**Richard: Data Breach Report**

**Discussion:**

- Many points raised by the report are covered by the General Data Protection Regulation (GDPR) in the EU. What could be the engagement for ISOC, apart from promoting the GDPR outside the EU?

- GDPR implies a lot of new responsibilities for business and governments by May 2018.

Whose role is it to educate business on implementation of GDPR/Network and Information Security (NIS) directive? Can ISOC play a role here?

- Implementation of GDPR may be problematic, as it will have national flavor. The results may be incoherent.

- Data breaches not yet a government priority, because impact still limited. But when impact will be a risk to human lives, this will become a priority.

- Regulation changes market circumstances, makes opportunities different that they were.

- Role of standards is important as a measure of market development. Only a group of people understand their relevance and importance. Standard bodies should become knowledge hubs.

- Regulation/ standards do not remove the duty of care of citizens.

- We may see an emergence of cyber insurance.

**Brandt: Search ranking technologies (no slides available)**

**Key points:**

- 50% of Google staff involved in manual manipulation of search results.

- Rules for ranking search results change constantly.

- Fake news suppliers know how to manipulate search results. Google a gameable system.

- Google actively represses unwanted searches.

- Role of paid content/ advertisements.

- Tactics are available to combat ‘fake news’.

- Customisation of search results can be established through browsing patterns. Google wants to please people, not give you the truth. Goal to keep you as a Google user.

- Personal profiling is the largest source of revenue in the Internet market.

**Ansgar: Editorial responsibility for online content/ ‘fake news’**

**Discussion:**

- Potential solutions to ‘fake news’ may risk moving onto censorship territory.

- Role of advertising vis-à-vis ‘fake news’.

- Who can judge the reliability of news?

- Different solutions and ideas to combat ‘fake news’ have been proposed, or are already in practice:

\* Cognitive fact checker (Vint Cerf)

\* Wikipedia/ Wikileaks an example of bringing out the truth. Correct data is available through references/ sourcing.

\* Make people responsible for the news their share. Create a chain of information. Wikipedia is a current example.

\* Alexa-like system for news based on different types of fake news.

\* Regulatory approach has been implemented/ is being discussed e.g. in Russia and Malta. News aggregation services e.g. search engines or even bloggers need to register/ have a license.

\* Naming and shaming.

\* People-based approach e.g. ethics board.

\* Finding a way to prove the authenticity of the author of the information.

\* Funding a certain level of news production e.g. state funding.

\* Media literacy guide to be used in the general education system e.g. by ISOC.

\* Obligation to rectify of news (parallel with news papers).

- We have various different world views, so no objective fact checker is possible. We should counter ‘fake news’ by pushing out our world view.

- Propaganda is harmful and hence counter propaganda is necessary. In practice, this could mean just public discourse.

- No use of software can tell truth from lies. This is a possible means for propaganda and ultimately a reflection of someone’s mentality.

- Trust needed to establish the truth (by a group of people). Governments jumping on the topic with potential regulation. This creates a risk that the cure is disproportionate to the problem.

- Facebook is a monopoly, and news in FB have a FB stamp on them. Solution should be open source/ liberal/ pro-competition.

- Definition of media platform needs to be clear e.g. social media.

- We live the post-truth era. Do we really want to know the truth?

- No universal truth. We should favor diversity of sources (McChesney).

- Revealing the source of information may be risky for individual users/ groups in non-democratic countries.

- ISOC should not engage in finding solutions to ‘fake news’, as this can be interpreted as censorship. Everyone should be able to state their opinion.

- ISOC can provide guidance on what to communicate to legislators, who want to impose ‘fake news’ legislation.

**Olaf: Collaborative Security**

**Discussion:**

- Collaborative security = People’s action or inaction might have an impact on the global properties of the Internet.

- Examples of collaborative security: Responsible disclosure, CSIRTs, MANRS. We need more examples of collaborative security!

- Collaborative Security is a messaging framework and a framework where you can develop solutions. Trying to identify specific solutions vis-à-vis specific challenges using the multistakeholder model.

- Global Commission on the Stability of the Cyberspace (GCSC) was launched in Munich on 18 February 17. ISOC is a member. This is another example of collaborative security.

**Jonas: Security of IoT devices**

**Discussion:**

- Business model to manufacture IoT devices is ‘broken’.

- Consumer awareness about home automation is low. Consumers don’t care about security.

- Software development environment has a ‘toy’ mentality. It is ok for software to crash – updates/ patches will solve this. This approach will not work when IoT solution can have a life-threatening impact.

- IPv6 compatibility of IoT devices might cause further problems.

- Potential solutions to address the security challenge of IoT devices:

\* Industry will repair the situation, as a market failure has already happened. Best practices needed by industry.

\* Expert committees on best practices, norms and potential regulation. Soft regulation based on best practices the way to go.

\* Regulation has its place, but time-proof regulation difficult at the moment. Customary practice should emerge before regulation.

\* Threat of regulation by governments is important to emphasise the urgency of the problem vis-à-vis vendors.

\* Research, public consultations, procurement are examples of a non-regulatory approach.

\* Current IoT apps are connected to the global Internet as a separate channel, which creates an insecure, unstable model. Middleware/ platform/ operation system is needed to separate devices from the global Internet. ‘Home management platform’ is one example.

\* IETF standards should play a leading role.

\* Licensing for IoT devices.

\* Setting new standards for marketing e.g. trusted devices/ trust marks.

- Industry have the responsibility and an opportunity to solve the problem of IoT device security.

- Governments reactive not proactive, lack of knowledge prevails. Industry is in a leading position.

- In the EU context, EU guidelines play a key role.

- Industry liability is a must.

- There are societal questions about boundaries we want to set. The toolbox exists.

- How do we define a set of solutions collectively? Everyone needs to bear their responsibility.

- We should rely on self-interest of people rather than good nature of people.

- Practices and mindsets about data collection vary greatly by region/ geography.

- Insurance industry may impose limits through requirements for e.g. home devices. Agreements between insurance companies and home security/ surveillance companies already exist to ensure device security.

- New professionals/ consultants job market may emerge e.g. licensed IoT installers.

- What do we do with the data collected through IoT devices? Access to data and use of data is an ethical issue. Security plays a key role.

- Perfection is not a realistic goal. In car industry five digit casualties are accepted. We cannot boil an ocean – a point of maximum impact should be defined.

- No urgency for immediate reactions, but urgency for immediate discussions. G20 is talking about standards, reference architectures… this is too early.

- Industry segments have to be treated separately when identifying solutions. Consumer space the most difficult to deal with.

- Why do very cheap/ bad quality devices get an IP address? Example of the ‘garage door regulation’ in the US (Ansgar). IP not allowed based on distance/ human vigilance.

- Will there be an ISOC position on IoT and security? Where can we steer the conversation? Can we work through the EU? What about large retailers, who might be liable at some stage.

**National trust agendas in Europe – Your priorities/ activities**

- Georgia: Trust a key point. Freedom of expression and user awareness (re privacy, data protection).

- Ireland: Too must user trust, not enough awareness. How to get the right balance of trust? Government is captured by the large American companies.

- Switzerland: ISP blocking of gambling sites was rejected by the Parliament in the context of a surveillance law proposal. ISOC Switzerland was part of the campaign against this. Swiss government reports and provides alerts on current security threats through a website (Melanie?). Preventive action is needed to avoid unwanted legislation.

- UK: Priorities include ‘fake news’ (re referendum/ Brexit); investigatory powers act (opposed by many rights organisations); personal data.

- Romania: Prepare ISPs and users on the upcoming NIS Directive/ GDPR Regulation implementation. This could be done through awareness raising, training, e-learning.

- Serbia: Challenge of access in rural/ remote areas; copyrights law (pirating); issue of privacy.

- Netherlands: Dutch snooping law in the making (including IXP).

- Turkey: State of emergency prevails. Freedom of expression. Data protection and privacy are hot topics (data breach scandals and recent data protection law).

- Portugal: Fake news & freedom of expression; ‘demilitarisation’ of critical infrastructure protection. Not enough awareness amongst political institutions beyond the regulator.

- Malta: Proposed law to counter ‘fake news’ (similar to the Russian one).

- Estonia: EU presidency motto ‘free flow of data’ as the 5th freedom.

- Italy: Taskforce for digital transformation, aligned with ISOC principles. G7 in Italy.

- Sweden: Privacy.

**Guido: User trust and healthcare in the Netherlands**

**Discussion:**

- This trust solution was tailored to secure communications between the different layers of healthcare and the user in the decentralised Dutch system.

- It was pointed out that the governance of healthcare systems can vary greatly between European countries, and protecting user trust may take different forms e.g. policy, technology.

**Michiel & Alex: Dutch chapter and website project**

**Discussion:**

- A substantial part of chapters present in the meeting expressed interest to deploy the new website format in their country.

- Buy-in by other chapters essential to continue to attract funding for the project.

- One way to promote ‘website project’ more globally would be to present it to the Chapters Advisory Council.

**Feedback session & actions**

**Ongoing/ upcoming ISOC activities at global level:**

- Global ISOC 25-year celebration to take place in the context of ICOMM 2017 (Sept). Details to follow.

- Internet Hall of Fame nominations are open! Please nominate candidates: <http://internethalloffame.org/nominations>

- Internet scenarios consultation is open! Please provide inputs through the website: <https://www.internetsociety.org/future-internet>

- We need more practical examples, where the principles of collaborative security have been applied.

**ERB actions:**

- ERB to include chapter news/ project in the weekly newsletter. Special section will be created. Send your news items to eubureau@isoc.org.

- Share link to the old ISOC paper on blocking and filtering: <https://www.internetsociety.org/sites/default/files/Perspectives%20on%20Domain%20Name%20System%20Filtering-en.pdf>. An updated version to be launched at Rightscon in the last week of March 17.

- In general, ISOC policy papers are helpful. Physical copies important for policy-makers.

- Find out about possibilities for ISOC 25 ‘celebratory package’ for chapters.

**Proposed chapter actions:**

- Chapter-led initiative to draft materials e.g. GDPR.

- Turkish chapter to share project detail/ videos on their education project with children once ready. Project details: <http://www.internetsociety.org/safer-and-conscious-use-internet-and-icts-among-k-12-children-turkey>

- Armenian chapter to share survey results on trust (600 people interviewed).

- Dutch chapter to propose ‘website project’ presentation to the Chapters Advisory Council meeting in early March.