WSIS Forum 2019 OUTCOME DOCUMENT (draft)

Workshop on Blockchain and Data Protection

Tuesday, 8 April 2019

1) **Workshop on Blockchain and Data Protection**

2) **Organized by Jörn Erbguth, University of Geneva**

3) **There are links to most WSIS-action lines since privacy is one of the most important ethical dimension of information society and impacts many other issues. We have identified links to C1, C2, C5, C7, C10 and C11**

4) **Blockchain was identified by Jörn Erbguth (a consultant) as a technology that can also be a tool to provide better privacy, but – if improperly used – also a threat to privacy. Katrin Kirchert (a lawyer) gave a summary about how blockchains can comply with privacy regulation. She reported about a workshop at the University of Geneva held that same morning. (See https://wsis.erbguth.ch - The audience asked that a link to the morning workshop be included in this report.) The panelists identified and emphasized the need for creating best-practices on this topic. Martin Adolph (ITU) described the efforts of ITU, ISO and JPEG in this field whereas Anja Grafenauer (privacyblockchaindesign.com) spoke about the German DIN SPEC 4997 that is focused on blockchain and privacy.**

5) **The main outcomes highlighted the following:**

   I. **Debated Issues**

   - Jörn Erbguth (independent consultant, University of Geneva and certified DPO) introduced the topic by pointing out that huge centralized data collections controlled by powerful private or government actors are a threat to privacy. We need to decentralize control and blockchain is a tool that can help to do that. Blockchain can foster privacy by empowering individuals rather than big players. Immutability of blockchains does not have to be a contradiction to the right to be forgotten if used correctly. Best practices for using blockchain in a privacy enhancing way are needed.

- Katrin Kirchert, LL.M. (lawyer for privacy and data protection law and certified DPO) summarized the outcome of an in-depth workshop on this issue the same morning at the University of Geneva and the different presentations held there. She also reported about the position of the French data protection authority CNIL that alone has issued a detailed statement on this topic. Furthermore, Katrin presented five different ways how blockchain can be used in a data protection regulation compliant way as a conclusion of the participants´ discussion in the morning:
  - **Do not put any personal data (at all) on a blockchain.** However, this is easier said than done, since the definition of personal data under GDPR is very broad.
  - **Use privacy enhancing technology and ensure that no personal data can be derived from the blockchain.** Technology like hashes or zero knowledge proofs – if used correctly – can securely protect personal data. However, there remains legal uncertainty whether this will still be considered personal data.
  - **Obtain a justification that is permanent. Don't rely only on consent!** Consent can always be withdrawn, so it should not be used as a basis for putting information on an immutable blockchain. However, when the processing is needed for the performance of a contract with the data-subject (e.g. a Bitcoin-payment) or there is a legal obligation to publish something permanently, you can put that information on a public blockchain.
  - **Let users put their data on a public blockchain themselves.** GDPR wants to empower the users. So, if you put users in direct and informed control and they store their personal information on a blockchain themselves, this is GDPR-compliant.
  - **Build specialized blockchains that forget.** Of course, this sounds like a contradiction. When a blockchain can forget anything at any time, you should rather use a conventional database. However, a special blockchain can be built that can store only part of the data forever or can keep immutability only for a limited time – for example in order to implement a book-keeping blockchain that forgets after a fixed retention period – e.g. 10 years.

  It is sufficient to follow one of these five ways or they can be combined in a privacy enhancing application.

- Martin Adolph (study group advisor at the ITU) introduced the standardization activities of ITU in that field. He highlighted the work of the ITU-T Focus Group on application of distributed ledger technology (FG DLT) that will conclude and publish

its deliverables later this year. He explained the difference between ITU-T focus groups (pre-standardization open to non-members) and study groups, which develop international standards (ITU-T Recommendations). For instance, study group 17 is developing several standards that address various security aspects of DLT. Martin also mentioned activities by other standards bodies like ISO and JPEG.

- Anja Grafenauer (Co-Founder at privacyblockchaindesign.com) presented the newly founded DIN SPEC 4997 Privacy by Blockchain Design: a standardized model for processing personal data using blockchain technology. She co-initiated a light standard on privacy-compliant blockchain applications at the Deutsches Institut für Normung (the German standards organization), to be published by the end of this year. The DIN SPEC aims at providing practical guidelines and best practices to achieve privacy by design (art. 25 GDPR) in blockchain scenarios. In particular, the group will focus on creating a common language between law and IT as well as using design patterns derived from law to facilitate the work of IT professionals.

II. Quotes

- "Blockchains used correctly can foster privacy. Immutability and the right to be forgotten do not have to be contradictions", Jörn Erbguth (independent consultant, lecturer at the University of Geneva, certified DPO)
- "Don´t be afraid to use the blockchain technology in your company because of data protection regulation like the GDPR. There are possible ways to secure privacy on a blockchain", Katrin Kirchert, LL.M., lawyer for privacy and data protection law and certified DPO
- "All interested parties are welcome to review and comment on the draft deliverables of the ITU Focus Group on Distributed Ledger Technology. The protection of personally identifiable information is an important point to be considered at this early stage of blockchain's development", Martin Adolph, study group advisor at the International Telecommunication Union (ITU)
- "Blockchains can help us raise levels of data sovereignty in the digital world. However, we first need to start bridging the gap between law and IT and put the principle of privacy by design (art. 25 GDPR) at the core of IT architecture.", Anja Grafenauer, co-founder at privacybyblockchaindesign.com

III. Overall outcomes of the session highlighted that:

- Blockchains can foster privacy.

- There are different ways to achieve GDPR compliance, however, not every blockchain application use case can be made GDPR-compliant.
- Privacy needs to be taken into consideration from as early as the design stage of a project (privacy by design).
- There is still a lot of legal uncertainty.
- Best practices for privacy enhancing use of blockchains are needed.
- There are activities on distributed ledger technology and blockchain in different standardization bodies. Only few of these activities address privacy and protection of PII.
- There exits coordination between different standardization activities.

IV. Main linkages with the Sustainable Development Goals (SDG)

Privacy is a human right and required for achieving many SDGs. To name just some of them:

- SDG 8 Decent work and economic growth: Privacy at the workplace is important for providing a decent work environment.
- SDG 9 Industry, innovation and infrastructure: Many see blockchain as one of the main future information infrastructures. Companies and governments need to make sure that this infrastructure is not a threat to privacy but that it fosters it.
- SDG 11 Sustainable cities and sustainable communities: Blockchain is often debated in the context of smart cities and IoT. Smart cities need to protect everyone´s privacy in order to be sustainable.
- SDG 12 Responsible consumption and production: Responsible industries do not invade people's privacy and do not abuse their personal data.

V. Emerging Trends related to WSIS Action Lines identified during the meeting

Emerging Trends are blockchain, privacy, privacy by design and user empowerment.

VI. Suggestions for Thematic Aspects that might be included in the WSIS Forum 2020

The discussion on blockchain and privacy has just started. It will be an important topic in future governance forums like the EuroDig 2019, the IGF 2019 and the WSIS forum 2020.