CENTER FOR DEMOCRACY & TECHNOLOGY

Via e-mail to EDPB@edpb.europa.eu

9 September 2019

European Data Protection Board
Rue Wiertz 60, B-1047 Brussels

RE: Guidelines 3/2019

On 10 July 2019, the European Data Protection Board (EDPB) adopted its Draft Guidelines on the processing of personal data through video devices (Draft Guidelines). The EDPB has invited public comments on this document by 9 September 2019. The Center for Democracy & Technology (CDT)[1] welcomes the opportunity to submit the comments below as input for the EDPB's final Guidelines.

Comments

CDT appreciates the Draft Guidelines' recognition that video surveillance analytics and associated facial recognition technologies (FRT) create "massive" data protection implications. Video captured at a distance and combined and processed at the scale possible today is in tension with basic Fair Information Practices (FIPs) and the fair processing principles in the General Data Protection Regulation (GDPR). Video analytics raises its own ethical concerns,[2] but CDT's comments are focused on (1) the need for additional clarity in GDPR-mandated balancing tests for video processing and (2) FRTs, which implicate special category data under the GDPR.

- Video surveillance should remain the exception and not the rule -- even when talking about security purposes.

One aim of the GDPR is to encourage data controllers to think more holistically about their data collection and processing practices. The proliferation of cheap and connected cameras makes this mandate more pressing. As the EDPB notes, video surveillance has implications for how data subjects behave in both public and private. Entities deploying video cameras in public spaces are directed to provide clear evidence to demonstrate this is strictly necessary and proportionate under the circumstances and that there is a legal basis for such activity.[3]

[1] CDT is a non-profit advocacy organization working to promote democratic values online and in new, existing, and emerging technologies. CDT pursues this mission by supporting laws, policies, and technical tools which empower users, protect privacy, and preserve individual rights online.

[2] ACLU Report

[3] https://www.biometricupdate.com/201908/uk-information-commissioner-investigates-automatic-facial-recognition-use-and-issues-warning

This demand raises special challenges for security-related purposes for video surveillance.[4] While security-related applications are one of the primary drivers of video surveillance, it is unclear whether data controllers have given sufficient thought to their data protection obligations for these activities. One of the earliest fines for noncompliance with the GDPR related to an Austrian's retailers use of CCTV cameras.[5]

The Draft Guidelines reiterate that organisations must justify their use of video monitoring, even for security-related purposes, but the EDPB should provide more guidance and clarification as to how this must be done initially and over time. For example, paragraph 20 encourages organisations to document and present statistics of criminal activity in their neighborhood prior to deploying CCTV. This begs several questions that warrant further analysis: What level of criminal activity is necessary before a business can reasonably determine in has a legitimate interest in surveilling its grounds? Beyond petrol stations and jewelers, the Draft Guidelines might offer other scenarios that arise to imminent danger situations. Once a situation is determined to be sufficiently risky, however, must this information be reassessed over time? And how frequently? Otherwise, this would seem to suggest video surveillance can be used indefinitely upon an initial documentation of a specific issue.

- As the UK Information Commissioner's Office has noted, the widespread, realtime use of FRTs represents "a step change from the CCTV of old."[6]

CDT's baseline position is that organisations using FRTs generally obtain informed consent from data subjects prior to identifying them via facial characteristics in public places or in places of public accommodation. Deployment of FRTs also requires entities to provide data subjects with clear, prominent notice of any use of FRTs in use.[7] We appreciate, also, that the Draft Guidelines make clear that disclosure by itself has "no relevance when determining what a data subject objectively can expect."

FRTs and video analytics capabilities fundamentally challenge what an individual's reasonable expectation of privacy can and should be. While touting these technologies' benefits to the public, both public and private organisations have not been forthcoming about how they intend to use face tracking capabilities.[8] If entities are confident that their use of these technologies is reasonable and justified, there is no reason for them not to be open about their practices.[9] Unfortunately, as the Draft Guidelines

[4] Many existing recording best practices specifically exclude security applications: https://www.ntia.doc.gov/files/ntia/publications/privacy_best_practices_recommendations_for_commercial_use_of_facial_recogntion.pdf

[5] E.g., https://iapp.org/news/a/austria-announces-first-gdpr-fine/

[6] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/blog-live-facial-recognition-technology-data-protection-law-applies/

[7] See Face Recognition Principles are a Step Forward But Congress Needs to Act (21 Sept. 2018), https://cdt.org/blog/face-recognition-principles-are-a-step-forward-but-congress-needs-to-act/.

[8] https://www.aclu.org/blog/privacy-technology/surveillance-technologies/are-stores-you-shop-secretly-using-face

[9] https://www.aclu.org/sites/default/files/field_document/061819-robot_surveillance.pdf

acknowledge, biometrics systems are being deployed in uncontrolled environments. Neither an appropriate degree of transparency nor the required standard of consent are being obtained from data subjects.[10] Policymakers have already questioned the legality of these deployments.

Meaningful transparency of FRTs and video analytics may prove challenging. We appreciate the Draft Guidelines proposal to encourage multi-layered notices, but as CDT cautioned the U.S. Federal Trade Commission in 2012, iconography takes both time and consumer education to be meaningful and merely appending biometrics and profiling disclosures to existing CCTV signs is not adequate.[11] Developing a standardized set of icons or symbols to convey different forms of video surveillance may be a worthwhile endeavor, but it will be difficult.[12] A standardized symbol, such as the recycling symbol or wheelchair icon, can be an ideal form of notice, but success requires industry-wide adoption and public education. Neither seems likely or effective with respect to FRTs.

Furthermore, any such transparency effort should also be separated from any discussion of consent by a data subject to the use of FRTs. While industry stakeholders have pushed for implied consent mechanisms for face tracking,[13] the Draft Guidelines reiterate the high standard under the GDPR that consent both be meaningful and affirmative. We agree that merely entering a marked area cannot constitute either a state or a clear affirmative action needed to satisfy the conditions for consent under Article 7. The Draft Guidelines' recommendation that FRTs only be deployed in separate and user-initiated circumstances is warranted, and addresses the lack of meaningful choice that exists in many of these situations such as where landlords use FRTs as building access mechanisms.[14]

- Facial analysis applications raise their own data protection implications.

However, beyond longstanding challenges to providing meaningful notice and obtaining meaningful consent, wide-scale usage of FRTs and video analytics present a threshold question of whether any entity can responsibly undertake such processing in a manner that complies with the GDPR.

Video analytics technologies are reliant upon training datasets and widespread access to and sharing of images. This disclosure and sharing of video data with third parties remains fundamentally problematic. [15] The EDPB ought to provide guidance as to what processing -- and in what fashion -- is in the public interest under the GDPR. For example, the Draft Guidelines acknowledge that FRTs introduce bias issues

[10] https://twitter.com/riptari/status/1141687908824432640
See also https://www.theguardian.com/commentisfree/2019/aug/18/facial-recognition-is-now-rampant-implications-for-our-freedom-are-chilling
[11] https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf, at 15, footnote 54.
[12] https://www.engadget.com/2019/04/19/sidewalk-labs-digital-transparency-icons-signs/
[13] MS/WPA blog
[14] https://gothamist.com/2019/05/08/hells_kitchen_landlord_sued_for_key.php
[15] FaceFirst data sharing: https://www.buzzfeednews.com/article/leticiamiranda/retail-companies-are-testing-out-facial-recognition-at

separate from privacy and data protection concerns. Addressing these bias issues may require additional data processing activities and the creation of training datasets that are, by themselves, highly sensitive. For example, to address errors in perceived gender classification, facial analysis algorithms will need to be assessed against nonbinary and trans datasets.[16] Care should be taken that these datasets are developed in an ethical and transparent fashion, unlike several existing photo datasets produced by academic institutions[17] or scraped from photos made available online.[18] The EDPB is well positioned to clarify how organisations may process video and image data for research purposes to improve FRTs and facial analysis algorithms.[19]

However, we acknowledge, as the Draft Guidelines do, that certain types of video processing and FRTs are intended to distinguish one category of people from another but not to uniquely identify anyone. CDT has traditionally understood the data protection impact of face tracking as ranging on a spectrum from individual counting towards demographic targeting and individual identification.[20] Industry stakeholders have suggested reassessing these categories, introducing the concept of "pseudonymous facial recognition" via unique persistent identifiers that can be used by data controllers to track individual behaviors across time and space without linking this to other personal data.[21] We support the approach taken by the Draft Guidelines per paragraph 81 that these activities constitute identifying an individual subject and should be subject to Article 9.

- Images and biometric templates warrant the strongest possible security measures

CDT supports the Draft Guidelines discussion of organisational and technical security measures in Section 9.2. Recent reports of a breach of biometrics systems used by banks, law enforcement, and defense companies in the United Kingdom highlight the rudimentary data security lapses that continue to plague controllers and processors of the most sensitive data.[22] In addition to the practical measures put forward by the Draft Guidelines, this report demonstrates the need for organisations holding special category data to have procedures in place for communicating with security researchers.

---

[16] https://jezebel.com/amazons-facial-analysis-program-is-building-a-dystopic-1835075450

[17] https://www.dukechronicle.com/article/2019/06/duke-university-facial-recognition-data-set-study-surveillance-video-students-china-uyghur

[18] https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921

[19] https://iapp.org/news/a/how-gdpr-changes-the-rules-for-research/

[20] https://cdt.org/insight/seeing-is-iding-facial-recognition-and-privacy/

[21] https://fpf.org/2018/09/20/fpf-releases-understanding-facial-detection-characterization-and-recognition-technologies-and-privacy-principles-for-facial-recognition-technology-in-commercial-applications/

[22] https://www.engadget.com/2019/08/14/biometric-security-flaw-fingerprints/

CENTER FOR DEMOCRACY & TECHNOLOGY

Conclusion

CDT thanks the EDPB for this opportunity to provide comments on the Draft Guidelines. If you would like to discuss any of these comments or require additional information, please contact our Director for European Affairs, Jens Jeppesen, at jjeppesen@cdt.org or our office at eu@cdt.org.