Clearview AI, TikTok, and the Collection of Facial Images in International Law

Miriam Kohn*

Abstract

Private companies' collection of facial images is on the rise globally, which has major implications for both economic development and privacy laws. This Comment uses the facial recognition technology company Clearview AI and the video sharing app TikTok as case studies to examine the problems raised by these practices. After summarizing the relevant legal regimes created by the United Nations (U.N.) and the European Union (E.U.), it applies the E.U. privacy regime to TikTok's most recent Privacy Policy. The Comment concludes by proposing updates to the E.U. and U.N. privacy regimes to more effectively regulate TikTok's data collection and analogous business practices. These proposed updates include treating all facial images as special category biometric data under the E.U. regime and amending the U.N. regime to specifically cover digital privacy.

* BA 2017, University of Rochester; JD Candidate, 2023, The University of Chicago Law School. I would like to thank Professor Richard McAdams, Rachel Katzin, and Joshua Fox for their editorial guidance; Christopher Perkins for his explanation of the technical details of hash values; Professor James Hathaway, Professor Benedict Kingsbury, Navya Dasari, Helena von Nagy, Theresa Oliver, Diana Kenealy, Rebecca Jin, Julia Krusen, and Mason Pazhwak for their feedback through the 2022 Salzburg Lloyd N. Cutler Fellowship; and the entire editorial board and staff of the Chicago Journal of International Law for their invaluable assistance throughout the publication process.

Table of Contents

I. INTRODUCTION

Facial recognition technology (FRT) facilitates the identification of individuals from photos and videos based on their facial images.[1] The technology is increasingly prominent.[2] For example, the North American facial recognition market is expected to double by 2027.[3] The Chinese facial recognition market is also large and growing, connected to broad investment in artificial intelligence (AI).[4]

Although both China and the United States (U.S.) are leaders in AI, their markets reflect different investment patterns.[5] In China, the government has invested heavily in AI and FRT, boosting its surveillance capabilities.[6] In the U.S., AI development is primarily driven by private sector commercial applications.[7] The global growth of FRT and AI in both the private and public sectors has spawned a host of privacy and data protection issues.[8] Opponents are particularly concerned about invasion of privacy and misidentification, which seems to occur more often for non-male and non-white surveillance subjects.[9]

This Comment explores the implications of FRT and facial image collection through two case studies: Clearview AI (Clearview) and TikTok. Clearview is a pioneering FRT company.[10] As discussed in Section III, the novel ways in which its controversial software infringes on consumer privacy have spawned numerous court cases and regulatory complaints. TikTok is a popular video sharing app whose data collection practices include collection of users' facial images.[11] Clearview and TikTok are effective case studies because they have both achieved success through cutting-edge data collection. Other companies will likely follow suit, rendering these practices widespread. Additionally, because Clearview and TikTok are both powerful players in their respective markets, resolution of the legal issues they raise is important independent of implications for other

---

1 For more information on facial recognition systems, see Steve Symanovich, *What is Facial Recognition? How Facial Recognition Works*, NORTON (Aug. 20, 2021), https://perma.cc/Y4FK-4MFF.

2 Antoaneta Roussi, *Resisting the Rise of Facial Recognition*, NATURE (Nov. 18, 2020), https://perma.cc/D5HD-FT98.

3 *In Charts: Facial Recognition Technology — and How Much Do We Trust It?*, FIN. TIMES (May 16, 2021), https://perma.cc/Z9JF-CWHZ [hereinafter *In Charts: Facial Recognition Technology*].

4 *Id.*

5 *Id.*

6 *Id.*

7 *Id.*

8 *See* Eric Lander & Alondra Nelson, *Americans Need a Bill of Rights for an AI-Powered World*, WIRED (Oct. 8, 2021), https://perma.cc/M47B-GDX7.

9 *In Charts: Facial Recognition Technology*, *supra* note 3.

10 *See* Section I.A.

11 *See* Section I.B.

companies. Issues associated with facial image collection and FRT reach beyond traditional privacy law to implicate broader societal concerns such as the health of democracies,[12] political freedoms and human rights, and conceptions of consent in the digital age. This means that data collection by companies like TikTok and Clearview affects even people who do not use TikTok or are unconcerned about abstract notions of privacy.

Recent decisions by the Hamburg Privacy Guarantor[13] and other regulatory authorities[14] suggest that facial image collection is likely to be under-regulated under E.U. privacy laws. Accordingly, this Comment will argue that it is important to update the E.U. and U.N. privacy regimes to adequately address concerns raised by facial image collection practices before they become more widespread.

A. Clearview and Photo Scraping Practices

Although recent FRT innovation in the U.S. has occurred primarily in the private sector,[15] law enforcement demand has driven development. Law enforcement has historically relied on databases that use images from government records, such as mug shots and driver's license photos.[16] Both the availability of photos and technical details of photo searches have constrained the utility of these databases. That left a space in the market for larger, more user-friendly databases.

Clearview, a U.S.-based facial recognition service that made waves when a *New York Times* article highlighted its business practices,[17] is distinct from other FRT in three ways. First, Clearview "can automatically collect images of people's faces from across the internet, such as employment sites, news sites, educational sites, and social networks including Facebook, YouTube, Twitter, Instagram and even Venmo."[18] It collects these images despite sources' policies prohibiting "photo scraping."[19] Second, because Clearview does not require a head-on photo to generate a match, it utilizes photos more effectively than many other

---

12 *See generally* Scott Skinner-Thompson, *Agonistic Privacy and Equitable Democracy*, 131 YALE L.J.F. 454 (2021) (arguing that legal privacy protections are key for the health of democracies because they promote participation of marginalized groups).

13 *See* Section III.A.

14 *See generally* Section III.

15 *Id.*

16 Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Mar. 18, 2021), https://perma.cc/ETL3-J4YJ.

17 *Id.*

18 *Id.*

19 *Id. See also* Lori Kalani, et al., *Web Scrapers and Their Targets Beware. Regulators Are Zeroing in on Privacy Implications*, LEXOLOGY (Nov. 17, 2021), https://perma.cc/A55E-YCKT.

databases.[20] Third, Clearview is a private company that can monitor searches carried out in its software.[21]

Use of Clearview has taken off among law enforcement agencies, primarily due to its large database and ease of use. Clearview's CEO, Hoan Ton-That, said in 2021 that 3,100 government and law enforcement agencies use the service.[22] As Clearview's user base has grown, agencies have shared anecdotes about using the software to solve crimes ranging from child exploitation to bank fraud.[23]

This explosion in use has amplified privacy concerns connected to Clearview. Although "the accuracy of the tool is no longer a prime concern" after recent federal testing, its legality is still uncertain.[24] Additionally, privacy advocates remain concerned about photo scraping and Clearview's invasive nature.[25] As rapid growth has brought Clearview into the public eye, it has been the subject of lawsuits and regulatory complaints around the world.[26] The European Union (E.U.)'s responses to Clearview are discussed in Section III.

B. TikTok's June 2021 Privacy Policy

TikTok is a popular social media app. In 2020, it was the most downloaded app in the world.[27] TikTok is widely used around the world, but its parent company, ByteDance, is based in China.[28] Together with general privacy concerns, TikTok's ties to China have led to heightened suspicion of its business practices in countries whose governments have fraught relationships with the Chinese

---

20 Hill, *supra* note 16.

21 *Id.*

22 Will Knight, *Clearview AI Has New Tools to Identify You in Photos*, WIRED (Oct. 4, 2021), https://perma.cc/M8ME-RZSB.

23 Memorandum from Paul D. Clement on Legal Implications of Clearview Technology to Clearview AI 7 (Aug. 14, 2019), https://perma.cc/B5H7-7P5B (memorandum provided to potential customers by Clearview AI).

24 Kashmir Hill, *Clearview AI Does Well in Another Round of Facial Recognition Accuracy Tests.*, N.Y. TIMES (Nov. 23, 2021), https://perma.cc/K2PD-NC4N.

25 *Id. See also* Kashmir Hill, *Clearview AI Finally Takes Part in a Federal Accuracy Test.*, N.Y. TIMES (Oct. 28, 2021), https://perma.cc/L9BH-ZVWG.

26 *See, e.g.*, Byron Kaye, *Australia Says U.S. Facial Recognition Software Firm Clearview Breached Privacy Law*, REUTERS (Nov. 3, 2021), https://perma.cc/NC9B-BXE9; *Canada's Laws Need Updating to Protect Against Abuse from Surveillance Tech, Watchdog Says*, CBC RADIO (Oct. 8, 2021), https://perma.cc/A9EV-Z95S.

27 Rei Nakafuji, *TikTok Overtakes Facebook as World's Most Downloaded App*, NIKKEI ASIA (Aug. 9, 2021), https://perma.cc/QYU8-HRB9.

28 Megan McCluskey, *TikTok Has Started Collecting Your 'Faceprints' and 'Voiceprints.' Here's What It Could Do with Them*, TIME (June 14, 2021), https://time.com/6071773/tiktok-faceprints-voiceprints-privacy/.

government. The Trump administration's moves to ban TikTok in the U.S. illustrate this.[29]

TikTok enables users to upload short videos and view other users' content.[30] Because the platform is based on video sharing, TikTok necessarily has access to users' facial images. Its newest privacy policy, last released in June 2021 and updated in October 2021, authorizes the app to collect "biometric identifiers and biometric information," such as users' "faceprints and voiceprints."[31] The policy empowers the company to collect "information about the images and audio that are a part of your User Content," including "identifying the objects and scenery that appear, the existence and location within an image of face and body features and attributes, the nature of the audio, and the text of the words spoken in your User Content."[32] Privacy advocates have sounded the alarm based on the idea that "faceprints" and "voiceprints" are inherently personally identifiable information.[33]

Previous legal challenges related to TikTok's privacy practices are covered in Section IV. The new privacy policy has not yet faced serious legal challenges.

C. Roadmap

This Comment proceeds as follows. Section II summarizes two pertinent privacy and data protection regimes: those of the U.N. and E.U. Section III summarizes the legal treatment of Clearview's business practices to date. Section IV summarizes legal treatment of TikTok's data collection practices to date. Section V applies the E.U. legal regime discussed in Section II to TikTok's Privacy Policy and uses recent regulatory decisions regarding Clearview to analyze TikTok's data collection practices. Section VI argues that the E.U. and U.N. privacy regimes should be updated to more effectively regulate TikTok, Clearview, and other companies engaging in similar practices. The Comment concludes by briefly discussing the implications of Section VI.

---

29 Charlie Campbell, *How TikTok Found Itself in the Middle of a U.S.-China Tech War*, TIME (Aug. 6, 2020), https://time.com/5876610/tiktok-china-tech-war/.

30 For more information on how TikTok works, see Heather Schwedel, *A Guide to TikTok for Anyone Who Isn't a Teen*, SLATE (Sept. 4, 2018), https://perma.cc/CWK2-63QF.

31 Sarah Perez, *TikTok Just Gave Itself Permission to Collect Biometric Data on US Users, Including 'Faceprints and Voiceprints,'* TECH CRUNCH (June 3, 2021), https://perma.cc/2KEY-HTV4.

32 *Privacy Policy*, TIKTOK, https://www.tiktok.com/legal/privacy-policy-eea?lang=en (last visited Apr. 11, 2022). Although TikTok has separate privacy policies for users in the U.S. and users in the European Economic Area (EEA), the same language appears in both privacy policies. Both policies are available on TikTok's website, at the link provided. The link defaults to the EEA policy.

33 McCluskey, *supra* note 28.

II. INTERNATIONAL PRIVACY REGIMES

There is no global online privacy regime on point here. This Section, therefore, begins by discussing the U.N. privacy regime, which is global but does not clearly cover TikTok and Clearview. It then moves to the E.U. regime, which is not global but covers TikTok and Clearview.

A. The U.N.

The U.N. privacy regime is based on the Universal Declaration of Human Rights (UDHR)[34] and the International Covenant on Civil and Political Rights (ICCPR).[35] Because they are part of the U.N. privacy regime, they have a broader reach than do E.U. regulations. However, unlike the E.U.'s General Data Protection Regulation (GDPR), they are not specific to the modern privacy challenges stemming from cybersecurity and digital technologies. They also lack enforcement mechanisms.

1. UDHR

UDHR, which was published in 1948, articulates high-level formulations of fundamental rights.[36] UDHR does not contemplate the rise of the internet, which fundamentally reshaped the privacy landscape. It has not been updated since its drafting. UDHR Article 12 guarantees the right to privacy. It provides that "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[37] Because UDHR Article 12 is much briefer than the relevant provisions of GDPR, it is more difficult to clearly demonstrate its applicability to modern practices like photo scraping. Additionally, UDHR does not create legally binding obligations for signatory states.[38]

---

34 G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948) [hereinafter UDHR].

35 International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR].

36 UDHR, *supra* note 34.

37 *Id.* art. 12.

38 *See What is the Universal Declaration of Human Rights?,* AUSTL. HUM. RTS. COMM'N, https://humanrights.gov.au/our-work/what-universal-declaration-human-rights (last visited Apr. 11, 2022) ("The Universal Declaration is not a treaty, so it does not directly create legal obligations for countries . . . Some argue that . . . it has become binding as a part of customary international law.").

2. ICCPR

ICCPR, which was drafted in 1966, is similarly brief.[39] ICCPR Article 17 reads identically to UDHR Article 12.[40] Therefore, it is equally difficult to demonstrate its applicability to modern data collection practices.

3. The Special Rapporteur on the Right to Privacy

In 2015, the U.N. Human Rights Council adopted a resolution appointing the Special Rapporteur on the Right to Privacy for a three-year term.[41] That term was subsequently renewed for another three years.[42] The Human Rights Council reaffirmed the right to privacy protected in UDHR Article 12 and ICCPR Article 17 in its 2015 resolution appointing the Special Rapporteur.[43] That resolution explicitly stated that "the same rights that people have offline must also be protected online, including the right to privacy."[44]

The Special Rapporteur does not produce legislation. Instead, its primary role is to "gather relevant information, including on international and national frameworks, national practices and experience, to study trends . . . in relation to the right to privacy."[45] It provides guidance for U.N. organs and legislating bodies. Its reports include components assessing protection of privacy rights by judicial authorities.[46]

4. Issues under the U.N. privacy regime

Clearview and TikTok's data collection practices raise two potential issues under UDHR and ICCPR. First, does casting a wide net for data collection constitute "arbitrary . . . interference with . . . privacy?"[47] The answer could change based on interpretations of "arbitrary," "interference," or "privacy." Sweeping collection of facial images may belong under this category. Previous

---

39 ICCPR, *supra* note 35.

40 *Id.* art. 17.

41 Human Rights Council Res. 28/16, U.N. Doc. A/28/16, at 3 (Mar. 26, 2015) [hereinafter Human Rights Council Res. 28/16].

42 Human Rights Council Res. 37/2, U.N. Doc. A/37/2 (Mar. 22, 2018).

43 Human Rights Council Res. 28/16, *supra* note 41, at 3.

44 *Id.*

45 *Id.*

46 *See, e.g.*, Report of the Special Rapporteur on the right to privacy, U.N. Doc. A/HRC/40/63, at 7 (Oct. 16, 2019) ("The Special Rapporteur supports the strict application of the tests of proportionality and necessity in a democratic society as an important benchmark with global repercussions.").

47 ICCPR, *supra* note 35, art. 17.

interpretations of ICCPR Article 17 have not squarely addressed this.[48] However, the Special Rapporteur has recommended minimizing data collection, "clear and detailed controls" in privacy laws, and a risk management approach,[49] which cut against sweeping facial image collection.

Second, what does "protection of the law" mean?[50] A law like GDPR might suffice, depending on its interpretation and application. However, a less strict solution might also suffice. Alternatively, if GDPR is interpreted in extremely permissive ways, more stringent regulations might be necessary.

B. The E.U.

1. General Data Protection Regulation (GDPR)[51]

GDPR, the main E.U. law on this topic, entered into force in 2016.[52] According to its official website, GDPR is "the toughest privacy and security law in the world."[53] It reaches beyond the borders of the E.U. because "it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU."[54] TikTok and Clearview are both regulated under GDPR because they process Europeans' data. The primary enforcement mechanism is fines.[55] "There are two tiers of penalties, which max out at €20 million or 4% of global revenue (whichever is higher), plus data subjects have the right to seek compensation for damages."[56]

GDPR compliance requirements differ for different types of data. This Comment discusses "biometric data" and "personal data." Under GDPR Article 4, "biometric data" is "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person,

---

48 *See, e.g.*, Human Rights Council General Comment No. 16, U.N. Doc. HRI/GEN/1/Rev.9, ¶ 10 (Apr. 8, 1988) (discussing the requirement for data collection to be regulated by law but not specifically commenting on sweeping data collection).

49 *See* Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, U.N. Doc. A/76/220, at 22–23 (Jul. 23, 2021) (discussing data privacy in the context of pandemic response).

50 ICCPR, *supra* note 35, art. 17.

51 Regulation 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. (L 119) [hereinafter GDPR].

52 Ben Wolford, *What is GDPR, the EU's New Data Protection Law?*, GDPR.EU, https://perma.cc/F67K-5SQW.

53 *Id.*

54 *Id.*

55 *See id.*

56 *Id.*

such as facial images or dactyloscopic data [fingerprints]."[57] "Personal data," on the other hand, might cover "a name, an identification number, location data, an online identifier" or "one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[58] In short, biometric data is a type of personal data that uniquely facilitates identification of individuals.

Personal data processing is regulated by GDPR Article 5.[59] Data processing must fall within a legal basis for collection of personal data under GDPR Article 6(1).[60] Additionally, data must be processed according to high-level principles: lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability.[61]

Lawfully processing special category biometric data requires satisfying both the Article 6 legal basis requirement and the conditions imposed by Article 9. Under Article 9, processing of "biometric data for the purpose of uniquely identifying a natural person," along with other "special categories of personal data," is prohibited except for prescribed exceptions.[62] The most pertinent exceptions for this Comment are when "the data subject has given explicit consent to the processing of those personal data for one or more specified purposes," "processing is necessary to protect the vital interests of the data subject," "processing relates to personal data which are manifestly made public by the data subject," or "processing is necessary for reasons of substantial public interest."[63]

In short, although all personal data is protected under GDPR, Article 9 restricts data processing more than Article 5 does. This distinction is especially important because many data processors and controllers[64] fail to comply with GDPR requirements[65] and regulators cannot possibly monitor or bring

---

57 GDPR, *supra* note 51, art. 4(14). "Dactyloscopy" is "the science of fingerprint identification." *Dactyloscopy*, ENCYC. BRITANNICA, https://perma.cc/F27P-V6SB.

58 *Id.* art. 4(1).

59 *See id.* art. 5.

60 *See id.* art. 6(1). *See also* Edward S. Dove & Jiahong Chen, *What Does It Mean for a Data Subject to Make Their Personal Data 'Manifestly Public'? An Analysis of GDPR Article 9(2)(e)*, 11 INT'L DATA PRIVACY LAW 107, 107–08 (2021).

61 GDPR, *supra* note 51, art. 5.

62 *Id.* art. 9(1). Article 9(1) also prohibits processing of other "special categories of personal data" that are not discussed in this Comment.

63 *Id.* art. 9(2). These terms are not defined in the text of GDPR and guidance on their interpretation is discussed in Sections V and VI.

64 *See* GDPR, *supra* note 51, arts. 4(7)–(8) ("'[C]ontroller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data." and "'[P]rocessor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.").

65 *See* Tamjid Al Rahat, et al., *Automated Detection of GDPR Disclosure Requirements in Privacy Policies Using Deep Active Learning*, ARXIV (preprint) (Nov. 8, 2021).

enforcement actions against every noncompliant company. In a context of imperfect enforcement, relative restrictiveness and specificity of regulatory requirements are critical for protecting sensitive data.

GDPR Articles 13 and 14 are also important for assessing the legal status of Clearview and TikTok's data collection practices in the E.U. Article 14 stipulates that, in cases "[w]here personal data have not been obtained from the data subject," data controllers and processors must provide data subjects with "the purposes of the processing for which the personal data are intended as well as the legal basis for the processing."[66] Article 13 imposes the same requirement "[w]here personal data relating to a data subject are collected from the data subject."[67]

Finally, GDPR Article 22 has important implications for Clearview and TikTok. Article 22(1) provides that "[t]he data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."[68] Because Clearview does not get data subjects' explicit permission, its practices would not qualify for the consent-based exception to the prohibition on automated processing laid out in Article 22(2).[69] Even if Clearview is not collecting special category biometric data, its practices could run afoul of the Article 22 prohibition on automated processing. This provision may also pose problems for TikTok.

2. The European Commission's Proposed AI Regulations[70]

The European Commission "is the EU's politically independent executive arm" and is responsible for proposing new E.U. legislation.[71] In April 2021, it released Proposed AI Regulations.[72] The regulations, which outlined "a risk-based framework for applications of artificial intelligence, included only a partial prohibition on law enforcement's use of biometric surveillance in public places—with wide ranging exemptions that have drawn plenty of criticism."[73]

While the Proposed AI Regulations are not binding, they may serve as a basis for future binding legislation. In the meantime, they reflect E.U. attitudes towards

---

66 GDPR, *supra* note 51, art. 14(1).

67 *Id.* art. 13(1).

68 *Id.* art. 22(1).

69 *See id.*

70 *Proposal For a Regulation of The European Parliament and of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts*, COM (2021) 206 final (Apr. 21, 2021).

71 *European Commission*, E.U. (last visited Nov. 19, 2021), https://perma.cc/TK3A-3U7M.

72 *See* Mark MacCarthy & Kenneth Propp, *Machines Learn that Brussels Writes the Rules: The EU's New AI Regulation*, BROOKINGS INST.: TECHTANK (May 4, 2021), https://perma.cc/CCW3-3HGX.

73 Natasha Lomas, *UK's ICO Warns Over 'Big Data' Surveillance Threat of Live Facial Recognition in Public*, TECHCRUNCH (June 18, 2021), https://perma.cc/7VR9-TQRK.

FRT and may provide clues about regulatory authorities' application of GDPR to Clearview, TikTok, and other companies collecting facial images. The law enforcement exception is particularly significant because it opens the door to many potentially under-regulated uses of FRT.

3. The Council of Europe's Guidelines on Facial Recognition[74]

The Council of Europe is an international human rights organization that promotes democracy, human rights, and the rule of law in Europe.[75] Unlike the similarly named European Council, it is not an E.U. institution.[76] In 2021, the Council of Europe released new guidelines on facial recognition.[77] These guidelines provide high-level guidance for parties making decisions regarding FRT.[78] The guidance for legislators advises that, for each use, the legal framework should provide: "a detailed explanation of the specific use and the intended purpose; the minimum reliability and accuracy of the algorithm used; the retention duration of the photos used; the possibility of auditing these criteria; the traceability of the process; [and] the safeguards."[79] Based on GDPR, the guidance also says FRT use must have a legal basis, and must be assessed based on factors including proportionality and "the impact on the rights of the data subjects."[80]

Another noteworthy provision is that "[c]onsent should not, as a rule, be the legal ground used for facial recognition performed by public authorities in view of the imbalance of powers between the data subjects and these authorities."[81] This guidance also encompasses "private entities authorised to carry out tasks similar to those of public authorities."[82]

Finally, the guidance focuses on facial image processing that enhances identifiability of data subjects, not mere possession of facial images.[83] It is particularly focused on "biometric data templates," defined as "digital representation[s] of the unique features that have been extracted from a biometric sample and [are] stored in a biometric database."[84]

---

74 COUNCIL OF EUR., GUIDELINES ON FACIAL RECOGNITION (2021) [hereinafter GUIDELINES ON FACIAL RECOGNITION].

75 *See Do Not Get Confused*, COUNCIL OF EUR., https://perma.cc/ZMH7-9VK2.

76 *See id.*

77 *See* GUIDELINES ON FACIAL RECOGNITION, *supra* note 74.

78 *See id.* at 3.

79 *Id.* at 7.

80 *Id.*

81 *Id.* at 9.

82 *Id.*

83 *See id.*

84 *Id.*

4. Key issues under the E.U. privacy regime

Although individual regulators have ruled on Clearview's practices under GDPR, they have not issued general opinions, and Clearview has not been banned from the E.U. altogether. There have been no regulatory decisions regarding TikTok's latest privacy policy. Future treatment of Clearview and TikTok will likely turn on four questions.

First, are the facial images at issue biometric data or personal data for purposes of GDPR? There is an ongoing debate about whether all pictures of individuals are "biometric data."[85] Because both TikTok and Clearview collect facial images, the classification of images has implications for both entities' GDPR compliance requirements.

Second, how will Clearview's data be used? Decisions based on photo scraping-supported FRT may present additional GDPR compliance challenges. Decisions "based solely on automated processing, [including profiling], which produces legal effects concerning [the data subject] or similarly significantly affects him or her"[86] may violate GDPR independent of concerns about consent and data classification.

Third, could Clearview satisfy any of the GDPR Article 9 exceptions? Clearview markets itself as a service for law enforcement, not private parties.[87] Superior FRT used exclusively by governmental authorities for critically important public goals like terrorism prevention could theoretically satisfy the "substantial public interest"[88] exception for Article 9.[89] Similarly, Clearview could argue that it qualifies for the Article 9 exemption based on the scraped photos being "manifestly made public by the data subject"[90] because they are pulled from social media and other public-facing websites. Although TikTok is not marketing itself as geared toward law enforcement, it might similarly attempt to fit its practices

---

85 Catherine Stupp, *Clearview AI Raises Disquiet at Privacy Regulators*, WALL ST. J. (Feb. 4, 2021), https://perma.cc/3MES-CHFR (citing authorities weighing in on whether a facial image is inherently biometric data).

86 GDPR, *supra* note 51, pmbl. (71).

87 *See* CLEARVIEW AI, https://perma.cc/5JEN-2EJK.

88 GDPR, *supra* note 51, art 9(2)(g).

89 *See* Louis-Philippe Gratton, *Expert Commentary*, GDPR TEXT: ARTICLE 9 GDPR PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA, https://perma.cc/XXF5-FHQG:

> The terms 'substantial public interest' are not defined in the General Data Protection Regulation. As the exception refers to the Union or Member State law, article 9 2) (g) gives a margin of appreciation to the national jurisdictions . . . A substantial public interest may be related to the exercise of fundamental rights and freedoms, like organizing the electoral process, or the maintenance of order and security, like fighting terrorism."

90 *Id.* art. 9(2)(e).

under the "manifestly made public" exception to Article 9 if the images it collects are Article 9 special category data. This is discussed in Section V.

Fourth, to what degree can TikTok and Clearview be said to provide notice to data subjects, as required under GDPR Articles 13 and 14? Because data subjects must agree to TikTok's terms of use to use the app, this is primarily a question about adequacy of disclosures. As discussed in Section III, lack of data subject consent has already posed problems for Clearview.

III. LEGAL TREATMENT OF CLEARVIEW AND OTHER FACIAL RECOGNITION SOFTWARE IN THE E.U. TO DATE

A. The Hamburg Privacy Guarantor (HPG) Complaint

German citizen Matthias Marx filed a complaint with the HPG, a state-level data protection authority in Germany, seeking deletion of his personal data collected by Clearview.[91] Because the data was collected without Marx's consent, HPG ordered Clearview to delete the data.[92] However, HPG's order only required deletion of the hash values associated with images of Marx.[93] The order did not require Clearview to delete the captured images, which Marx had also requested.[94]

A hash value pseudonymizes sensitive data. From a technical perspective, "[a] digest or hash function is a process which transforms any random dataset in a fixed length character series, regardless of the size of input data."[95] The output of a hash function is a hash value.[96] Hash values allow data grouping because the same unique input always generates the same unique output.[97] "[A]pplying a hash function to a direct identifier should prevent the re-identification of this direct identifier."[98] However, features of the input and the hash function may increase the chances of re-identification.[99]

---

91 DER HAMBURGISCHE BEAUFTRAGTE FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT (HAMBURG COMM'R FOR DATA PROT. AND FREEDOM OF INFO.), CONSULTATION PRIOR TO AN ORDER PURSUANT TO ARTICLE 58(2)(G) GDPR 1 (2021) [hereinafter HAMBURG DPA DECISION].

92 *See id.* at 4.

93 *See Clearview AI Deemed Illegal in the EU, But Only Partial Deletion Ordered*, NOYB (Jan. 28, 2021), https://perma.cc/77NJ-9WKB.

94 *See id.*

95 AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS & THE EUR. DATA PROT. SUPERVISOR, INTRODUCTION TO THE HASH FUNCTION AS A PERSONAL DATA PSEUDONYMISATION TECHNIQUE 5 (2019) [hereinafter INTRODUCTION TO THE HASH FUNCTION].

96 *See id.* "Hash" is sometimes used to refer to both the hash function and the hash value output. This Comment will use the terms "hash function" and "hash value" to avoid confusion.

97 *See id.* at 7.

98 *Id.* at 10.

99 *See id.* at 10, 12.

In plain English, a hash function is like a code. Because the same hash value always refers to the same input, a hash value is like an extremely complex codename. Whether a computer without access to the original hash function can "break the code" to figure out the data subject's identity depends on the nature of the hash function. A well-written hash function should be extremely difficult to "break."

In its decision, HPG classified the hash value associated with Marx as special category biometric data.[100] It reached this conclusion because Clearview "uses a specially developed mathematical procedure to generate a unique hash value of the data subject which enables identification."[101] Under this decision, Marx's data was governed by GDPR Article 9. HPG specifically stated that Clearview failed to qualify for any of the exceptions provided in GDPR Article 9(2), reiterating that Marx never consented to processing of his data.[102]

HPG's decision is particularly interesting for three reasons. First, the decision ordered the deletion of Marx's hash value but not his photos. The distinction is not necessarily meaningful for Clearview. However, it leaves images collected and stored without associated hash values in a legal gray area. Are they Article 9 special category data? Second, HPG wrote that Clearview failed to qualify for any of the Article 9(2) exceptions. However, it did not preclude the possibility that other FRT might fulfill Article 9(2) in the future. Third, HPG issued a narrow order applying specifically to Marx's complaint.[103] "Any European Data Protection Authority (DPA) has the right to issue general orders that go beyond the individual complaint."[104] Absent a general order, data subjects must submit individual complaints to have their data deleted.[105] This is significant because an individual complaint requirement will likely lead to fewer individuals' data being deleted. Data subjects must know they need to file a complaint, understand the relevant administrative procedures, and feel strongly enough to complete the submission process.

B. The Privacy International Complaints

Privacy International, noyb – European Center for Digital Rights, the Hermes Centre for Transparency and Digital Human Rights, and Homo Digitalis filed complaints against Clearview with multiple E.U. regulators on May 27,

---

100 *See* HAMBURG DPA DECISION, *supra* note 91, at 3.

101 *Id.*

102 *See id.*

103 *See* NOYB, *supra* note 93.

104 *Id.*

105 *See id.*

2021.[106] The complaints attacked Clearview's handling of both "regular" personal data and "biometric data."[107] They specifically alleged that Clearview failed to obtain the necessary data subject consent and lacks a "lawful basis for collecting and processing" any of its data.[108] Regulators were required to respond within three months of filing.[109] Since the filing of these complaints, data protection authorities in Greece, France, and the United Kingdom have started official investigations into the company's practices.[110]

C. The Commission Nationale de L'informatique et des Libertés (CNIL) Decision

CNIL, the French Data Protection Authority, ordered Clearview to cease collecting data of individuals located within French territory on December 16, 2021.[111] It also ordered Clearview to delete the data within two months of the decision.[112] The decision, which was a response to the Privacy International complaints and the other complaints, found that Clearview violated Articles 6, 12, 15, and 17 of GDPR.[113] CNIL specifically found that Clearview lacked a legal basis for collecting and processing biometric data under Article 6.[114] Failure to comply with the CNIL order within two months could result in sanctions and/or fines.[115] At the time of this writing, there have been no updates about Clearview's compliance with the CNIL decision.

D. The United Kingdom Information Commissioner's Office (UKICO) Opinion

UKICO, the U.K.'s national authority regulating data privacy, published an opinion condemning the use of Live Facial Recognition Technology (LFRT) in

---

106 *See Challenge Against Clearview AI in Europe*, PRIV. INT'L (May 27, 2021), https://perma.cc/NK4T-F2JA [hereinafter *Challenge Against Clearview*].

107 *Id.*

108 *Id.*

109 *See* Robert Hart, *Clearview AI — The Facial Recognition Company Embraced by U.S. Law Enforcement — Just Got Hit with A Barrage of Privacy Complaints in Europe*, FORBES (May 27, 2021, 08:22am) https://perma.cc/W892-BXK3.

110 *See* Privacy International (@privacyint), TWITTER (Sept. 23, 2021, 7:12AM), https://perma.cc/LRS6-P8LW.

111 *See Facial Recognition: the CNIL Orders CLEARVIEW AI to Stop Reusing Photographs Available on the Internet*, CNIL (Dec. 16, 2021), https://perma.cc/8ZHZ-UUPJ [hereinafter CNIL Opinion].

112 *See id.*

113 *See id.*

114 *See id.*

115 *See id.*

June 2021.[116] One source of law that it applied was U.K. GDPR.[117] Although neither Clearview nor TikTok utilize LFRT, UKICO's analysis has implications for both companies.

First, the opinion refers to biometric data being extracted from facial images, rather than facial images themselves constituting biometric data.[118] "Facial images become biometric data when 'specific technical processing' is carried out 'which allow or confirm the unique identification' of an individual. The individual does not have to be identified for this data to become biometric data—it is the type of processing that matters."[119] This conception mirrors HPG's categorization of the hash value associated with Marx as biometric data.

Second, the opinion notes that "[b]iometric data constitutes special category data whenever it is processed 'for the purpose of uniquely identifying a natural person[.]' . . . As such, biometric data will be special category data in the majority of cases."[120] Special category data must be processed according to the more stringent requirements of Article 9, rather than the more permissive requirements governing processing of other personal data.[121]

Third, the UKICO opinion highlights concerns that LFRT is unlikely to obtain adequate data subject consent for automated processing.[122] This fits with both the HPG decision and the regulatory complaints filed by Privacy International et al.[123] Because adequate consent under GDPR requires disclosure of the intended purposes of the data collection,[124] this affects both Clearview and TikTok.

Fourth, the opinion highlights bias and discrimination concerns.[125] Although the UKICO opinion does not discuss Clearview, one of privacy advocates' main concerns about Clearview is its lack of proven accuracy, especially when coupled

---

116 *See* Natasha Lomas, *UK's ICO Warns over 'Big Data' Surveillance Threat of Live Facial Recognition in Public*, TECHCRUNCH (Jun. 18, 2021), https://perma.cc/7VR9-TQRK.

117 *See Information Commissioner's Opinion: The Use of Live Facial Recognition Technology in Public Places*, INFO. COMM'R'S OFF. (Jun. 18, 2021), https://ico.org.uk/media/for-organisations/documents/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf (last visited Nov. 12, 2021) [hereinafter UKICO Opinion].

118 *See id.* at 5.

119 *Id.* at 26.

120 *Id.*

121 *See id.*

122 *See id.* at 31.

123 *See* HAMBURG DPA DECISION, *supra* note 91, at 3 (discussing consent of the data subject); *Challenge Against Clearview*, *supra* note 106 (alleging lack of data subject consent).

124 *See supra* Section II.B (discussing GDPR Articles 13 and 14).

125 *See* UKICO Opinion, *supra* note 117, at 6.

with broader concerns about FRT bias.[126] These concerns speak to the broad principles governing GDPR and may shape its application.

E. Other Statements by E.U. Regulatory Authorities

Other E.U. authorities have issued decisions that are relevant but not directly on point for this Comment. For example, the Office of the Deputy Data Protection Ombudsman (DDPO) of Finland, part of the Finnish national data protection regulator, reprimanded the Finnish National Bureau of Investigation (NBI) for its use of Clearview AI.[127] "[I]n late 2019 and early 2020 . . . four individuals at the NBI carried out a total of 120 searches on the system over the period of one month."[128] DDPO ordered the NBI to notify individuals whose identities were known that their images were used in the Clearview searches.[129] "Police were also directed to request Clearview to delete the information that it uploaded to the company's servers."[130]

The Swedish Data Protection Authority (SDPA), Sweden's national data protection regulator, likewise fined a school for GDPR violations for using FRT to take attendance.[131] Although the school obtained parents' consent to run a pilot program, the consent was inadequate because of the power imbalance between the students and the school board.[132] SDPA also concluded that the program was an unjustifiable invasion of privacy because there are less intrusive ways to take attendance.[133] Although the program at issue was not Clearview, this analysis about the characteristics of legally adequate consent for FRT applies to Clearview's practices. The focus on a less restrictive alternative is also pertinent.

Similarly, in 2020, the French Administrative Court of Marseille invalidated the use of FRT to control access of students and visitors to a high school.[134] The court based its decision on legally inadequate consent and proportionality, with the FRT regime failing the proportionality inquiry because there was a less restrictive alternative available.[135] Notably, the opinion did not comment on the

---

126 *See* Hill, *supra* note 16.

127 *See Data Protection Ombudsman Raps Finnish Police over Controversial Facial ID App*, YLE –FINNISH BROAD. CO. (Sept. 29, 2021), https://perma.cc/NVH7-K836.

128 *Id.*

129 *See id.*

130 *Id.*

131 *See Facial Recognition in School Renders Sweden's First GDPR Fine*, EUR. DATA PROT. BD. (Aug. 22, 2019), https://perma.cc/R9KJ-MKY6 [hereinafter *Sweden's First GDPR Fine*].

132 *See id.*

133 *See id.*

134 *See* Julie Schwartz, *Facial Recognition Challenged by French Administrative Court*, HOGAN LOVELLS (May 29, 2020), https://perma.cc/55ML-8QGZ.

135 *See id.*

particularities of processing minors' biometric data under GDPR.[136] The decision also highlights the importance of clearly establishing an appropriate legal basis for data processing.[137] While security, public health, and other concerns that governmental authorities might address using Clearview are stronger legal bases than school attendance,[138] the legal basis for data processing remains important. For TikTok, which is not pursuing key governmental objectives, the threshold question of legal basis may be a major hurdle.

Finally, the European Parliament recently called for a ban on police use of FRT in public places, predictive policing, and private facial recognition databases like Clearview.[139] Although the resolution is non-binding, it is a strong indicator of current attitudes toward Clearview and commercial FRT.[140]

IV. TREATMENT OF TIKTOK'S DATA PRACTICES TO DATE

A. The Dutch Data Protection Authority (DDPA) Complaint

In July 2021, DDPA fined TikTok €750,000.[141] The DDPA fine was based on violations of GDPR Article 12, rather than failure to safeguard biometric data.[142] Specifically, "during the period from 25 May 2018 to 29 July 2020 inclusive, TikTok Inc. infringed Article 12(1) of the GDPR by failing to inform children in an intelligible language about the processing of personal data."[143]

The DDPA opinion indicates that European regulators may subject TikTok to heightened scrutiny as the app becomes increasingly popular. However, it does not shed light on regulators' attitudes toward TikTok's broader data collection practices. First, it focuses on practices affecting children, who receive special protection under GDPR.[144] Second, it focuses on the notice function of providing a privacy policy in Dutch, rather than the content of the policy.[145] Third, it

---

136 *See id.*

137 *See id.*

138 *See id.* (discussing a previous Deliberation by CNIL and noting that "[w]here there are no strong security reasons or societal issues legitimating the processing, the identification of the legal basis for the implementation of facial recognition is therefore a crucial point that requires a high level of attention").

139 *See* Melissa Heikkilä, *European Parliament Calls for a Ban on Facial Recognition*, POLITICO (Oct. 6, 2021), https://perma.cc/PQ2A-G7CW.

140 *See id.*

141 *DPA Decision to Impose a Fine on TikTok*, AUTORITEIT PERSOONSGEGEVENS (Apr. 9, 2021) at 1, https://perma.cc/8D63-P9X5 [hereinafter *Dutch DPA Decision*].

142 *See id.* at 1.

143 *Id.* at 2.

144 *See* GDPR, *supra* note 51, art. 8 (specifying conditions for processing of children's data).

145 *See Dutch DPA Decision*, *supra* note 141, at 1 (providing a Privacy Policy to Dutch users only in English violated GDPR Article 12).

considers TikTok's practices prior to the introduction of its new privacy policy, which authorizes more extensive data collection. The data referenced in the decision,[146] which is classified as personal data under GDPR Article 4,[147] does not include "faceprints" or "voiceprints."

B. The Irish Data Protection Commission's (IDPC) Probe

In September 2021, the IDPC, Ireland's national DPA, opened two probes into TikTok's business practices.[148] The first probe will examine TikTok's handling of children's data, including age verification measures.[149] The second will investigate whether TikTok's transfer of personal data to China violates E.U. law.[150] IDPC has not provided an expected end date for either probe. If the probes find violations of GDPR, IDPC "is allowed to impose fines of up to 4% of global revenue."[151]

The IDPC probes exemplify a larger controversy. Other data regulators have historically been unhappy with the long investigations conducted by IDPC, which regulates many foreign companies whose E.U. headquarters are in Ireland.[152] This tension has led at least one regulator to say that GDPR's decentralized enforcement mechanisms may be ripe for reform.[153]

V. APPLICATION OF GDPR TO TIKTOK'S PRIVACY POLICY

This Section considers four applications of GDPR to TikTok: defining biometric data, assessing TikTok's legal bases for data collection, evaluating the Article 9(2) exemptions under which TikTok might fit its activities if the images are classified as biometric data, and examining whether TikTok's data collection satisfies the proportionality requirement.

---

146 *See id.* ¶ 69.

147 *See id.* ¶ 78.

148 *TikTok's Lead EU Regulator Opens Two Data Privacy Probes*, REUTERS, (Sept. 15, 2021) (last visited Nov. 5, 2021), https://www.reuters.com/technology/ireland-regulator-opens-data-privacy-probes-into-tiktok-2021-09-14/ [hereinafter IDPC Probe].

149 *See id.*

150 *See id.*

151 *Id.*

152 *See EU Privacy Enforcement not Working, Says GDPR Architect*, IRISH TIMES (Nov. 18, 2021), https://perma.cc/K7MQ-R6Z4.

153 *See id.*

A. Are the "Faceprints" and "Voiceprints" that TikTok Is Collecting Special Category Biometric Data under GDPR?

Classification of the "faceprint" and "voiceprint" data will depend on how TikTok stores and analyzes it. This is because classification of special category biometric data under Article 9 turns on data processing. Article 4, describing the characteristics of the data itself, defines biometric data as "allow[ing] or confirm[ing] the unique identification of [a] natural person."[154] To fall within Article 9, such biometric data must be processed "for the purpose of uniquely identifying a natural person."[155]

The first question is whether TikTok stores the images and recordings with associated hash values. Although it declined to issue a pan-European order, HPG interpreted unique hash values as biometric data in its decision regarding Clearview's database.[156] HPG's decision, which is likely to be persuasive to other data protection authorities (DPAs), focused on the fact that this type of hash value is unique and "enables identification."[157] The same concerns would apply to any hash values used by TikTok because a hash value associated with a specific user is by definition unique.[158] Therefore, if TikTok's software stores the collected "faceprints" and "voiceprints" using associated hash values, those hash values would almost certainly be classified as biometric data. Because such hash values are specifically created to render users identifiable, the hash values themselves ought to fall squarely within Article 9.

The second question is whether TikTok stores the facial images and voice recordings in other ways that are easily searchable. These might include manually created tags such as "white" or "male." Manual tags would not necessarily be hashed because each individual tag does not contain sensitive information that needs to be protected. The inquiry is the same as the inquiry that led HPG to consider hash values biometric data. The more clearly the tags identify a specific person, the more clearly they fit within the language of GDPR Article 9. The number and specificity of the labels matter because an increase in either one is likely to increase the odds of identifying a given individual.[159] By way of illustration, if an image is labeled with 300 tags, it may be feasible to identify the data subject by running a sufficiently narrow search. Such identification would be possible even though no single tag or small number of tags would contain enough information to identify the subject of the photo. The dearth of regulatory

---

154 GDPR art. 4(14).

155 *Id.* art. 9(1).

156 *See* Section III.A.

157 HAMBURG DPA DECISION, *supra* note 91, at 3.

158 *See* INTRODUCTION TO THE HASH FUNCTION, *supra* note 95, at 7.

159 *See id.* at 14–15 (discussing how pseudoidentifiers may be at risk of re-identification).

decisions makes it difficult to pinpoint a specific standard for whether non-hash value labels incorporated into data processing would be considered Article 9 special category biometric data.

The third question is whether the facial images and voice recordings themselves would be considered special category biometric data, regardless of how they are stored. This is murkier than the inquiries regarding hash values and other storage parameters. The HPG order, which only required deletion of the hash value associated with Marx's photos,[160] suggests that facial images themselves are not necessarily special category biometric data in the eyes of DPAs. TikTok would likely advance this logic by arguing that, from a technical perspective, the images and recordings are not readily identifiable without further processing. This would probably be compelling because, unlike Clearview, TikTok's business model is not premised on identifying the subjects of photos. However, the vagueness of the purposes laid out in the Privacy Policy complicates third parties' ability to draw conclusions about the precise nature of TikTok's business model.[161]

B. What Is the Legal Basis for TikTok's Data Collection?

Regardless of whether the facial images and voice recordings it collects are special category biometric data under GDPR Article 9, TikTok must satisfy one of the legal bases enumerated in Article 6.[162] TikTok's privacy policy cites several legal bases for its collection and use of information. These are "contractual necessity, legitimate interests (ours, yours or those of another party), consent, compliance with a legal obligation, performing a task in the public interest, and protection of vital interests."[163] However, the privacy policy does not specifically state which basis TikTok is relying on to collect facial images and voice recordings.

TikTok might be using data subject consent as its legal basis for collection of facial images and voice recordings, given that users must accept TikTok's terms of use and privacy policy as a prerequisite to using the platform. However, this superficially plausible characterization of users' consent could be challenging to substantiate because E.U. regulatory authorities have closely scrutinized consent in recent cases involving facial images.[164] The Swedish school decision,[165] in particular, suggests general skepticism towards consent as a basis for processing sensitive data. Instead of taking nominal consent at face value, regulators seem to

---

160 *See* HAMBURG DPA DECISION, *supra* note 91, at 4.

161 *See* Section I.B.

162 *See* Dove & Chen, *supra* note 60, at 107–08.

163 Privacy Policy, *supra* note 32.

164 *See* Schwartz, *supra* note 134; *Sweden's First GDPR Fine*, *supra* note 131; Guidelines on Facial Recognition, *supra* note 74, at 9.

165 *Sweden's First GDPR Fine*, *supra* note 131.

be looking to the factors affecting the making of the agreement. This may be a problem for TikTok because anybody who wants to use the platform is forced to agree to the terms of use and privacy policy, rather than meaningfully opting in.

However, TikTok may be able to successfully argue consent as a legal basis for collecting facial images and voice recordings. Unlike the school in the Swedish DPA case, TikTok is a private entity. That mitigates concerns about coercion because, unlike a school or other public service, consumers are free to not use TikTok if they dislike its practices. Although "EU data protection law does not generally make a substantial distinction between personal data in a private space and in a public one,"[166] the ability to meaningfully opt out of private services like TikTok means that user consent is more robust than consent to data processing by monopolistic public services. Additionally, it is not clear that TikTok is collecting special category biometric data under GDPR Article 9. This contrasts with the Swedish school case because FRT clearly falls under Article 9. On balance, it seems likely that adequately informed consent would allow TikTok to carry out its data collection in compliance with recent interpretations of GDPR.

Even if TikTok was unable to successfully argue consent as a legal basis for collecting facial images and audio recordings, it could still use one of the other legal bases highlighted on its web page.[167] For example, providing enjoyable, interactive content is a legitimate interest of the company. So is content moderation. TikTok could justify data collection by demonstrating connections between the specific data collected and these interests.

C. Evaluating the GDPR Article 9(2) Permissions

The default under GDPR Article 9 is that collection and processing of special category data are not permitted. If regulators regard the facial images and audio recordings collected by TikTok as special category biometric data, the collection must fall within one or more of the enumerated Article 9(2) exceptions to be lawful. TikTok's activities are most likely to fit under either Article 9(2)(a) or Article 9(2)(e). Article 9(2)(a) allows processing where "the data subject has given explicit consent."[168] Article 9(2)(e) allows processing of the data where "processing relates to personal data which are manifestly made public by the data subject."[169]

166 Dove & Chen, *supra* note 60, at 108.

167 *See* Privacy Policy, *supra* note 32.

168 GDPR art. 9(2)(a).

169 *Id.* art. 9(2)(e).

1. Contrasting GDPR Articles 9(2)(a) and 9(2)(e)

Regulatory interpretation of the 9(2)(a) "explicit consent" exception is somewhat more developed than regulatory interpretation of the 9(2)(e) "manifestly made public by the data subject" exception.[170] The two exceptions differ in three important ways.

First, they have different downstream effects. The consent-based justification allows the data subject to withdraw their consent at any time, which allows restriction of downstream uses of their data.[171] In contrast, "if the data subject is deemed to have manifestly made their data public, they will not be able to restrict downstream uses of such data as one would by withdrawing their consent."[172] It is an open question whether removing the data from all public platforms would allow the data subject to curtail future use.[173]

Second, the exceptions differ in their interactions with the right to erasure. A data subject has the ability to pursue the right to erasure after withdrawing consent for the processing of their data.[174] It is more difficult for a data subject to access the right to erasure under the 9(2)(e) "manifestly made public" justification.[175] This is because such requests must pass a balancing test to be granted.[176] Additionally, data subjects may only make such requests under 9(2)(e) when the Article 6 bases are either public interest[177] or legitimate interests.[178]

Third, national governments have differing abilities to restrict the two justifications. Under 9(2)(a), national governments can prevent prohibitions on processing from being lifted based on explicit consent.[179] There is no comparable provision for 9(2)(e).[180] Article 9(4), which allows additional legislative restrictions on processing of biometric data, may or may not allow states to prohibit processing of "manifestly made public" data altogether.[181]

---

170 Dove & Chen, *supra* note 60, at 117 (explaining that 9(2)(e) "was perhaps one of the least discussed provisions in the course of legislating the GDPR."). *See also id.* at 108 ("There is little guidance from national data protection authorities (DPAs) or the European Data Protection Board (EDPB) on Article 9(2)(e); nor does there seem to be much precedent for its invocation.").

171 *See id.* at 112.

172 *Id.*

173 *See id.* at 112–13.

174 *See id.* at 113. *See also* GDPR art. 17.

175 Dove & Chen, *supra* note 60, at 113.

176 *See id.*

177 GDPR art. 6(1)(e).

178 *Id.* art. 6(1)(f). *See also* Dove & Chen, *supra* note 60, at 113.

179 GDPR art. 9(2)(a). *See also* Dove & Chen, *supra* note 60, at 113.

180 *See* Dove & Chen, *supra* note 60, at 113.

181 *Id.* at 113–14.

In summary, data controllers like TikTok may prefer to rely on the "manifestly made public" exception because it imposes a lower ongoing regulatory burden than the "explicit consent" exception. However, there is not yet a clear standard for determining when data has been "manifestly made public by the data subject."[182] The guidance issued to date is discussed below.

2. Defining "manifestly made public by the data subject"

Neither GDPR Article 9 nor the relevant recitals define "manifestly made public by the data subject." Therefore, defining the exception requires a two-step inquiry. First, what does it mean for the data to be "manifestly made public?" Second, what constitutes publicization "by the data subject?" Based on regulators' answers to these two questions, it is possible to piece together an idea of how this exception has been, and will be, interpreted.

One source of information is UKICO.[183] UKICO has interpreted "manifestly made public" as requiring a condition of accessibility by anyone.[184] According to UKICO's guidance, "[t]he question is not whether [the information] is theoretically in the public domain . . . The question is whether any hypothetical[ly] interested member of the public could access this information."[185]

UKICO has also written about how to consider the requirement that the information be publicized "by the data subject." According to its guidance, reliance on this justification requires confidence that the data subject's disclosure of the information "was unmistakably a deliberate act on their part."[186] The UKICO guidance includes a specific mention of social media posts, noting that:

> You might also find it hard to show that someone has manifestly made information public if, for example, they made a social media post for family and friends but default audience settings made this public. You should therefore be very cautious about using this condition to justify your use of special category data obtained from social media posts.[187]

---

182 *Id.* at 108.

183 The guidance discussed in this Section was written prior to Brexit. It should remain informative after Brexit, particularly because UK GDPR will remain part of UK law. *See Overview – Data Protection and the EU*, INFO. COMM'R'S OFF. (UK), https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/overview-data-protection-and-the-eu/ (last visited Mar. 20, 2022) ("The General Data Protection Regulation has been kept in UK law as the UK GDPR.").

184 Dove & Chen, *supra* note 60, at 117.

185 *What Are the conditions for Processing?*, INFO. COMM'R'S OFF. (UK), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/#conditions5 (last visited Nov. 7, 2021).

186 *Id.*

187 *Id.*

Overall, UKICO's guidance focuses on the key criteria of awareness and voluntariness.[188] As Dove and Chen note in their discussion of the UKICO guidance, "the data subject's misunderstanding of who would have actual access to their data may render the disclosure involuntary, and as a result, the processing invalid altogether."[189] Other legal scholars have reached the same conclusion, arguing that this standard "requires an affirmative act by the data subject."[190] This aligns with *The Handbook on European Data Protection Law*, which says that the permission "must be construed strictly and as requiring the data subject to deliberately make his or her personal data public."[191]

Scholars and authorities issuing guidance have converged on a narrow reading of the "manifestly made public" exception. "In practice, however, courts seem to have embraced broader interpretations than those of DPAs and legal commentators, thereby casting a wider scope."[192] According to the High Court of Justice for England and Wales, "the disclosure does not have to be an action directly triggering the dissemination of the sensitive data."[193] Although this opinion and others like it suggest that courts diverge from the scholarly consensus, the degree of divergence remains unclear.

Reconciling the narrow scholarly consensus and broader court decisions, Dove and Chen have proposed a legal test for GDPR Article 9(2)(e) that incorporates both data subjects' intent and their reasonable expectations.[194] Their test is neither a "standard of implied intention" nor an absolute standard of consent.[195] Instead, it occupies a middle ground through a three-step inquiry. First, it asks whether there is a close or attenuated connection between the data processing at issue and data allegedly manifestly made public by the data subject.[196] Steps two and three then consider whether the data was "manifestly made public" and whether it was publicized "by the data subject," respectively.[197]

---

188 *See* Dove & Chen, *supra* note 60, at 117 ("[T]he ICO has emphasized the importance of the awareness and voluntariness by the data subject.").

189 *Id.* at 117.

190 *Id.* at 118 (quoting and discussing the work of Ludmila Georgieva and Christopher Kuner).

191 EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, EUROPEAN COURT OF HUMAN RIGHTS, & EUROPEAN DATA PROTECTION SUPERVISOR, HANDBOOK ON EUROPEAN DATA PROTECTION LAW 162 (2018).

192 Dove & Chen, *supra* note 60, at 119.

193 *Id.* at 120 (discussing the High Court's opinion in *NT1 & NT2 v Google LLC* [2018] EWHC 799 (QB)).

194 *See id.* at 121.

195 *Id.* at 122.

196 *See id.*

197 *Id.*

Step one has a "relatively low threshold" and "would be met where a controller wished to process any special category of personal data concerning an individual, and that personal data emanates from the data subject themself."[198] As such, step one is unlikely to be a barrier for a data processor or controller wishing to pass the Dove and Chen test. Steps two and three are more difficult hurdles to overcome.

Step two begins by evaluating the data subject's intention. Did they mean to publicize the data? "What is required is objective evidence (eg [sic] a record of signature) of the explicit subjective intention (e.g. a statement of making the uploaded file accessible by anyone)" of the data subject.[199] For the "public" portion of the test, Dove and Chen adopt UKICO's stance, writing that "'public' must mean available to everyone."[200] They apply a pragmatic perspective, noting that "if a disproportionate, resource-intensive amount of effort is needed to access the data, it is less likely to be considered 'public.'"[201]

In step three, Dove and Chen consider whether the data was publicized by the data subject or another actor. For this portion of the test, they adopt a "literal interpretation of the phrase" by looking at whether the public nature of the data is a direct result of the data subject's actions.[202] In the case of data publicized via social media companies and other third-party intermediaries, "there would need to be a clear indication made by the data subject that they were relying upon the intermediary to make their data public."[203]

Dove and Chen's test fits with the limited guidance from regulatory authorities interpreting the "manifestly made public" exception under GDPR Article 9(2)(e). Because it also reconciles this guidance with scholarly consensus on the issue, the test has both predictive and normative value. Therefore, even though courts and regulatory authorities might interpret the provision differently if consumers bring complaints against TikTok, the test provides a useful framework for this Comment. Accordingly, Section V.C.3 applies the test to TikTok's new data collection practices, based on the possibility that the "faceprints" and "voiceprints" will be considered Article 9 special category biometric data.

198 *Id.* at 121.

199 *Id.* at 122.

200 *Id.*

201 *Id.*

202 *Id.*

203 *Id.*

3. Is the data collected by TikTok "manifestly made public by the data subject" under the Dove and Chen test?

This Section will apply the Dove and Chen test to TikTok's data collection practices. First, it will consider the connection between the data and its processing. Second, it will consider the "manifestly made public" prong. Finally, it will consider the "by the data subject" prong of the test. In summary, "faceprints" and "voiceprints" from certain kinds of TikTok accounts most likely fit under 9(2)(e). For other TikTok accounts, the answer is debatable.

TikTok's collection of "faceprints" and "voiceprints" most likely passes the first prong regarding the connection between the data and its processing. Assuming the information is only used for content moderation and technical features like filters, the link is direct. If TikTok processes the data to use it in other, less technical ways, the answer to this question becomes considerably more complex. Because TikTok's privacy policy is written to cover all of TikTok's data collection and discusses a wide range of uses for that data, it is not entirely clear how TikTok is using facial images and audio recordings.

The outcome of the second prong of the test depends on whether a TikTok user's profile is public or private. Public TikTok profiles are accessible to any TikTok user.[204] Private profiles are only accessible to approved followers.[205] Although any user may switch their account from a public account to a private account, the default setting is a public account.[206] The public/private setting provides the "objective evidence" required by the test.[207] The inquiry does not end there, however. We must consider three distinct groups of users: 1) public profile users regularly interacting with members of the public, 2) public profile users not regularly interacting with members of the public, and 3) private profile users.

Public profile users who are frequently interacting with new users, making efforts to gather new followers, and taking similar steps are clearly and consistently demonstrating their knowledge that their profiles are publicly accessible. We can thus infer that, by uploading content to a platform whose purpose is to publicize videos with the knowledge that their specific profiles are public, they intended to publicize their content. Because TikTok videos necessarily include facial images and audio recordings, "faceprints," "voiceprints," and other data extracted from those videos become fair game for data processing.

The behavior of public profile users not regularly interacting with members of the public does not provide the same support for the application of 9(2)(e). If

---

204 *See Controlling What People See on Your Profile*, TIKTOK (May 8, 2019), https://perma.cc/D8SN-ZBGP.

205 *See id.*

206 *See id.*

207 Dove & Chen, *supra* note 60, at 122.

users are only interacting with their known followers, they might not realize that their profiles are public due to TikTok's default settings. Although TikTok might argue constructive consent, based on the idea that users should have known their profile's settings and read the terms of use, constructive consent does not fulfill the standard of voluntary and informed consent. It would also be in tension with the specific reference to social media default settings in the UKICO guidance, which casts doubt on the idea that posts made public by default settings should be used as evidence of the posts being manifestly made public.[208] Therefore, these users' "faceprints" and "voiceprints" should not be considered "manifestly made public" under 9(2)(e). In practice, these users may be difficult to distinguish from users with public profiles who regularly interact with the general public. How much interaction with people who are not one's known followers is enough to put a TikTok user "on notice" that their profile is public? How much interaction is enough to allow regulators and data processors and controllers to reasonably infer the data subject's intentions? This would be much clearer if the default profile setting was private.

The final group of users to consider is those with private profiles. These individuals should not satisfy the "manifestly made public" inquiry for two reasons. First, they have taken the affirmative step of switching their profiles from public to private. This suggests that they deliberately avoided making their information publicly accessible. Although TikTok could argue constructive consent based on its privacy policy, as discussed above, this is not a realistic conception of how consumers make decisions.[209] Second, the information from private profiles is not accessible to the public. Neither the fact that TikTok has access to the information from the back end nor the fact that a technologically savvy person might find a way around privacy settings changes this determination. Those are not average members of the public and finding ways around profiles' privacy settings is clearly a "disproportionate, resource-intensive amount of effort."[210]

This three-part categorization is somewhat complicated by the idea of making public posts private after the fact. Users who undertake after-the-fact privatization could fall within any of the three groups described above. There is a colorable argument that after-the-fact privatization should be treated like initial privatization because privatizing is an affirmative step, regardless of when it is done. In practice, a thorough inquiry in these cases might turn on indicia of a TikTok user's sophistication. If a user seems active and sophisticated, as evidenced by regular public engagement with other users, the initial public setting ought to be taken at face value. That reduces the weight of after-the-fact

---

208 *See* Section V.C.2.

209 *See* Section V.C.4 for more discussion of robust consumer consent.

210 Dove & Chen, *supra* note 60, at 122.

privatization decisions. Conversely, if a user appears unsophisticated, that lends weight to the proposition that their initial public settings might have been inadvertent. That, in turn, undermines the idea that they ought to satisfy the "manifestly made public" inquiry.

In summary, TikTok can only make a compelling case that its collection of "faceprints" and "voiceprints" is permissible under 9(2)(e) for certain kinds of user profiles. Because it is likely not feasible for TikTok to consistently disaggregate different types of users, 9(2)(e) is not a strong legal argument on which to base the entire data collection regime. Although TikTok could, and likely would, argue constructive consent, available regulatory guidance suggests that constructive consent arguments would not succeed. Moreover, as discussed in Section VI, such arguments should not succeed as a normative matter. Nonetheless, even if TikTok fails to satisfy the requirements of 9(2)(e), collection of special category biometric data may still be justified under 9(2)(a).[211]

4. Have TikTok users explicitly consented to processing of their data?

Whether TikTok's collection of "faceprints" and "voiceprints" is permitted under GDPR 9(2)(a) will depend on the robustness of data subjects' consent. In the digital age, privacy laws are struggling to keep pace with rapidly shifting data collection norms. This is because "[b]asic principles of information privacy developed in an age where technology and data simply did not exist in the way they do now."[212] As a result, even advanced legal regimes like GDPR are largely silent on algorithmic products and other technological innovations with major implications for consumer privacy.[213] This Section begins with a normative discussion of consent in the age of Big Data and concludes with a discussion of user consent to TikTok's data collection under GDPR Article 9(2)(a).

In the U.S., conceptions of privacy rely at least partially on individuals' "reasonable expectations."[214] Although "an individual's subjective expectation of privacy is fluid and case-specific,"[215] subjective expectations of privacy must be objectively reasonable to be protected.[216] Different circumstances give rise to

---

211 *See* Section V.C.4.

212 Matt Bartlett, *Beyond Privacy: Protecting Data Interests in the Age of Artificial Intelligence*, 3 LAW, TECH. & HUM. 96, 100 (2021).

213 *Id.*

214 Smriti Krishnan, *Tiger by the Tail: Navigating Modern Technologies and Privacy Interests*, 42 LAW & PSYCHOL. REV. 103, 104 (2017-2018). This is mostly true of U.S. Fourth Amendment protections. But note that Congress can (and has) passed privacy laws that go above and beyond what the Fourth Amendment requires and do not turn on reasonable expectations of privacy. *See* the Privacy Act of 1974, Electronic Communications Protection Act of 1986, Health Insurance Portability and Accountability Act of 1996.

215 *Id.* at 107.

216 *See id.* at 104.

different reasonable expectations of privacy.[217] Although GDPR and other international privacy regimes afford consumers more protection than U.S. privacy laws do, European privacy doctrines also incorporate the concept of reasonable expectations of privacy.[218] The difference lies in which circumstances are considered to give rise to those reasonable expectations.[219]

Things become more complicated in the digital space for three reasons. First, there is a major information and literacy gap between data subjects and processors.[220] Additionally, the legal language used in agreements such as terms of use and privacy policies is not readily comprehensible to most non-lawyers.[221] When this fact is considered in conjunction with users' unsophisticated understandings of the technical parameters of the services they use, it is unsurprising that one recent study found that "approximately 52% of users believe that a privacy policy ensures complete confidentiality of online information."[222] Even if some users are genuinely informed and have their eyes wide open when interacting with digital service providers, it is not safe to assume most users are so well informed.

Second, modern technologies can be accessed from anywhere, blurring the lines between public and private spaces and content.[223] For example, anybody with a smartphone can access TikTok. The same is true of other apps and websites, from Instagram to Google. Therefore, a user's physical location is no longer critically important in determining reasonable expectations of privacy. A user is likely to have the same privacy expectations whether they open an app at work, at home, or elsewhere.

Third, many apps and social media platforms force agreement to their terms of use to create a profile.[224] This requirement calls into question the voluntariness of consent to those terms of use. Consumers are theoretically free to simply not make profiles or use platforms. However, there are few meaningful alternatives to some of these services. For example, while a consumer may opt out of a specific email service provider, opting out of email altogether is unrealistic. Social media

---

217 *See id.*

218 *See, e.g.*, Ronald J. Krotoszynski Jr., *Reconciling Privacy and Speech in the Era of Big Data: A Comparative Legal Analysis*, 56 WM. & MARY L. REV. 1279, 1298 (2015) ("In the jurisprudence of the ECHR and many signatory states, a reasonable expectation of privacy can arise while a person is in public.").

219 *See id.* at 1298–02.

220 *See* Bartlett, *supra* note 212, at 104 ("There is a huge information asymmetry incumbent in the data economy that makes genuine consent extremely difficult to determine.").

221 *See generally* Michael Masson & Mary Anne Waldron, *Comprehension of Legal Contracts by Non-experts: Effectiveness of Plain Language Redrafting*, 8 APPLIED COGNITIVE PSYCH. 67 (1994) (assessing comprehension of contracts and finding overall low comprehension, even with simplified drafting).

222 Krishnan, *supra* note 214, at 111.

223 *See id.* at 106.

224 *See id.* at 111–12.

is more complex because it is less professionally essential than email. Nonetheless, opting out of all social media can lead to harms such as reduced social connections and increased difficulty developing professional networks. As things stand, opting out is the only alternative to accepting companies' invasive terms of service.

How, then, should GDPR regard TikTok users who "consent" to collection of their "faceprints" and "voiceprints?" This turns on users' ability to opt out of data processing at least as much as it turns on their opting in by consenting to TikTok's privacy policy. GDPR requires that data subjects must be able to withdraw their consent at any time. If users' ability to withdraw their consent includes the ability to stop collection and storage of their "faceprints" and "voiceprints" moving forward, this will likely pass muster. Because social media is not an essential service, regulators are unlikely to be concerned that users must agree to TikTok's terms of use to make a profile. If, however, withdrawing consent does not allow users to prospectively opt out of further data collection, users' consent may be legally inadequate. The fact that facial images and audio recordings are listed as data that TikTok collects automatically suggests that it may be difficult to prospectively opt out of their collection, even if users can request that TikTok delete images and recordings it has already collected. That, in turn, calls into question whether they are truly able to withdraw their consent, even if the original consent was adequate.

D. Does TikTok's Data Collection Meet the Proportionality Test?

Assuming regulators considered the consent obtained by TikTok adequate, the final question is whether TikTok's data collection would pass the proportionality inquiries built into GDPR.[225] In the European rights framework, proportionality is a balancing tool used to reconcile competing rights or interests.[226] Proportionality, as a general tool, relies on three subtests: suitability, which examines instrumental rationality; necessity, which examines infringement of the "essence" of the right; and proportionality *stricto sensu*, which looks to overall balancing of the costs and benefits.[227]

In the wake of recent regulatory guidance and Court of Justice of the European Union (CJEU) decisions, proportionality inquiries are now firmly embedded in GDPR interpretation.[228] However, "the exact understanding of proportionality in data protection law remains uncharted . . . [and] nobody knows

---

225 *See* Darius Kloza & Laura Dreschler, *Proportionality Has Come to the GDPR*, EUR. L. BLOG (Dec. 9, 2020), https://perma.cc/F9LS-VQ86.

226 *See id.*

227 *See* AHARON BARAK, PROPORTIONALITY: CONSTITUTIONAL RIGHTS AND THEIR LIMITATIONS 3 (2012).

228 *See* Kloza & Dreschler, *supra* note 225.

exactly how to assess proportionality in the context of personal data protection."[229] In the absence of a data protection-specific conception of proportionality, this Section considers whether TikTok's practices are likely to pass a general proportionality inquiry.

Whether TikTok's activities are proportional depends on technical specifications. Could TikTok offer the filters and other features that are a signature component of its platform without collecting "faceprints" and "voiceprints?" How closely the data is tied to the services offered determines whether the data collection passes the suitability subtest. If the data is not clearly necessary to offer TikTok's services, TikTok's data collection is likely to fail the suitability inquiry. Failing to employ the least restrictive means available could also prevent TikTok from passing the necessity subtest. If TikTok could not provide these features without the data collection at issue, and if TikTok can demonstrate that it is only collecting the data necessary to fulfill these technical requirements, its data collection practices would pass the suitability and necessity inquiries.

If a complaint turns on a proportionality *stricto sensu* inquiry, things may become more difficult for TikTok. Fun social media filters do not necessarily provide substantial societal value, regardless of how much users enjoy them. That is fine if courts and regulators do not perceive TikTok as infringing on major rights. However, social media filters are not a sufficiently important interest to clearly outweigh substantial limitations on fundamental rights. In short, whether TikTok passes this step of the proportionality test hinges on whether its data collection practices are meaningfully infringing on rights.

VI. TIKTOK AS A CASE STUDY: A FRAMEWORK FOR REGULATION OF FACIAL IMAGES

While Section V is descriptive, applying recent interpretations of GDPR to TikTok's practices, this Section is prescriptive. Specifically, it will argue that GDPR and ICCPR should both be updated to respond more effectively to cases like Clearview and TikTok. These cases will only increase in number and importance based on technological developments like mass-scale FRT-based payment systems,[230] use of FRT by major airlines,[231] and the introduction of

---

229 *Id.*

230 *See* Pjotr Sauer, *Privacy Fears as Moscow Metro Rolls out Facial Recognition Pay System*, GUARDIAN (Oct. 15, 2021) https://perma.cc/H84L-3YFX.

231 *See, e.g.*, *Could Facial Recognition Be the Future of Airport Security? Delta Air Lines Is Testing It out*, CBS NEWS (Oct. 27, 2021), https://perma.cc/F6BD-6HXA; *FACES - Fast Airport Clearance Experience System*, AIRASIA, https://perma.cc/3ZF4-BRBF.

cameras that use FRT to automatically snap and frame shots of your loved ones using built-in "subject recognition."[232]

A. Updating Interpretations of GDPR

This Section argues that regulators should implement four changes to GDPR interpretation: treating all facial images as special category biometric data under GDPR Article 9, codifying consent standards, clarifying the proportionality inquiry for data processing, and prohibiting photo scraping as a general practice.

1. Treating all facial images as special category biometric data under GDPR Article 9

Regulators should consider all facial images, even those that have only been processed to the degree necessary for collection, to be special category biometric data under GDPR Article 9. This would be a more manageable standard because the boundary between "processed" and "unprocessed" images grows increasingly fuzzy with data collection by entities like TikTok. A bright-line rule for all entities collecting and retaining facial images would better keep pace with technological developments. Limiting this to entities that retain facial images would avoid over-inclusion of entities such as traffic camera operators.

Treating all facial images as biometric data would also accord with the plain meaning of "uniquely identifying a natural person."[233] Because facial images are representations of unique individuals, looking at a picture allows you to identify the person depicted. Attaching a sufficient number of non-hash value labels might also allow a user to "triangulate" a person, making them functionally identifiable with a sufficiently narrow search. In short, a "person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers."[234] The link to identification of a natural person is intuitive.

Processing for identification of a natural person is the standard for inclusion under GDPR Article 9. Data processors and controllers with non-pretextual business reasons for retaining facial images should have the burden of proof to demonstrate that their practices do not implicate identifiability concerns through manually viewing images or "triangulation"-style identification. Some data processors and controllers might argue that the facial images they collect should not be considered special category biometric data because photos are not

---

232 James Vincent, *Canon's PowerShot PX Is a Home Surveillance Camera for Happy Memories*, VERGE (Oct. 29, 2021), https://perma.cc/N5DD-3KR8.

233 GDPR, *supra* note 51, art. 9(1).

234 *Von Hannover v. Germany (No. 2)*, Case nos. 40660/08 and 60641/08, ¶ 96 (Feb. 7, 2012) https://perma.cc/HX4S-6JFW.

inherently biometric data.[235] However, cases where this argument is strong are likely an extremely small portion of processors, assuming they exist. Therefore, it would be better to treat all facial images as special category biometric data. Regulators could allow an appeal process for processors to argue that their data does not raise identifiability concerns. However, such an appeals scheme is likely to raise manageability issues for regulators.

Certain private entities would not be affected by these new limitations. Due to the so-called household exemption, GDPR does not apply to processing of personal data "by a natural person in the course of a purely personal or household activity."[236] This provision is construed extremely narrowly. Home security cameras and other privately operated video surveillance technology are not exempt if their coverage area includes any public spaces.[237] However, any commercial entity running video surveillance on its premises would need to pass the inquiries discussed in Section V. Therefore, small stores might find it advantageous to hire external security companies to collect and store surveillance footage. Larger commercial entities whose primary activity is video surveillance should be well equipped to manage GDPR regulatory burdens.

Although this framework would limit most private entities' ability to collect and process facial images, it would not prevent government entities like police from doing so. This is because GDPR Articles 6 and 9 contain explicit carve-outs for government activities. Article 6 creates a legal basis for processing data where "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller."[238] Although the "public interest" basis requires the processing to be done according to either E.U. law or member state law,[239] each member state is fully entitled to pass laws authorizing its police force to store and analyze facial images. Article 10, which requires processing of personal data related to criminal convictions, offenses, or related security measures to be carried out by official authorities, further supports this.[240] Therefore, police processing of facial images to address criminal activity fulfills the required legal bases for data processing.

Processing by police for purposes of crime prevention, investigation, and prosecution further fulfills the requirements for processing special category data. Article 9 permits processing of biometric data where "processing is necessary for

---

235 *See* Stupp, *supra* note 85 (citing a commentator as saying "a person's photo isn't automatically considered biometric").

236 GDPR, *supra* note 51, art. 2(2)(c).

237 *See Guidelines 3/2019 on Processing of Personal Data through Video Devices*, EUR. DATA PROT. BD. (adopted Jul. 10, 2019) 6, https://perma.cc/N4FF-HQFJ.

238 GDPR art. 6(1)(e).

239 *Id.* art. 6(3).

240 *See id.* art. 10.

reasons of substantial public interest."[241] Processing under the Article 9 "public interest" permission must provide safeguards and be both proportional and lawful.[242] However, a narrowly circumscribed use carried out with strong safeguards by police seems likely, on face, to pass a proportionality inquiry.

A shift to treating all facial images as special category biometric data governed by GDPR Article 9 may be challenging to administer. However, companies doing business in the E.U. already must demonstrate GDPR compliance. Therefore, providing additional explanation of Article 9 permission for their activities does not create a substantial new regulatory compliance burden. It simply requires them to include additional information in disclosures.

Retroactivity is a bigger potential problem than administrability. However, this proposal could be phased in, with penalties only applying to conduct carried out after the new rules are in force. That would give data processors and controllers an opportunity to adjust their business practices in the E.U. member states are well within their rights to change laws to protect consumers and address other compelling societal interests.

2. Codifying consent standards

Regulators should codify standards for consent obtained by private actors. When evaluating the adequacy of consent, entities like TikTok raise a different set of concerns than public entities like school boards. Clarifying these standards is increasingly important with the rise of "data harvesters" whose business models are based on monetizing data.[243] Because consumers may not be fully aware of the economic value of the data they are signing away and it is not in data harvesters' interest to make them aware of that value, regulators should promulgate robust, ongoing consent requirements. Clarifying consent standards would enhance both enforcement and voluntary compliance efforts. It may also raise public awareness of the issue, which would allow data subjects to make more informed decisions.

3. Clarifying the proportionality inquiry

Regulators should promulgate guidance on applying the least restrictive means subtest of the proportionality test to entities such as TikTok, whose choice of methods for processing data is constrained by technical requirements.[244] This would allow private data processors and controllers to proactively comply with GDPR, rather than reacting when their policies are found to be impermissible. It would also facilitate uniform application of the proportionality test by regulators.

---

241 *Id.* art. 9(2)(g).

242 *See id.*

243 For discussion of the concept of "data harvesters," see Bartlett, *supra* note 212, at 98.

244 For discussion of the current ambiguities, see Section V.D.

Without clear guidance, there is a serious risk that different regulators will develop and apply different versions of the least restrictive means subtest.[245]

4. Prohibiting photo scraping

Regulators should prohibit photo scraping as a general practice, rather than relying on individual data subjects to bring regulatory complaints requesting that companies delete their scraped data. Although it is nominally public, the information scraped by Clearview and similar companies generates privacy interests that should be protected.[246] Collecting and processing facial images in this way entails: 1) a loss of anonymity, even if such loss is incremental; 2) infringement on both control[247] and economic[248] interests; 3) loss of "protection of personality;"[249] and 4) damage to the "fundamental human values of dignity and autonomy."[250] Exploiting this kind of data also harms a social interest. "[T]hinking about data rights solely from the individual's perspective, as through the lens of privacy, fundamentally misunderstands how data is now used in the data economy."[251] Illustratively, "data harvesters" use algorithms to gather data on individuals who have not provided them with any data, based on predictions generated from information provided by their friends and family.[252] Similarly, the racial disparities in false positives in FRT speak to broader societal interests stemming from processing of individuals' data.[253] In these ways, and a myriad of others, what happens to an individual's data has broad ripple effects, creating a societal interest in regulation.

Photo scraping also creates incentive problems for individuals whose photos might be scraped by services like Clearview. To reduce the risk of photos being caught in Clearview's scraping, individuals might wish to minimize the number of their photos available on the internet. That, in turn, could result in damage to networks with weak ties. For example, if individuals choose to not allow their employers to publish headshots, that makes identification of unknown individuals in the office more difficult. Similarly, a heightened risk of identification relative to

---

245 *See* Barak, *supra* note 227, at 3 (discussing the basic proportionality test, including the least restrictive means subtest).

246 *See* Geoffrey Xiao, *Bad Bots: Regulating the Scraping of Public Personal Information*, 34 HARV. J.L. & TECH. 701, 717–18 (2021).

247 *See* Bartlett, *supra* note 212, at 102.

248 *See id.* at 103.

249 Eugenia Georgiades, *A Right That Should've Been: Protection of Personal Images on the Internet*, 61 IDEA 275, 304 (2021).

250 *Id.* at 305–06.

251 Bartlett, *supra* note 212, at 101.

252 *Id.* at 98.

253 *See* Drew Harwell, *Federal Study Confirms Racial Bias of Many Facial-recognition Systems, Casts Doubt on Their Expanding Use*, WASH. POST (Dec. 19, 2019), https://perma.cc/4SQM-DT2Q.

manual identification of photos reduces individuals' incentives to engage in controversial activities like attending political protests or unionizing.[254] A defined privacy interest in facial images protects these kinds of networks and behaviors.

If they are concerned about foreclosing public benefits, rather than banning all photo scraping, legislators could draft legislation to cover photo scraping that is structured similarly to GDPR Article 9. As discussed in Section II.B.1, beginning with a prohibition on processing and carving out narrow exceptions leads to tighter regulation of data processing than alternative frameworks. A law like GDPR Article 9 could allow photo scraping for purposes like academic research while prohibiting monetization of unsuspecting individuals' online activities.

B. Updating ICCPR

Because ICCPR has 173 parties,[255] it has the potential for a far broader impact than GDPR. However, this must be balanced against the fact that ICCPR cannot, by its nature, be nearly as specific as GDPR. On balance, several critical updates would markedly increase its utility, even though they would not be as specific as GDPR or national legislation. Given the difficulty of building consensus among 173 States Parties, having the U.N. Human Rights Committee release new interpretive comments is likely to be a more productive path forward than updating the text of ICCPR itself. The Human Rights Committee would be particularly well served by releasing three new comments.

First, it should interpret ICCPR Article 17 as requiring robust consent for digital data collection generally and facial image collection specifically. Specific interpretive language about consent and other high-level principles would be useful for countries looking to enhance their privacy regimes.

Second, it should release a comment codifying heightened protection for minors' data in the specific context of facial images. As GDPR and other privacy regimes recognize, minors are a more vulnerable population than adults. They also have a reduced capacity for consent, which heightens their vulnerability.

Third, it should release a comment codifying the expectation of "privacy in public."[256] Shifting the burden to companies to demonstrate waiver of a presumption of privacy, rather than putting the burden on consumers to show

---

254 *See* Amory Starr, Luis A. Fernandez, Randall Amster, Lesley J. Wood & Manuel J. Caro, *The Impacts of State Surveillance on Political Assembly and Association: A Socio-Legal Analysis*, 31 QUAL. SOCIO. 251, 258 (2008) ("Recent publicity of massive surveillance databases, along with codes and tags such as "criminal extremist" and "domestic terrorist," have created widespread fear to participate in completely legal political events.").

255 *International Covenant on Civil and Political Rights*, U.N. TREATY COLLECTION, https://perma.cc/4GAT-VG4C.

256 Xiao, *supra* note 246, at 702.

that they have created a special privacy interest, would substantially increase the efficacy of a privacy regime based on ICCPR.

VII. CONCLUSION: LOOKING BEYOND THE E.U.

Updating GDPR and providing additional interpretive guidance of ICCPR would be tremendously beneficial for protecting ordinary individuals' privacy rights. The status quo is, at best, one of uneven digital privacy rights. Current models of consent are undermined by a widening expertise gap that "is eroding the very idea of autonomy as a pillar of the data protection framework."[257] The problem is compounded by rapid technological developments, which are swiftly outpacing regulations designed to constrain them. Individual consumers lack power to address the situation. Therefore, having comprehensive regulatory schemes that adequately address these challenges is critical.

Regulations like GDPR and ICCPR will only become more important considering technological developments like those discussed in Section VI. Given the importance of both individual privacy interests and the broader societal concerns affected by the rise of FRT and facial image collection, the time to update GDPR and ICCPR is now, while there is still time for regulations to shape technological developments. Delaying necessary updates increases the odds that technological innovations will constrain regulatory developments, rather than the inverse.

---

[257] Emile Antoine Ennosuke Douilhet, The Information / Guarantees Balance - Protecting Informational Privacy Interests within the European Data Protection Framework 124 (Doctoral thesis, Bournemouth University, 2019), https://perma.cc/N46N-HBW3.