COMPUTER LAW & SECURITY REVIEW ■■ (2017) ■■–■■

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Having yes, using no? About the new legal regime for biometric data

E.J. Kindt [a,b,*]

[a] *KU Leuven – Citip, Leuven, Belgium*
[b] *Universiteit Leiden – eLaw, Leiden, The Netherlands*

Keywords:
Biometric data
Data protection
New definition
Unique identification
Sensitive data
Regulation (EU) 2016/679
GDPR
Directive (EU) 2016/680

A B S T R A C T

The rise of biometric data use in personal consumer objects and governmental (surveillance) applications is irreversible. This article analyses the latest attempt by the General Data Protection Regulation (EU) 2016/679 and the Directive (EU) 2016/680 to regulate biometric data use in the European Union. We argue that the new Regulation fails to provide clear rules and protection which is much needed out of respect of fundamental rights and freedoms by making an artificial distinction between various categories of biometric data. This distinction neglects the case law of the European Court of Human Rights and serves the interests of large (governmental) databases. While we support regulating the use and the general prohibition in the GDPR of using biometric data for identification, we regret this limited subjective and use based approach. We argue that the collection, storage and retention of biometric images in databases should be tackled (objective approach). We further argue that based on the distinctions made in the GDPR, several categories of personal data relating to physical, physiological or behavioural characteristics are made to which different regimes apply. Member States are left to adopt or modify their more specific national rules which are eagerly awaited. We contend that the complex legal framework risks posing headaches to bona fide companies deploying biometric data for multifactor authentication and that the new legal regime is not reaching its goal of finding a balance between the free movement of such data and protecting citizens. Law enforcement authorities also need clear guidance. It is questioned whether Directive (EU) 2016/680 provides this.

1. Introduction

The launch of the iPhone X with face recognition deserves our attention in many respects. The 10th anniversary of the introduction of the now omnipresent smart phone was celebrated with the confirmation of the use of face recognition – as widely speculated – for unlocking the phone. It is in the first place irrefutable that for a widespread population, biometric data use becomes evident and becomes the norm in all kinds of personalised objects which need security and convenience. This type of use therefore leads to a considerable *increased public acceptance* of collecting unique human characteristics in a context other than crime, for a large number

* KU Leuven – Law Faculty – Citip – iMec, Sint-Michielsstraat 6, B-3000 Leuven, Belgium
E-mail address: els.kindt@law.kuleuven.be (E.J. Kindt)

https://doi.org/10.1016/j.clsr.2017.11.004
0267-3649/

Please cite this article in press as: E.J. Kindt, Having yes, using no? About the new legal regime for biometric data, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.11.004

of purposes.[1] In addition, and when looking closer, we should discern that precisely these types of biometric deployment will further increase important *collections* of biometric data.[2] At the same time, it remains unsure *where* these types of data are or will be stored, all depending on the 'playbook' of the architect of the system.[3] Laws have not provided clear guidance in the past. The question is whether this will change with the 'modernised' data protection legislation in the European Union.

The place of storage of biometric data is a relevant and critical factor. The storage place will to an important extent determine how such unique characteristics can be used: once the data is stored *in a database,*[4] biometric technology permits anyone to conduct an analysis and *searches* by comparing biometric information[5] captured in real-time or collected in any other way *post factum* with this pre-existing enrolment database. In this way one can in an automated manner directly or indirectly identify a person, i.e., to find out *who this person is,* based on physical, physiological or behavioural characteristics. As mentioned, the number of these biometric databases are growing, both in the hands of private and public entities. In other words, if someone has a face of a person and any database containing information about this individual and for example facial images, he or she could use this facial information to identify this individual and to take any action as desired. The central storage of biometric data allows for the identification of individuals, in both private and public places, which definitely changes such spaces. But it also changes government, policing and intelligence activities. In a technocratic society, this given may presently only be known or understood by a limited group of experts, resulting in limited or no discussion about the collection or use of biometric data and about the powers and risks of the misuse of biometric technology. 'The greatest dangers to liberty lurk in insidious encroachment of men of zeal, well-meaning but without understanding'.[6] While biometric technology surely can be supported and be effective for specific purposes such as crime investigation by competent authorities under clear legal conditions and independent oversight, any widespread use of such technology without or outside a clear legal framework should be worrying, but also the data collection of the biometric information *allowing* for such use. Once information is collected, such information will be used. This has been clearly proven already by the ever largest biometric collection and database Aadhaar in India, which was at its set up to be voluntarily and of which the objective was to provide citizen with a unique citizen ID. Soon thereafter, the collection became mandatory, for example to receive school meals or to open bank accounts, and access was provided to numerous non-governmental private sector entities for clearly different purposes.[7] This risk of collection and re-use was also at stake in the European Court of Justice cases *Schwarz* and *Willems* initiated by citizens who did not wish to part with their 'biometric data', which we discuss later. The collection of biometric data and the loss of anonymity pose risks to the exercise of fundamental rights, including but not limited to the rights to non-discrimination, freedom of expression, information and communication, freedom of assembly, due process and privacy and data protection and the entitlement to the presumption of innocence.[8] The Constitutional Court in France was in 2012 clear on the issue and stated that the keeping of a database with biometric identity information allowing identification interfered with the fundamental right to respect of privacy.[9]

The powers of biometric technology seem overall to be more a point of attention and debate in the United States. The Federal

[1] The next step our information society is awaiting is the seamless carry-over of the login based on unique human characteristics to other 'Things', e.g., when one steps into her or his car or home, realising the perfectly convenient body to machine communication.

[2] Such important data collections have been induced already by other so-called Big Five tech companies (Alphabet, Amazon, Apple, Facebook and Microsoft) such as when improving social network services and users were invited in posting (profile) pictures.

[3] While Apple announced in 2013 at the release of the iPhone 5S, embedding fingerprint recognition (Touch ID) for unlocking the phone that the fingerprint would never leave the phone and would not be stored in the cloud, one needs to discern that the technology functions as a black box. In addition, and shortly thereafter, Apple filed patents for synchronising Touch ID with other mobile devices and points of sale systems via iCloud whereby the (encrypted) fingerprints would actually be stored in the cloud. About these patents, see e.g., Ch. Zibreg, *Apple patents Touch ID iCloud sync, Apple Pay POS with embedded fingerprint sensor*, 15 January 2015. Available from: http://www.idownloadblog.com/2015/01/15/apple-patent-touchid-icloud/.

[4] For example, a database with mug shots of the police, a national registry with the facial images (and possibly fingerprints) and other identity details of citizens to whom an eID, passport or driver's license has been issued, a database with facial images uploaded on a social network site, an employee database with pictures, a membership list of a sports club with facial images, a list of missing persons, etc.

[5] E.g., facial images from a CCTV system, facial images from simultaneous high quality video streams brought together on a platform or taken by a body worn camera, facial images from a social network platform or taken by a smart phone, real-time scanned faces of pedestrians, latent (found) fingerprints of an unidentified person, etc.

[6] Justice Brandeis, dissenting, in *Olmstead v United States*, 277 US 438 (1928), 277. This Supreme Court case concerned the question whether wiretapping technology allowing governments tapping public telephone conversations invaded privacy. The Supreme Court affirmed a privacy invasion by wiretapping public telephone conversations only forty (40) years later in *Katz v. United States* of 1967.

[7] Several individuals filed complaints against this biometric collection. In the meantime, the Supreme Court of India recognised the right to privacy as a fundamental right, which decision will further impact Aadhaar: Supreme Court of India, No. 494 OF 2012, 24 August 2017. Available from: http://supremecourtofindia.nic.in/pdf/LU/ALL%20WP(C)%20No.494%20of%202012%20Right%20to%20Privacy.pdf.

[8] See also E. Kindt, *Privacy and Data Protection Issues of Biometric Applications*. A Comparative Legal Analysis, Dordrecht, Springer, 2013, pp. 297–306 ('Kindt, Biometric Applications 2013').

[9] Cons. const. (France) no. 2012-652, 22 March 2012 (*Loi protection de l'identité*), Article 6. The Court stated: '. . .la création d'un fichier d'identité biométrique (. . .) dont les caractéristiques rendent possible l'identification d'une personne à partir de ses empreintes digitales porte atteinte inconstitutionnelle au droit au respect de la vie privée'.

Please cite this article in press as: E.J. Kindt, Having yes, using no? About the new legal regime for biometric data, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.11.004