Outlook: Data Privacy and Security - What Can Businesses, Regulators and Individuals do to Ensure a Safe and Responsible Future?

In our Outlook section we ask a cross-disciplinary range of experts to answer important questions on how emerging technology will impact society. Each contributor will provide their unique perspective on a particular issue thereby generating novel and important insights. In this edition we ask: What Can Businesses, Regulators and Individuals do to Ensure a Safe and Responsible Future?

Bernie Boscoe

Postdoctoral Researcher at The Information School, and Postdoctoral Data Science Fellow at University of Washington, Seattle

Businesses that use data containing Personally Identifiable Information (PII) are legally, if not ethically, bound to safeguard these data to prevent harm to individuals. Five recommendations follow: 1. **Prioritize Data Privacy.** Privacy-sensitive data should be viewed as entities requiring care, maintenance, and stewardship. A deep understanding of which PII is contained in these data, where and how the data are stored, how they travel in and out of the business, and for how long these data are kept should be well-understood. Hold individual(s) responsible for keeping track of the businesses’ data stores, to audit in appropriate intervals. 2. **Make Privacy Policies in Plain Language.** Purposefully obfuscating privacy policies is an unfair, widespread practice. Clearly explain what data are collected, sold, bought, or stored. Make opt-out policies easy to use and provide granular options. 3. **Store only What is Needed.** It is common for businesses to end up with unnecessary data attributes of individuals. Munging datasets together can also create extensive personal profiles that are simply overkill. Data lakes of privacy-sensitive data are a huge security and liability risk. Decide what data are necessary to accomplish goals and destroy the rest. 4. **Secure the Data.** Take security measures very seriously. Employ security specialists to ensure servers are protected, sharing methods are vetted, and that employees have proper training when handling PII data. Adopt encryption techniques to protect data, and two-factor authentication to verify appropriate access, to name a few. 5. **Consider Obfuscation Techniques to Protect Data.** Noise can be injected into datasets to prevent individuals from being identified yet the dataset is still statistically equivalent. Differential privacy is one method to ascertain the level of noise necessary to add, businesses are increasingly employing these methods to prevent re-identification.

Tine A. Larsen

Chair of the National Data Protection Commission, Luxembourg

Businesses, regulators and individuals all have a role to play in order to ensure a safe and responsible future when it comes to data privacy and security. Profit should not be the only motivation for businesses. Even though financial and economic aspects are by necessity their key drivers, companies also need to respect regulatory demands and meet their customer’s expectations regarding the safety of their personal data. Therefore, it must be cheaper for businesses to not only be compliant with, but also to invest in continuous improvement for data protection and security. Companies shall fully integrate such aspects into their risk management system.

Regulators have to make sure that the legislation on data privacy and security is respected. However, their interests are not limited to regulatory compliance only. They also advise the government on key issues, provide guidance to private and public actors

DOI: 10.21552/delphi/2019/3/7
and play a crucial role in raising awareness. One of the challenges regulators face in their interactions with businesses is to find ways to achieve more tangible results with soft empowerment based on a real dialogue and a solution finding process. Confrontation and sanction should only be the last step but not the default option. However, enforcement actions and subsequent communication are helpful to push businesses towards higher levels of responsibility and accountability.

Individuals want their personal data to be protected when they share it with businesses. If they are not confident how a company deals with privacy and security, they should look for alternatives. This will help new companies to gain market shares and motivate current market leaders to make the issues of privacy and security a top priority. In that sense, individuals probably have the biggest leverage to change businesses through their day to day behaviour and the trust they can gain ... or lose.

To conclude, it is clear that none of these stakeholders can ensure success on their own. Progress is only possible if businesses, regulators and individuals interact in an efficient and respectful way.

Robert van den Hoven van Genderen

Director of the Center for Law and Internet of the Law Faculty of the University of Amsterdam and Professor of AI and Robot Law at University of Lapland

A very broad question has to be answered in a concise formula. So what can the mentioned actors do to protect privacy in the all permeating development of AI? Will we all be slaves to the algorithm? The European Union, Council of Europe and OECD have all issued guidelines for the ethical use of AI. High level terminology is to be found in those documents: robustness, security, safety, human dignity, fairness, meaningful human control and of course transparency and do not forget inclusiveness. Furthermore all requirements of the GDPR such as minimalistic processing, purpose orientation and proportionality and information and control by data-subjects are mentioned. All these high level principles have to be applied in the development and application of AI by industry and governments to protect the individual data-subject. The problem is that all applications of governments and industry consist of analyzing (big) personal data of individual data subjects by AI which hardly can be made transparent; impossible to be controlled by processors, data-subjects or regulators. On top of that it will be impossible to predict to what level and in what areas AI will be based on self-learning algorithms and who and how the responsible actor can be identified. Article 12, referring to the rights of the individual in article 15 to 22 of the GDPR offers no protection against intrusions where nobody has any knowledge about when self-learning algorithms do the processing.

Already industry and authorities use AI for decisions with legal effects contrary to article 22 but who will know that? One cannot protest against unknown processing of personal data. And as long as the data-subjects gladly submerge in the ‘free’ apps and services, go for the easy profit and accept a risk based society in health care insurance and even in security by a surveillance state, AI will have provided the last kick in the weak belly of future privacy for the individual data subject.

Yoon Ho Auh

Founder at NUTS Technologies

For homo sapiens, privacy exists in a primordial form written into our DNA: your thoughts are born private until you decide to share it. The majority of our current digital technologies do the opposite: a most unnatural technical predicament. Tis the cause of much angst.

Exposition is the only method of transferring our most human and precious thoughts across time and minds. As a digital interloper, it is fascinating to know that each person must gather and process information entirely on their own. We cannot short circuit this hard reality even if science fiction would suggest otherwise.

We have enough cryptography to keep data private, and yet, we yearn for something better, something more. Unfortunately, data security and interoperability are typically technical after thoughts. We should demand more from technology and not settle for incremental innovations that expend enormous capital and resources for trivial gains.

Perhaps the answer lies within ourselves. A self-evident data model operates within us when we observe how a collection of simple organic molecules
can form such complex creatures. There are no man made data models which self-perpetuates 99.9% of its content across a span of two hundred millennia.

Can we extract a data model from the evolved designs of our DNA? Can we re-frame digital data security and privacy using this DNA data model? Not only is this possible, it is implementable and the future is bright for this emergent technology.

Data privacy should be an extension of our innate natural privacy. For lack of universally agreeable values regarding data security and privacy, perhaps biomimicry can extend and perpetuate evolutionary methods favorable to the survival of our DNA into the digital realm: a natural data privacy.