Event summary of the Meet the Author seminar on the book Privacy is Hard and Seven Other Myths – Achieving Privacy Through Careful Design with Jaap-Henk Hoepman

Tatiana Duarte (Vrije Universiteit Brussel (VUB) - Law, Science, Technology & Society Research Group)

On 30th May 2022, the Brussels Privacy Hub hosted the 13th seminar in the [Meet the Author series on the book Privacy is Hard and Seven Other Myths – Achieving Privacy Through Careful Design](), by **Dr. Jaap-Henk Hoepman** (Radboud University Nijmegen- iHub, University of Groningen).

The seminar could be divided in five parts: (i) an introduction to the topic by the chair **Hielke Hijmans** (Belgian DPA, Vrije Universiteit Brussel (VUB) - Institute For European Studies); (ii) a brief presentation of the book by the author, Jaap-Henk Hoepman; (iii) remarks by **Prof. Mireille Hildebrandt** (Vrije Universiteit Brussel (VUB) – Radboud University Nijmegen) and **Christian D'Cunha** (European Commission, DG Connect), followed by (iv) a reaction from the author and ending with (v) questions and comments from the audience, to which the author responded.

Hielke Hijmans kicked off the seminar with the remark that this was the first Brussels Privacy Hub in-person event since the COVID-19 pandemic, highlighting the importance of bringing together people from different fields of study. Hijmans recalled that the events from Brussels Privacy Hub are an opportunity for authors to present their work, which also means an opportunity of being challenged. Hijmans proceeded to underline the core question of the book: can technology ensure the protection of privacy? The chair ended the introductory note by mentioning some of the assumptions that might endanger privacy, such as the myths of *you got nothing to hide*; *it's just metadata*; *we need to know your location*, and the handover of power from governments to tech giants.

Dr. Jaap-Henk Hoepman talked about the history of the book, which started 7 years ago, when, discussing with a friend, he realized that there was no book on Privacy Enhancing Technologies (PETs) written for the general public. The title of the book was thought of as a teaser to catch the attention of a broader audience, who might need to be persuaded to engage with these topics. The illustrations that figure in the book, authored by Gea Smidt, are inspired on the work of Kafka.

The first discussant to comment Jaap-Henk Hoepman's book was **Prof. Mireille Hildebrandt**, who started by saying that the book should not just be read, but studied, as it explains technical features of PETs in a language accessible to non-experts. Addressing the title, Prof. Hildebrandt underlined that one of the reasons why *privacy is hard* are the legacy systems on top of which some systems are developed, meaning that design decisions important to protect fundamental rights are not made upstream. In this regard, the myths about privacy are themselves part of the problem, as that they enclose assumptions that must be questioned, rather than being uncritically embedded in technological tools. The subtitle reflects this point by underscoring the idea of *careful design*, which means care, concern, time and attentiveness to its consequences. Prof. Hildebrandt added that optimizing for a single goal might blind designers to other relevant values and concerns.

Prof. Hildebrandt stated that the myths discussed in the book are an opportunity to discuss the stack and the operating systems. Evoking the AI act, and the idea that the whole development process must ensure the protection of fundamental rights, Prof. Hildebrandt asked the author how a fundamental rights impact assessment would affect constrained based computing. Then, Prof. Hildebrandt asked the author whether he would agree that unlinkability is key for privacy and for machine learning research design, and whether the link between individual behaviour and that of the others is key for profiling and discrimination.

The commentary continued with the remarks of **Christian D'Cunha**, who noted that the myths on privacy distilled on the book were the result of a process of selection by the author, as there are many more myths about privacy. One of them is that data is abstract, which overlooks that data means computer power (with serious environmental impact) and the underlying supply chain where the labour conditions are detrimental to workers. Another myth is that privacy violations are committed by companies only, while states may intrude disproportionately in individual's lives. D'Cunha referred as an example the overturning of Roe v. Wade in the United States and its consequences in terms of state intervention in individual decision-making.

Christian D'Cunha then wondered about whose privacy is being protected, arguing that the global self is excluded from this protection. Furthermore, according to D'Cunha claimed, privacy protection is uneven and deterring for certain states and underprivileged individuals, giving as example the fact that poor countries are colonized by companies, that migrants are targeted and that employees are subjected to workplace surveillance.

The dominant business model is based on tracking and on the impossibility of providing valid consent for data processing. D'Cunha questions whether Google or Facebook actually know everything about us or whether they just convinced advertisers that that is the case? If the latter is correct, then what are Google and Facebook in fact monetizing? D'Cunha argued that Google and Facebook are just hoarding data and that perhaps what they are really monetizing is the belief that the business model they promote and afford actually works.

D'Cunha evoked the idea of trust in social and economic relationships, contending that there is no chance of gaining trust before using a technology that processes personal information. In this line, privacy and security should be thought of as 'cousins' and suggested that the book *Privacy is hard* could expand more on the topic of security. D'Cunha finalized his commentary by saying that technological fixes cannot be expected to fix societal problems.

Jaap-Henk Hoepman responded to the comments by Prof. Hildebrandt and D'Cunha, starting by responding to D'Cunha's questions.

On privacy and security, Jaap-Henk Hoepman noted that, on a previous version of the book, there was a part that expanded on security which was not included in the final version of the book. Hoepman stated that privacy and security are not opposites and need to be balanced against each other. Hoepman pointed out that the digital world is not about zero-trust relations, arguing that, similarly to a bridge that we cross every day without knowing anything about construction, nobody needs to be an expert in computer science or software engineering to trust a system. What is relevant is that the system does not bring any surprises concerning fundamental rights. Hoepman agreed that data involves computer power that might deter other relevant values.

Answering Prof. Hildebrandt's, Hoepman responded that where the business model is data hoarding, privacy is hard, but once we step out of such model, privacy might actually be *easy*. Hoepman stated that design is always about constrains, acknowledging that there might be second level constraints not related to the functionality, but, for instance, with the business model. According to the author's experience, the decision concerning the trade-offs are generally made by those who have more economic power to impose them.

A lively Q&A followed where the audience addressed questions concerning the possibility of reversing hash functions, the incentive structure for developing privacy preserving technologies and the decisions on trade-offs.