January 2019

A blog by

Michiel van der Veen
EAB

Els Kindt
KU Leuven & Leiden University

Biometrics challenges in the age of GDPR

Finding the right balance between technical, legal and ethical demands

As the world is quickly moving into the Fourth Industrial Era, more people put more of their personal data and that of their devices online. In this vast digital landscape, a wide range of private companies and government agencies collect, process and (re-) sell this data, and establish digital identities around them. With fingerprints, face recognition and iris scan technology, biometric systems can then authenticate and verify individuals to allow or deny access to a wide array of services. But as always, all these new developments also present a whole new range of ethical, legal and technical difficulties. Overcoming them will be one of the main challenges of our times.

By Dr Michiel van der Veen and Dr. Els Kindt

According to this year's World Economic Forum report , the average internet user today has 92 online accounts, and is likely to have over 200 by 2020[i]. All these online "logins" and related data are created by institutions to improve efficiency or increase revenue, but as common norms are lacking, individual users have no understanding of, or control over how they are represented online. Recent scandals like the Facebook/Cambridge privacy breaches or the personal data hacks at Marriott underline once again the urgent need for better security and robust privacy legislation.

On the other side of the divide, the World Bank estimates that 1.1 billion people globally have no formal or civil identity at all, physical or digital, leaving them without access to much-needed healthcare, financial services or humanitarian aid. One of the UN Sustainable Development Goals is to solve this problem before 2030. This is where technology can play a pivotal role. Biometric systems in the world's poorest regions have created a verifiable digital identity for millions of people, enrolling them for free or low cost into large databases. But just like in the case of the online haves, the have-nots' digital identity must also be organized around a set of shared norms, if only to protect the most vulnerable from further exploitation.

Authenticate, profile, infer

The evolving scope of our digital identities encompasses a number of functions that are supposed to make our lives easier. Whenever we log in onto our internet banking, pass through customs or present our ID card to an official, we go through an authentication process where we assert who we are and our right to contact or use a service. To have our identity verified, we use passwords or biometrics like fingerprints, facial recognition or iris scans. Our ever-growing digital profiles can include inherent (biometric) data attributes or assigned attributes like our names or national ID numbers. Based on these data in combination with our credit and medical histories or purchasing behaviors, large data-owning organizations make all kinds of real-life judgements or decisions, such as granting a loan, allowing (or denying) access to one's banking account or medical services.

As more and more of our personal data finds its way online, privacy concerns are only rising. The use of biometrics for authentication is only likely to accelerate this trend. More sensitive than other types of personal data, biometric data can be uniquely linked up to an individual and may reveal sensitive information like gender, age, ethnicity and health conditions. If compromised once, the consequences may last a lifetime. Aside from cybersecurity threats perpetrated by folks with malignant intent, another issue is the threat of official (state) organizations with enormous power in gathering, centralizing and extracting sensitive data for tracking purposes; potentially adversely impacting citizens' lives and privacy. Security and privacy safeguards must therefore be impeccable.

Enter the GDPR

The most ambitious and far-reaching legislation to date aiming to protect individual users' digital ID is the European Union's General Data Protection

Regulation (GDPR). It clarifies how personal data is to be treated and establishes several rights for individuals relating to their personal digital data. Individuals, or 'data subjects' as they are called under the GDPR, have the right to access their data and know how organizations are collecting and processing data about them. They can also request that their data be erased and restricted and may even object to its use for marketing purposes.
The GDPR defines biometric data as 'personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person [ii], which allow or confirm the unique identification of that natural person .' As a special category of personal data, it can only be processed under specific exemptions. For example, the data subject must have given explicit consent for his data to be used. The processing of this data must be necessary for executing obligations and exercising specific rights between controller and data subject with regard to employment, social security and/or social protection law. Furthermore, processing is necessary to protect the vital interests of the data subject; for the establishment and exercise of defending legal claims; or for reasons of substantial public interest [iii].

Article 35: DPIA
One of the most important measures that the GDPR prescribes to organizations that gather and process large data volumes is to carry out a Data Protection Impact Assessment (DPIA). Whenever data processing is likely to result in a 'high risk' to the rights and freedoms of natural persons, the company or government agency has to carry out this assessment and take all necessary measures to safeguard the data and adhere to the EU law. There are nine criteria that constitute a high risk to people's rights and freedoms and meeting just one of these is enough to require the organization to execute a DPIA:

1. evaluation or scoring to build a user's profile;
2. automated-decision making including if there is a risk of exclusion or discrimination;
3. systematic monitoring;
4. sensitive data or data of a highly personal nature (e.g. medical records);
5. data processed on a large scale;
6. matching or combining datasets;
7. data regarding vulnerable data subjects (e.g. children, employees or the elderly);
8. innovative use or applying new technological or organizational solutions like fingerprints and facial recognition for physical access control;
9. if the data processing itself prevents data subjects from exercising a right or using a service or a contract.

Viewing these conditions up close, the conclusion will be that gathering and processing biometric data for whatever purpose inevitably triggers the obligation to carry out a DPIA. This seems also

the view of the European Data Protection Board, enforcing this obligation with the EU Member States. Although it isn't prescribed exactly how DPIAs should be executed, they do typically describe the nature, scope, context and purposes of the data processing; assess the necessity, proportionality and compliance measures; identify and assess risks to individuals and identify any additional measures to mitigate those risks. Failure to comply with the GDPR may lead to fines of up to 2% of the organization's annual global turnover or €20 million, and even double.

Good ID, strong biometrics

Beyond the European Union's GDRP, the participants of the 2018 World Economic Forum have identified five elements of 'good' identity in order to safeguard people's online ID as well as to bridge the gap with those that lack any identity. To meet technological requirements, remove any ethical concerns and overcome legal challenges, any (biometric) identity system ought to be-fit-for-purpose, inclusive, useful and secure, and offer choice to its users.

And as biometric data is increasingly used for authenticating individuals across the globe, the risks of using these systems rise accordingly. Collecting and processing biometric data interfaces with people's fundamental rights, and so only the strictest legal and technical safeguards will do. Wherever a legal and technical privacy framework has not (yet) developed, as is the case in many developing countries, a baseline set of common norms based on ethical criteria ought to be implemented as soon as possible. The GDPR is a good step towards protecting individuals' personal data, but discussions are ongoing about the scope and definition of biometrics and the practical compliance with this EU law. Whatever the outcome of these deliberations may be, companies and governments should always comply with the strongest obligation to handle our personal data in the most ethical way possible.

Dr. Els Kindt is a legal expert, post-doc researcher at the KU Leuven and associate professor, eLaw at Leiden University, the Netherlands. Dr. Michiel van der Veen is a biometric expert and chief Executive of the EAB (www.eab.org). They have recently teamed up to tackle questions of legal and technical challenges respectively, with regard to biometrics and the GDPR.

i. World Economic Forum Insight Report: 'Identity in a Digital World - A new chapter in the social contract', September 2018
ii. EU GDPR, Article 4 (14)
iii. EU GDPR, Article 9 (2a-j)

About the authors

Els J. Kindt

Els J. Kindt is a post-doc legal researcher at the KU Leuven, Belgium (https://www.law.kuleuven.be/citip) and an associate professor, eLaw, Leiden University, the Netherlands (https://www.universiteitleiden.nl/en/law/institute-for-the-interdisciplinary-study-of-the-law/elaw).

Her research domain is the law and new information and communication technologies. She is recognized as a specialist on legal aspects of biometric technologies and published with Springer a monograph on privacy and data protection issues of biometric applications (http://www.springer.com/us/book/9789400775213), among other various articles and book chapters on the topic. She gained her expertise in this domain through close collaboration with technical experts and policy makers in international research projects, mainly funded by the European Commission, including Turbine, Fidelity (http://www.fidelity-project.eu/), FastPass (https://www.fastpass-project.eu/), Eksistenz (http://eksistenz.eu/) and currently Victoria (https://www.victoria-project.eu/), as well as in national projects.

She is often consulted as expert by national and internatioal policymakers and research. She teaches since 2012 European Data Protection and Privacy law in the LL.M programme IT and IP law of the KU Leuven in Brussels. Els J. Kindt studied law and philosophy at the KU Leuven and in the U.S., where she obtained an LL.M. She is an attorney at the Brussels Bar as well, and - before pursuing her academic ambitions - was for about 15 years with Linklaters, Brussels, active in the domain of information technology law. In September 2018, she joined the EAB Board.

Michiel van der Veen

Inspired by "Good ID", and based on the values of trust and impartiality, Michiel supports the ID community with executive leadership and thought leadership in the field of digital ID & Biometrics ..... not to mention being a keen cycling enthusiast.

From 2000 onward, Michiel had several technical and leaderships roles in Philips Electronics, and received, in 2007, the Distinguished Employee Award. In 2008, Michiel founded priv-ID, an early innovator in biometric, digital identity and privacy-by-design. It later merged with GenKey in 2011, with Michiel appointed CEO. He has led GenKey through multiple stages of growth to become one of the most trusted brands in the market to provide Identity for Development.

In 2012 GenKey helped to deliver the world's first digital ID solution for Ghana's Presidential Elections. Since then, Michiel has been involved in many large-scale digital identity projects for governments and businesses, across Africa and Europe.

Michiel is Chief Executive of the European Association for Biometrics (EAB), a non-profit and vendor neutral organisation focusing on the strategic ID challenges that Europe is facing. Michiel is also senior consultant digital ID & biometrics for the Worldbank's ID4D program, and a regular industry contributor, speaking about digital identity and biometric; along with future thinking about innovation and market trends.

Michiel has a Ph.D from the Swiss Federal Institute of Technology (ETH Zurich) and further business education from Stanford.

KU LEUVEN CiTiP
CENTRE FOR IT & IP LAW

European Association for Biometrics eab

Europe's Leading ID community

The European Association for Biometrics (EAB) is the leading voice for digital ID & biometrics in Europe. We are a non-profit, non-partisan association.

The EAB's mission is to tackle the complex challenges facing ID in Europe, ranging from migration to privacy rights. Our role is to promote the responsible use and adoption of modern digital identity systems that enhance people's lives and drive economic growth.

Through a series of EAB initiatives we support all sections of the ID community across Europe, including governments, NGO's, industry, associations and special interest groups and academia. Our initiatives are designed to foster networking and debate, whether at an EAB hosted event across Europe, or in providing impartial advice & support to individual members.

We ultimately serve the citizens of Europe in the advancement of modern biometric identity systems that are fair, accessible, secure, while respecting privacy. More info: www.eab.org