YES, I WILL! CONSENT DILEMMAS INVOLVING FACIAL RECOGNITION TECHNOLOGY

Natalia Menéndez González

INTRODUCTION

Consent is one of the (most claimed) lawful grounds for data processing in general and by Facial Recognition Technology (FRT). However, the abuse of this ground for processing, along with several uncertainties when applied to actual FRT deployments have given rise to an important group of matters related to consent within the FRT field. This work will analyse the current covering given by the GDPR and the Law Enforcement Directive to the consent problems posed by FRT. Since both laws have not been thought to respond specifically to FRT, many consent issues arising from FRT implementation are not sufficiently addressed by the norms, ending up in privacy breaches. Moreover, the FRT industry has also spotted some incongruences when trying to apply the legal text to the actual situation. This work aims at shedding light on these conundrums and finding a remedy to them by using the instruments at hand within the GDPR.

CONSENT AS A LAWFUL GROUND FOR PROCESSING

Article 4.11 GDPR determines that consent should be a 'freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'. This definition is complemented by Recital 32 of the same legislative body, which states that '[c]onsent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them.' Consent is a fundamental (and often abused) piece within the GDPR, based on the 'notice and consent' model.[1]

According to Kim, the requirements of consent are twofold.[2] Firstly, a person must be able to validly agree with the activity proposed. This means that they can consent intentionally and have the necessary expertise to be able to exercise their will in the light of their motives. Secondly, social benefits must

[1] Many voices claim nowadays that the companies just 'made' the data subject agree with long consent statements and, by this formula, they relax their data protection measures, since they count on the consent of the data subject. *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L119) 1, 4.

[2] NANCY S. KIM, CONSENTABILITY: CONSENT AND ITS LIMITS (Cambridge Univ. Press eds., 2019).

outweigh the social damage to the activity. This last aspect might present a conflict in the specific case of FRT whose uses (at least, some of them) are supported by the 'public interest' clause, such as within the law enforcement field. In this case, the importance of clear and express individual consent might be outweighed by the greater 'social benefits of the activity'.

Kim identified three fundamental characteristics of legal consent determination at the individual level, being: a deliberate manifestation of consent; knowledge; and will.[3] However, the real situation is much more complex. Voluntarism is troubling because people are constrained by their environment such that no person is always truly or ideally autonomous. While these complications are overwhelming, Kim considers the condition of the knowledge the most difficult to meet. This is due to both a lack of relevant information and access to all the relevant details.

Regarding access, information must be intelligible, important and useful. To develop communication criteria that satisfy the knowledge condition, cognitive limitations are necessary, but also insufficient. When consent is sought, the quality of the information provided should be adjusted to two factors: the risk to the individual and collective autonomy of the transaction; and the confidence of the parties seeking consent. Therefore, the consent framework is adjusted to a slipping standard. The greater the risk of autonomy, the more a person can understand. Kim derives a basis for demarcating valid from invalid consent at the individual level by linking the level of risk to the quality or consent-seeking disclosure. She argues that consent is invalid when the threat to independence is beyond the strength of the conditions for consent. In other words, if there is a serious threat of autonomy for a transaction and the conditions of consent do not correspond to the risk, valid approval can not be given.

Although consent may appear either to be valid or to be invalid, because an offer can either meet the consent standard, things will be more complex. One of the two results is an offer accepted under poor conditions of consent. Either the transaction occurs without real consent, or the offer is accepted by defaulting approval. This might be the case in people consenting to be subjected to FRT in situations of a terrorist threat or health emergency.[4] Word choice might also affect framing because

---

[3] *Id.*

[4] **'**People fear the normalisation of surveillance but are prepared to accept facial recognition technology when there is a clear public benefit, provided safeguards are in place. For example, nearly half (49%) support the use of facial recognition technology in day to day policing. ADA LOVELACE INSTITUTE, BEYOND FACE VALUE: PUBLIC ATTITUDES TO FACIAL RECOGNITION TECHNOLOGY (2020), https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/.

how options and issues are presented can influence people's perception of risks and solutions.

The scholarship is divided regarding the real scope of consent. Some authors argue that consent is irrelevant: generally, it does not depend on actual information or a real option. As discussed by some scholars, the analysis of personal data today (especially in FRT contexts) is so complicated that most people lack the expertise to grasp them and foresee the risks involved.[5] Also, even if data subjects had that expertise, they would not have the time and resources to evaluate the information in each privacy policy. This makes individuals sensitive to user interfaces and dense and confusing privacy policies that are designed to use their exhaustion to obtain consent. If the damage is framed by abstract concepts of private protection, and the possibility to abuse is too far from readily predictable, the risk analysis by the people may be harmed by a lack of capacity to take stock of the threats adequately. Lastly, if many different decisions spread the risk of harm, there is no appropriate incentive for people to take every request for consent seriously.

LEGAL EFFECTS OF THE CONSENT PROVISIONS APPLIED TO FRT

It has been established that a denial of consent might mean that services which are essential or even required for data subjects could not be used (or limited). Other authors confirm that consent does not cover the potential, often undefined, use of data, even when such use is socially advantageous.[6] This is precisely the case pointed to by academics of an apparent incompatibility between Big Data (FRT databases are composed of plenty of facial images from diverse backgrounds) and Art. 6 GDPR.[7] Art. 6 GDPR establishes consent as a fundamental pillar

---

[5] Evan Selinger & Woodrow Hartzog, *The Inconsentability of Facial Surveillance*, 66 Loy. L. Rev. (2020); Stefan Schiffner et al., *Towards a Roadmap for Privacy Technologies and the General Data Protection Regulation: A Transatlantic Initiative*, 6 PRIVACY TECH. POL'Y 24 (2018), https://link.springer.com/chapter/10.1007/978-3-030-02547-2_2; Giovanni Sartor et al., *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence* (2020), https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf.; Genia Kostka et al., *Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States* (forthcoming 2021), https://journals.sagepub.com/doi/pdf/10.1177/09636625211001555.

[6] FRED H. CATE ET AL., DATA PROTECTION PRINCIPLES FOR THE 21ST CENTURY: REVISING THE 1980 OECD GUIDELINES (2014), https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf.

[7] ROSARIO GIRASA, ARTIFICIAL INTELLIGENCE AS A DISRUPTIVE TECHNOLOGY: ECONOMIC TRANSFORMATION AND GOVERNMENT REGULATION 3-21 (2020); Sartor, *supra* note 5; Schiffner, *supra* note 5; Sandra Wachter, *Data protection in the age of big data*, NATURE

for lawful data processing. Using Big Data to train AI systems and allow them to make inferences might be contradictory with the lawfulness of processing in the sense that, even, some of the purposes of the AI training stage could not be anticipated. The AI-empowered system could end up making inferences that the data processor might not have anticipated and therefore, collected consent for. Sartor argues that this incompatibility might be solved by 'a flexible application of the idea of compatibility, which allows for the reuse of personal data when this is not incompatible with the purposes for which the data were originally collected'.[8] Moreover, some research has pointed out that, in the case of face categorisation, consent might not be free and informed (because both the uses and functioning of the technology are uncertain up to some extent due to its innovative and 'black box' nature) and therefore, the processing might be considered unlawful.[9] The different functions that FRT may perform have to be also taken into account. In the worst scenario, the data subject might end up 'swamped' with consent requests.

The question raised by these statements is whether the notions of consent and purpose limitation might be applied in a manner which is both significant to the subject and compatible with the potential use of the data. In the same line, several authors have spotted a risk to privacy when biometric data, in general, are used for secondary purposes not compatible with the ones for which the data were initially collected. They make a special emphasis in cases where third parties with access to facial images (such as law enforcement agents), cross-check them along with any other information, without consent from the data subject. [10] This might present problems in cases where FRT is built on top of a different system, such as a thermal scanner. What kind of consent should then be asked? For the template extraction? Face detection? Temperature measurement? Furthermore, due to the innovative nature of the technology and the low degree of trust it enjoys, people do not possess enough knowledge and power to understand the true impact of what they are consenting to.[11] The only current 'countermeasure' in this respect is Art. 21 GDPR.[12] This article provides the data subject

---

ELECTRONICS, Jan. 2019, at 6-7, https://www.nature.com/articles/s41928-018-0193-y.

[8] Sartor, *supra* note 5.

[9] Sartor, *supra* note 5; Schiffner, *supra* note 5; Selinger, *supra* note 5.

[10] ANN CAVOUKIAN, PRIVACY AND BIOMETRICS (1999), https://www.ipc.on.ca/wp-content/uploads/resources/pri-biom.pdf; Ioannis Iglezakis, *EU data protection legislation and case-law with regard to biometric applications*, *in* AN INFORMATION LAW FOR THE 21ST CENTURY 40-53 (Maria Bottis ed., 2011).

[11] Selinger, *supra* note 5; Schiffner, *supra* note 5; Sartor, *supra* note 5; Kostka, *supra* note 5.

[12] '1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data

with the right to object, although it might not be sufficient according to the previously painted scenario.

According to Sartor, two aspects are necessary: first, notices of consent should concentrate on the main problem and be user-friendly and transparent. Easy to understand and transparent detail should be provided on how sensitive processing can be opted into or out of, such as when it comes to monitoring or data transfer to third parties. For instance, additional opt-out or opt-in options could be given to the data subject to convey desires relevant to surveillance, profiling, etc. Second, the GDPR provides the space for the processing of the data gathered for some reasons for additional purposes as long as they are consistent with those of the original. Therefore, it seems that the principles of consent and purpose limitation can tend to be construed in ways which are compatible with both data subject protection and allowing beneficial uses of FRT.

Art. 7 GDPR establishes the necessary conditions for consent.[13] A problem arising from such conditions is the

---

concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.'

[13] '1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing

difficulty for the data controller to determine when consent is specifically needed for a certain action or if other justifications, such as the use of the legitimate interest clause, might suffice.[14] However, particularly strong regard should be paid to what constitutes a legitimate interest. Legislators will have to take this notion seriously to strengthen the power of data controllers.

One of the possible solutions to the consent conundrum might be the establishing of a compliance standard for consent. This standard could include legal assessment and possible certification (in the same line as conformity assessments for product risk or ISO standards). It would act as an incentive for technology suppliers that currently express their uncertainty against a volatile technology in a rapid-changing scenario to try to include privacy by design and default criteria on their designs and deployments.[15]

---

based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.'

[14] Schiffner, *supra* note 5.

'Legitimate interest may be the most accountable ground for processing in many contexts, as it requires an assessment and balancing of the risks and benefits of processing for organisations, individuals[,] and society . . . . The legitimate interests to be considered may include the interests of the controller, other controller(s), groups of individuals[,] and society as a whole.' CENTRE FOR INFORMATION POLICY LEADERSHIP GDPR IMPLEMENTATION PROJECT, RECOMMENDATIONS FOR IMPLEMENTING TRANSPARENCY, CONSENT AND LEGITIMATE INTEREST UNDER THE GDPR (2017), https://iapp.org/media/pdf/resource_center/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf; *see also* CENTRE FOR INFORMATION POLICY LEADERSHIP GDPR IMPLEMENTATION PROJECT, CIPL EXAMPLES OF LEGITIMATE INTEREST GROUNDS FOR PROCESSING OF PERSONAL DATA (2017), https://iapp.org/media/pdf/resource_center/final_cipl_examples_of_legitimate_interest_grounds_for_processing_of_personal_data_16_march_2017.pdf.

[15] Article 25 GDPR: '1.Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures

CASE-STUDY: CONSENT IMPLICATIONS OF FRT'S USE BY LAW ENFORCEMENT

In compliance with the Law Enforcement Directive, the law enforcement authorities have different responsibilities to provide information to the data subjects.[16] For example, for the processing purposes and exercising of the data rights of persons. Forces must consider how best to explain this to the public (either through signposting and flyers within the physical space, on the Internet or a mix of methodologies). The police will need to use its Internet site and social media channels to offer updates and plans to the public about their FRT strategy.

The UK's DPA considers exceedingly doubtful that, for compliance where police use FRT in public spaces, people and others who are not on the watchlist will give legitimate consents for the collection of their biometrics.[17] The Commissioner, consequently, wants the police and other law enforcement authorities to focus on processing that is required to carry out a role undertaken by a competent authority. This is consistent with the judgments of the High Court in *Bridges v. SWP* (2019) (updated by the appealing decision).[18] However, the extent to which law enforcement authorities undertake this provision should be further developed, as suggested by the judgement.

As an example regarding the information requirement for consent, explained above, a minimum specification would provide a simple indication that FRT is used. Moreover, the public should be informed in advance about FRT's use to comply with the provisions of the legislation.

According to the Commissioner, signage ads for the existence of a FRT camera should be conspicuous to notify the public effectively. The signs should clarify the following:

- Use of FRT cameras;

---

shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.'

[16] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, 2016 O.J. (L119) 89.

[17] INFORMATION COMMISSIONER'S OFFICE, INFORMATION COMMISSIONER'S OPINION: THE USE OF LIVE FACIAL RECOGNITION TECHNOLOGY BY LAW ENFORCEMENT IN PUBLIC PLACES (2019), https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf.

[18] R (Bridges) v. Chief Constable of South Wales Police & Information Commissioner [2020] EWCA Civ 1058 (appeal taken from Eng.), https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf.

- Processing of biometric information;
- That the police is processing the data for the given reason.

Conversely, the criteria employed within law enforcement contexts might also enlighten the GDPR case.

CONCLUSION

There are several gaps within the actual procedure, the public expectations and the provisions of the legislation when it comes to consent. Whether or not a subject's consent is needed to use FRT and on what grounds depends on many factors, such as the function performed by the system, its use by law enforcement and on what role. As a result, the regulatory system must be updated and explained and ensure that improvements in technology as well as general standards are preserved rapidly. The danger to privacy of faulty consent for FRT must be carefully assessed because we might be at a case where social damage overshadows the autonomy of individuals.