRYPTO for everything.

-But end-to-end crypto makes sense only if we can have secure and trustworthy personal computers. We thus need SECURE OPERATING SYSTEMS for PERSONAL COMPUTERS.

-Finally, the heart of each personal computing device is its PROCESSOR. Currently the processors that fuel our laptops and other devices are designed and produced outside of the EU, by American and Asian corporations, without any possibility for others (e.g. EU states or citizens) to find out if they were not backdoored. We need regulations and more research in this area, i.e. making of TRUSTWORTHY and easy to verify/audit PERSONAL COMPUTING HARDWARE.

***

Jaap-Henk Hoepman

-Many secure and privacy friendly products and services are hard to use properly by the average user, or lack functionality that is important to the user. Sometimes this is because we still do not properly

understand how to make such systems more user friendly, or how to achieve certain functionality efficiently without sacrificing privacy or security. In these cases, policies should be developed to stimulate research to bride these gaps. In other cases we know how to make such user-centric products and services, but they are not actually developed or offered in the market. In these cases policies must be designed that help overcome these barriers to deployment of such user centric products and services, that protect the privacy and security of their users without sacrificing the functionality that users look for in such products and services.

-Any policy recommendation that aims to increase online privacy protection needs to acknowledge the fact there are strong forces from (national) security and law enforcement circles pushing for policies that aim to reduce privacy in order to increase (homeland) security. Both sides of the debate need to realise that privacy and security are both fundamental rights, and both deserve protection. Both sides also need to realise that they are not necessarily in contradiction with each other. I believe it is high time to have a fundamental debate involving all stakeholders to explore how to make progress on this issue. Europe could take the lead in this. Unfortunately, we are lacking solid and independently verifiable figures on the effectiveness of current investigative and surveillance powers. This makes it hard to determine the proportionality and subsidiarity of these measures. A first step towards resolving the issue is therefore to create policies that aim to increase the transparency of intelligence agencies and law enforcement. These policies should be aimed at increasing the amount of information available on the effectiveness of their operations, the negative impact of these operations on privacy and other civil liberties, and in general increase the transparency and the strength of independent oversight.

- Many companies and organisations struggle with implementing data protection requirements in their day to day activities. In particular, privacy by design turns out to be a hard concept to grasp and make concrete. Europe should stimulate the development of methodologies and tools that make privacy by design more concrete and that help companies and organisations to implement it in practice. Also, Europe could support the creation of an independent platform where knowledge institutes, companies, policy makers, data protection authorities and other stakeholders can meet to discuss gaps, exchange information on best practices, and perhaps join forces to develop such methodologies and tools.

***

Michael Sieber

-Provide a strategic communication from the EU top level, which needs to include a narrative on the scientific and technological excellence and the market opportunities of Europe, but also clearly explaining the condition that only a joint effort will bring success. Create a joint vision to follow, and a roadmap on steps to be implemented (which include new architecture, technologies, and industrial eco systems).

-Agree on game-changing policies, such as strategic non-dependence, or a socio-technological approach (bringing technology under constitutionally meaningful control (see free-and-safe.org); agree on an organisational body to manage the implementation, well-balanced between EU-centric and Member-States (e.g. a Joint Undertaking).

-Consequently and sustainably an overcome the fragmentation in our efforts (among EU institutions, Member States governments, industry/SME, financial contributors) and coordinate instruments, shareholders and stakeholders. There is a lot of money available, and many people are doing the right things (research, actions, funding), but not coordinated to a joint vision and action plan.

***

Hadi Asghari

Theme I

There is an interesting disconnect between demand and supply in the PET market. At the Amsterdam Privacy Conference last month, one speaker asked the attendees who wants a more privacy friendly smartphone; more than half the audience raised their hands. It would be very interesting to hear from Mr Zimmerman and other PET developers what they see as barriers to adoption.

Network effects and switching costs probably play a role in limiting adoption of PETs. Given that the Internet's dominant business model is behavioral profiling, many large intermediaries have incentives not to deploy technology that limits profiling. Another reason might be the inherent tension between the PET design philosophy of leaving no data to be observed, with the usefulness of data for some functionalities such as personalization, security, or other things. Conventional wisdom is that if data is out, it should be considered gone. But this need not be the case, as data needs to physically reside somewhere, making it auditable and erasable. (Perhaps we can call this 'ex-post' privacy protection). My proposals are to target these underlying incentives and increase transparency.

-Require content and service providers to unbundle their offerings from behavioral tracking. This means that they offer a choice to users to drop out of behavioral profiling—done in any technological manner—and still receive the content or service, possibly at a fee or with reduced functionality, but still usable. This would weaken the industry incentives against privacy (as in profiling), and additionally levels the field for more serious PETs.

-Do public data audits of companies collecting personal data—in particular for the largest data collectors. Knowing what is collected, retained, used, and shared on an aggregate level helps detect and deal with violations. It also facilitates consumers' choice among competing privacy policies and for businesses to verify supplier privacy claims. And it helps researchers and policy makers better understand the value of data and its ecosystem.

- Mandate all 'smart' devices to have a privacy/profiling 'mute' button, which takes the device into a local or net-view mode, and does not send any data to the cloud. This momentarily refuges users from surveillance, and encourages technology designers to think of separate modes of operation. (This idea I have heard from others and I like it a lot).

Theme II

-Clarify and remove restrictions on academic and public-interest research into security vulnerabilities of software products and devices powered by software.

-Research has shown Internet intermediaries can play an important role in securing the common backbone and platforms. They have technical know-how and often care about protecting users, albeit in selective ways driven by their incentives. Public policy should understand and correct the biases when necessary in different markets.

-Revisit the liability question for device manufacturers and software vendors concerning security flaws. Many 'smart' products are shipped today with outdated software that has known vulnerabilities at the moment of sale; in some cases, manufacturers have no mechanisms or otherwise refuse to offer free security updates (including currently millions of Android phones). It is unclear to me why this continues to be legally acceptable.

Theme III

The EU is in many sectors globally competitive or leading. It also has an excellent infrastructure for business. What makes the IT sector different, and how can that be addressed?

-Ensure EU and non-EU companies play under the same rules with regards to data protection. It makes little competitive sense for an American company to be allowed to retain, use, or share European data in

ways that EU companies consider illegal. (So the death of the safe harbor might actually be a blessing, and allow clarifying what is acceptable, and enforcing what is not).

-Stronger data protection laws in the EU (along with its other laws protecting citizens and the planet) can be a selling point for the EU, if clearly promoted, for instance to attract PET developers. Some customers might pay a premium for services with a 'privacy' certification, similar to the eco, bio, or fair-trade logos. The EU could further facilitate entrepreneurship via startup hubs, seed funding, or easing knowledge migration, that complement its excellent business infrastructures.

-Revisit and relax certain rules surrounding the great EU research funding programs that might be dampening innovation. For instance, the large number of participants required for FP projects sometimes induce overheard and rigidity in the research process—comparing projects with different funding sources at our own team. This might hold more in IT and cybersecurity projects.

***

Joe McNamee

-Promote privacy enhancing technologies: In line with several European Parliament Resolutions, ranging from the Enfopol Report in 2001 to the Mass Surveillance Report of 2014, support must be given to the development and implementation of encryption technologies by individuals. This implies support for positive measures such as the support for open source solutions, mandatory end-to-end encryption by default and the use of encryption by public authorities and negative measures, such as avoiding the mandating of "back-doors", key escrow or banning of encryption altogether.

-Legal immunity for legitimate security research to avoid chilling effects: The legal framework must be designed in a way that does not have a chilling effect on security research. Security research is needed to improve the overall digital infrastructure. As a result, all of the flexibilities foreseen in the Cybercrime Convention should be rigorously applied when implementing that instrument. Existing implementations of the Convention should re-evaluated from this perspective.

-Understanding of the implications of security measures: The recently adopted Parliament report on "radicalisation" implicitly supports some sort of arbitrary undermining of encryption, the criminalisation of internet companies for failing to "cooperate" with administrative requests and an ad hoc reporting (i.e. flagging content for deletion) by a police authority. These approaches have been supported by the European Parliament in the complete absence of any evidence that they would serve any positive purpose, despite the obviously undemocratic message that they send on a global level and despite the significant risk of counter-productive impacts on the public policy goals being pursued.

***

Michael Backes

-Understanding privacy at large: Online privacy of end-users is a largely unsolved problem. The wide circulation, easy accessibility and permanent nature of online data incur risks ranging from public embarrassment to disadvantages when applying for jobs or insurance. New business models have emerged, tracking and monetizing personal information in an unprecedented manner. Legislators have started to respond by tightening privacy regulations and demanding "privacy-by-design", but privacy is not a challenge that can be solved by laws alone. We arguably lack the understanding and technology to fully comply with such regulations, and users lack support for making informed privacy choices. Establishing an overarching scientific foundation for providing privacy in tomorrow's Internet is an endeavor requiring fundamental transnational and interdisciplinary research efforts. By combining the expertise of excellent EU research sites to find universal European solutions we can truly address the understanding of privacy

from a transnational point of view. This requires political and financial efforts on national and EU level. The current H2020 Digital Security scheme is too focused on innovation actions and too large consortia to foster fundamental transnational research efforts in the area of privacy and security.

-Rigorous assessment of and security guarantees for critical systems: Today, most of our hardware and software (like kernels, OS, hypervisors, central software systems) are built outside of the EU. We are able to build brilliant spot-wise security solutions. But we are doing it on an unstable basis. We lack the insights to assess security holistically in complex systems incorporating or connected with these untrusted systems. Therefore, we are currently unable to give meaningful security guarantees for complex systems. We have to focus our research efforts to find new and better means to rigorously assess, test and, optimally, verify these untrusted blackbox systems that we build our critical systems upon.

***

Seda Gurses

Theme I

Promote privacy engineering capacity building: Privacy engineering expertise is mainly limited to research centers, specialized companies or large enterprises with privacy engineering teams. While many proposals have been made for privacy enhancing technologies, little expertise exists in integrating these technologies into large-scale systems. Knowledge transfer from research centers to public and private organizations running information systems cannot scale if teams don't have well-trained privacy engineering capacity. In order to promote the integration of PETs across the board, efforts to develop methods, techniques and tools for developing and integrating privacy enhancing technologies in live systems should be promoted. Moreover, capacity building requires educating privacy engineers. This engineering practice should be informed by the state of the art in PETs research, industry practices and alternative practices, legal frameworks, as well as civil society's demands on fair information infrastructures.

Similarly, all the current whining about the impossibility of lawful access due to encryption when we are obviously in the golden age of data collection and processing suggests that some engineering/technical capacity building within LEAs may be necessary. In house experts may help them devise lawful access programs without having to break the security of all communications.

Theme II

If all its ends are broken, (network) resilience will remain a pie in the sky!

Due to a number of reasons -- including resource constraints, lack of industry incentive, costs, diversity of hardware, poor software practices, patch unavailability and limitations of static or host-centric security mechanisms-- industry and governments are moving away from classical security to a resilience model based on novel network defenses. Such defenses work by keeping strict control over policies that define acceptable input and outputs of devices, while dynamically developing attack signatures based on anomalies observed in the network. It is argued that in the current IoT marketplace -- and for the convenience of the user-- it is legitimate to introduce such intrusive and controlling network defenses. These models of network based resilience, however, come at the cost of security and privacy: it is not clear whether the network can assure security when all the hosts are compromised, and the user becomes increasingly vulnerable to an all watching network controller. The shortcomings of the resilience models should be well understood before switching away from existing security approaches. Until then, hardware and software security should be promoted internationally through regulatory and economic mechanisms.

Theme III

-Thinking beyond Service Oriented Architectures: SOA and Software as a Service models have come to dominate markets but this may not be for long. For security reasons, centralized services may have some

advantages, but what privacy and competition is concerned, their track record is unconvincing. The desire to save labor and technical costs while scaling up to millions of users has also come at the cost of privacy and security -- as well as disgruntled users struggling with customer service bots. Current cybersecurity agenda focuses on trying to make up for the shortcomings of these models. The efficiency of clouds with on demand computational facilities may also not hold up once the market is saturated. Hence, capacity building should focus on how to do security and privacy better in SOAs and on imagining what will replace these centralized architectures that are developed using poor labor practices.

-Future of European IT Education: Europe has great universities, however, lack of outreach, complications with visas, lack of support once on site and everyday racism are likely to keep international students streaming towards the anglo-american educational system.

-Success in IT is not just based on technical expertise, but interdisciplinary skills. Interdisciplinary research and practice at the crossing of computer science and engineering, design, organizational studies, HCI/UX, markets and governance needs immediate attention in Europe.

***

Stephen Farrell

Theme I

Aside from encouraging better and more ubiquitous use of cryptography, and data minimisation (in all services) and punishing those who leak data sets that expose information about the public, there is a need to develop better ways to manage networks where almost all of the traffic is ciphertext and without nullifying the security and privacy goals for which that ciphertext has been generated, i.e., no re-insertion of new copies of meta-data. Network operators need new technologies, help and encouragement to run efficient networks in this new but inevitable mostly-ciphertext Internet.

Theme II

Software update is needed in every device, there need to be standards for that and those need to be open-source friendly. That likely involves innovative handling of end-of-life for both open-source technologies and commercial products. For example, many vendors sell devices using busybox but no longer maintain those after product end-of-life. Mechanisms that allow open-source communities (or funded centres) to take over maintenance of such when there is sufficient need/interest are needed. There can be no exceptions based on the kind of device - the smallest sensor or actuator running some 10s of thousands of lines of code also needs to have an update mechanism. Non-research technology development funding mechanisms for open-source hardware designs and platforms (e.g. such as cryptech) should be put in place as a priority.

Theme III

Industrial policy is not my forte. The EU institutions should however encourage the development of home-grown IT businesses and semi-academic institutions and capabilities that are disassociated from the defence, aerospace and advertising industries - while those industries are valuable there is an imbalance between those and companies who are genuinely acting with the best interests of EU citizens are their one of their foremost goals.

***

Ahmad-Reza Sadeghi

-Real life privacy: Focus on providing real life privacy and how to protect it against stealthy surveillance that is coming surely but slowly. It does not really make sense to install thousands of cameras in Europe every other day and debate about using encryption. The same holds for meta data.

-Terms and definition: Agree on notions and terms about what is private and what not. We are still debating but we need clear definitions and immediate actions. It is not expedient to debate about whether "encrypted data" is personal information while not having the right tools for average citizen to even use encryption.

-Public visibility and awareness for privacy: Politicians misuse terms for their own purposes, and they have the advantage of using public platforms and media for their intensions. Privacy advocates on the other hand do not have access to these means to receive this visibility. Provide platforms for them for awareness of people.

-Usable privacy. Promote building strong, automatic, and usable privacy-enhancing technologies. The emphasize is here on "usable". For instance usable crypto for all citizens. After so many years of crypto and security research we are still lacking these tools: "crypto for people, crypto for you and me". Many available technologies are not accessible to majority of people, because they require too much of technical expertise.

-Commercial privacy and evaluation: Provide incentives for enterprises to consider privacy in their products, through legislation and evaluation processes. We have a number of evaluation criteria for security products, why not for privacy aspects. Privacy should become a business goal !

-Data leak fines: Penalties for customer data leaks (medium term).

-Privacy-enhancing infrastructure (long term): The development of social online networks shows that most people will have a "second life" in the future. We need user-friendly tools that allow user-controlled private communication over these networks.

***

Udo Helmbrecht

Theme I

Encryption is the only way to protect privacy in the digital age. In the past, several attempts have been made to regulate the use of cryptographic tools by law to support law enforcement. However, in today's fast moving world, computing costs are systematically decreasing in ever shorter periods; attacks that seem out of reach of any one but a nation state will not remain so for the lifetime of long lasting crypto regulation. Hence, the main difficulty is to develop public policies today that regulate the technology of tomorrow. Without doubt, the recently agreed GDPR could be a first step to this direction. Moreover, nowadays computing power is a fact and criminal or terrorist organizations have access to the technology to abuse backdoors and interception mechanisms designed to enable legal interception.

Theme II

Incentives for the development (through EU funded R&D) and deployment (e.g. through procurement) of open software solutions should be provided. Europe should not ignore the absence of an EU OS industry with a dominant position in any end device market segment (PC, smart phone, consumer electronics, etc.). A possible approach for the EU industry in this area could be focusing to the vertical markets that Europe has strong presence (e.g. car industry, etc.).

Theme III

The recently agreed GDPR represents an opportunity for EU industry in the areas of privacy and trust. Having said this the emphasis of the GDPR so far is mainly on enhancing the protection of EU citizens. Since GDPR may also be an opportunity for EU industry EU policy makers should take advantage of the transition period of two years that the Regulation will need in order to reinforce the position of EU industry.

***

Frederic Jacobs

-Investments done in European critical infrastructure should favor organizations involved in development of Open Source software and protocols. This provides a wide range of advantages. Peer-review will not only help reveal security flaws but it will also make it easier to hold contractors accountable. Code openness prevents vendor locked-in, lowering maintenance costs and enabling more competitiveness. Industry and individuals can benefit from these investments.

-Involve more technologists in IT Security policy making. A lot of policy discussions completely dismiss the technical reality. Vendors are likely to influence policy makers into adopting inefficient measures while placing their product. The voice of academics and independent security researchers needs to be heard. National security representatives should enter discussions about information security from an Information Assurance perspective. The current model can encourage them to keep infrastructures insecure to protect offensive capabilities.

-Increased liability for personal large data breaches. The adoption of end-to-end encryption is an important tool to help companies mitigate risk of compromise.

***

Fabio Martinelli

Theme I

-Data centric usage control policies, flexible enough to include cross border legislation and user preferences. Data protection as a service should also include trusted elements to allow auditing/accountability. Data protection policy should be easily understandable/verifiable either by human or by trusted devices by humans.

-Study privacy-by design approaches including privacy engineering. This also include privacy metrics and proper anonymization techniques. Privacy aware data mining is also relevant. Needless to say that security by design implies also approaches as Defence deep by design etc.

-Lawful interception mechanisms should be verifiable and under separate control. Strong verification tools and instruments for code should be widely used and available. Verification by third parties should be included.

Theme II

-Design for assurance. There is a quest for developing security/private/trusted systems by design. However, we need also to be able to prove that those systems are secure. This will be eased by proper design methodologies, tools and approaches. This would also ease adoption of working liability frameworks (once proper design principles are elicited).

-We need to develop/improve code analysis tools together with proper testing and certification approaches (including and especially for hardware).

-Security engineering principles should be though at all levels, including in basic software engineering courses.

Theme III

-Cyber security is a strategic asset for any country, including Europe. It must be treated and funded as such.

-Development of a EU security brand would be beneficial. We need to mitigate dependencies of EU technologies. It requires significant efforts. We need also certification of software and hardware.

-Investing in a EU based industry strategy, with interplay among SMEs (start-ups) and major companies. Public/private procurement should be fostered.