Virtual Reality, Augmented Reality & Biometric Data after 2017

--Edward Klaris & Alexia Bedat

I. Introduction

A particular type of private information became the focus of increasing attention in 2017: biometric data.[1] In May, Washington became the third state to enact a biometric privacy statute (following Illinois in 2008 and Texas in 2009[2]) while seven other states have similar bills pending[3]. Across the pond, European companies have started preparing for the new data protection regime coming into force in May 2018, the General Data Protection Regulation.[4] A number of non-EU countries have also furthered the trend, enacting biometric privacy laws or issuing updates on the collection of biometric data.[5] These legislative efforts have coincided with significant improvements in two distinct but related technologies: augmented[6] and virtual reality.[7] Augmented reality ("AR") overlays

---

[1] The term biometric data usually refers to digital data obtained by measuring an individual's characteristics, such as retina or iris scans, fingerprints, voiceprints or hand and face geometry. *See infra* note 25.

[2] The Illinois and Texas statutes were passed before the advent of AR or VR yet as part of the government's early effort to regulate biometric data collection. *See infra* note 38. Washington becoming the third state to enact such a statue is a key development as it is the home to a number of companies heavily involved in AR, including Amazon and Microsoft.

[3] *See infra* note 23.

[4] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*, O.J. 2016 (L 119), available at: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679 (hereinafter referred to as the "GDPR").

[5] *See* infra note 53.

[6] Some notable developments in the AR space in 2017 included Apple's release of ARKit, a software development kit for developers to make augmented reality applications for the iPhone and iPad, as well as Magic Leap's much awaited unveiling of its AR goggles after about 7 years of secrecy. Pokémon Go, launched in the summer of 2016, remained popular with consumers – and litigants in 2017. A class action was filed against Pokémon Go on grounds of nuisance and unjust enrichment, raising issues of virtual trespass, which are beyond the scope of this paper. *See* Jeffrey Marder, Individually and on Behalf of All Others Similarly Situated, Plaintiff(s), v. Niantic, Inc., The Pokemon Company, and Nintendo Co. Ltd., Defendants, 2016 WL 4073537 (N.D.Cal.).

[7] The extent to which 2017 was a big year for VR is debatable. VR remained associated with expensive headsets, tangled wires, pixelate images and disappointing content. In contrast, 2018 is already well positioned to be the year when the industry addresses at least two of VR's barriers to entry: the hardware and price point. Lenovo, HTC and Facebook-owned Oculus are all due to launch wireless VR headsets, and leading VR developers, such as Google, are now marketing headsets for under $100 (contrast this with the HTC Vive – $800 – or the Oculus Rift – $500). For an overview of developments in 2017, *see e.g.* Ramón Bretón, *M&E Journal: 2017: The Year of Quality VR*, MEDIA & ENTERTAINMENT SERVICES ALLIANCE (Jun. 8, 2017), http://www.mesalliance.org/2017/06/08/journal-2017-year-quality-vr/, *versus* Sherri L. Smith, *Has Time Run Out for Virtual Reality?*, TOM'S GUIDE (Oct. 11, 2017, 4:00 AM), https://www.tomsguide.com/us/state-of-virtual-reality,review-4735.html.

digital data over the real world, while virtual reality ("VR") is a fully immersive artificial environment, experienced through sensory stimuli in a headset.[8] Both AR and VR have the ability to collect significant amounts of biometric data. These technologies, once considered remote, are becoming increasingly common aspects of the consumer experience, scanning not just inanimate surroundings but human eyes and faces as they do so. Individuals in 2018 will unlock smartphones with a mere glance, visualize virtual new furniture in their homes, experience the Winter Olympics without leaving their desks and find VR experiences at every major film festival. The relevant question is not whether a consumer will be exposed to AR or VR, but when.[9] VR and AR thus offer a helpful and relevant prism through which to consider the potential of biometric data, how it is regulated, and what this means for companies in these areas[10].

II. VR/AR & Biometric Data

While these technologies could eventually track a range of biometric data, two particular functions of VR and AR will feature prominently in 2018: eye-tracking and facial recognition.

A) VR & Eye-Tracking

Until now, VR has functioned by a combination of sensors that track a user's head, body and hand movement.[11] As of January 2018, eye-tracking technology can be

---

[8] Readers wishing to try a VR experience may enjoy some of the following news stories in VR. *See e.g.* The Guardian's 'The Party – A virtual experience of autism', in which users experience a surprise birthday party through the eyes of a 15-year old autistic girl (*Guardian launches The Party - A virtual experience of autism*, THE GUARDIAN (Oct. 9, 2017, 4:43 AM), https://www.theguardian.com/gnm-press-office/2017/oct/09/guardian-launches-the-party-a-virtual-experience-of-autism) or Google and the Guardian's VR experience of solitary confinement (*Could this solitary confinement VR experience sway lawmakers?*, FAST COMPANY (Aug. 31, 2017), https://www.fastcompany.com/video/could-this-solitary-confinement-vr-experience-sway-lawmakers/gXHp82fG).

[9] *See e.g.* NBC's announcement that over 50 hours of live VR coverage of the Winter Olympics will be available as a result of its partnership with Intel True VR. *Experience the 2018 Winter Olympics in virtual reality*, NBCU (Jan. 22, 2018 at 6:00 AM), http://www.nbcolympics.com/news/experience-2018-winter-olympics-virtual-reality. *See also* Matt Adcock, *Augmented reality: Why 2018 might be the year AR tech goes mainstream*, ABC NEWS (Jan. 11, 2018, 8:56 PM), http://www.abc.net.au/news/2018-01-12/augmented-reality-why-2018-might-be-year-ar-goes-mainstream/9321472.

[10] "Companies" may refer to product developers, as well as companies that commission, license, distribute, display, and host AR and VR content.

[11] This is done with a system known as 6DoF (six degrees of freedom), which plots one's head in terms of the X, Y and Z axis to track and measure one's head movements. The plotting is made possible by internal components, such as a gyroscope, accelerometer and magnetometer. For further detailed information on how VR works, *see* Sophie Charara, *Explained: How does VR actually work?*, WEARABLE (Dec. 26, 2017), https://www.wareable.com/vr/how-does-vr-work-explained/.

added to this list.[12] VR and tech aficionados have already rejoiced at the prospect of increased "foveated rendering" and avatars that can mirror real time blinking.[13] Adding eye-tracking to VR headsets, however, offers more than an improved visual experience. It grants VR companies the tools to track where users look, what grabs their attention, for how long and how it makes users feel.[14] Combining eye-tracking with tools that can detect a user's emotional state by reading facial muscle movement or pupil dilation[15] potentially converts every individual donning a headset in the privacy of his or her own home into an instant consumer study.

B) AR & Facial Recognition

When combined with facial recognition, the potential of AR is equally impressive. Consider augmented glasses capable of gathering and displaying the social media profile of any person coming in one's range of vision, or billboards advertising services tailored to a consumer's purchasing history. While these scenarios may seem far-fetched, AR is already leveraging facial recognition to unlock or adjust the volume of smartphones (iPhoneX) and identify an individual's painting look-alike (Google's Arts & Culture App). These applications, and others like them, analyze a series of invisible dots (30,000 in the iPhone X's case) and create a unique and precise depth map of one's face, which can then be compared to a database of stored images.[16]

---

[12] Tobii, an eye-tracking company, released a VR development kit for eye tracking to be fitted with the HTC Vive (one of the main VR headsets), which was received with enthusiasm at the January 2018 Consumer Electronics Show in Las Vegas, Nevada. Eye tracking is accomplished by projectors that create a pattern of near-infrared light on a user's eyes. Sensors take high-frame-rate images of both those patterns and the user's eyes. Those patterns are then fed through image processing algorithms that find specific details in the patterns and use these to calculate the eyes' position and gaze point. *See* the website of Tobii Tech, available at: https://www.tobii.com/tech/technology/what-is-eye-tracking/.

[13] *See e.g.* Devindra Hardawar, *Tobii proves that eye tracking is VR's next killer feature*, ENGADGET (Jan. 13, 2018), https://www.engadget.com/2018/01/13/tobii-vr-eye-tracking/.

[14] While eye-tracking heat maps and ad-tracking technology already exist, these are largely based on an individual's clicking habits and browsing behavior. *See e.g.* Jaime Yap, *What are Web Heatmaps, Really?*, FOREWARD (Mar. 28, 2017), https://blog.fullstory.com/what-are-web-heatmaps-how-do-they-work-pros-cons-alternatives/. Eye-tracking technology, moreover, is not yet an integral component of computers in the same way that eye-tracking is set to become part of VR headsets. *See e.g.* Janus Kopfstein, *The Dark Side of VR*, THE INTERCEPT (Dec. 23, 2016, 9:12 AM), https://theintercept.com/2016/12/23/virtual-reality-allows-the-most-detailed-intimate-digital-surveillance-yet/) ("The information that current marketers can use in order to generate targeted advertising is limited to the input devices that we use: keyboard, mouse, touch screen. VR analytics offers a way to capture much more information about the interests and habits of users, information that may reveal a great deal more about what is going on in [their] minds.")

[15] *See e.g.* Dean Takahashi, *MindMaze reveals Mask to capture your facial expression in virtual reality*, VENTURE BEAT (April 12, 2017, 9:00 AM), https://venturebeat.com/2017/04/12/mindmaze-reveals-mask-to-capture-your-facial-expression-in-virtual-reality/).

[16] For more detailed information on how facial recognition works, *see* https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition1.htm.

While these innovations are exciting, individuals embracing VR and AR as a source of entertainment may be entirely unaware of the breadth of data simultaneously being collected and stored about them. Understanding the biometric data regulation framework is necessary for both the responsible enjoyment and development of AR and VR.

III. Biometric Data Collection Regulation in the US and the EU

A) Laws in the US

Privacy in the United States has historically been associated with the four torts identified by Warren and Brandeis in 1890.[17] Since then, only a narrow group of federal statutes have been enacted to protect certain sensitive data from being inappropriately gathered or disclosed.[18] Some industries have also engaged in a certain amount of self-regulation to avoid legislation being imposed on them.[19] The regulation of biometric data collection has only recently become the subject of state law. At a federal level, Congress has avoided the issue.[20] Only three states[21], Illinois, Texas and Washington, have enacted

---

[17] *See* Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV. L. REV. 193 (1890) and William L. Prosser, Privacy, 48 CALIF. L. REV. 383, 388-89 (1960).

[18] *See e.g.* the Fair Credit Reporting Act 1970 (consumer information); the Telephone Communications Privacy Act 1996 (information obtained by telemarketers); the Children's Online Privacy protection Act 19998 (information on children under 13 years of age) and the Health Insurance Portability and Accountability Act 2000 (health and medical records).

[19] The video game industry, for example, formed the Entertainment Software Rating Board (ESRB) in 1994 and is responsible for, among other things, attributing ratings to video games across the US. In 1971, the Better Business Bureau formed the National Advertising Division to self-regulate advertising standards and apply FTC guidelines. One may expect to see similar bodies form as the AR and VR industries continue to expand, particularly in light of the attention facial recognition has already received at the federal level. *See infra* note 20. For a review of self-regulation efforts, *see* Robert Gellman and Pam Dixon, *Many Failures: A Brief History of Privacy Self-Regulation in the United States*, WORLD PRIVACY FORUM (Oct. 14, 2011), http://www.worldprivacyforum.org/wp-content/uploads/2011/10/WPFselfregulationhistory.pdf.

[20] While no legislation has been enacted, concern over the collection of biometric data has been expressed at the Federal level. In 2012, the FTC released its report "Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies," advocating for clear disclosures by social media networks using facial recognition features and the ability for consumers to opt-out easily from such collection. (*Best practices for common uses of facial recognition technologies*, FEDERAL TRADE COMMISSION, (Oct. 2012), https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf). The U.S. Government Accountability Office also published its report in 2015, suggesting that Congress consider strengthening the consumer privacy framework to reflect changes in technology and the marketplace (*Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law*, GOVERNMENT ACCOUNTABILITY OFFICE (Jul. 30, 2015), https://www.gao.gov/products/GAO-15-621).

[21] We refer here to specific biometric data privacy statutes, not security breach notification laws, which 48 states have already enacted. *See* the website of the National Conference of State

laws regulating the collection of biometric information.[22] At least seven other states are considering enacting their own specific biometric privacy bills: Alaska, Connecticut, Arizona, California, Illinois, Massachusetts, and New Hampshire.[23] This state law trend is adding complexity to industries that market their products throughout the nation.

The Illinois (2008), Texas (2009) and Washington (2017) statutes are similar insofar as they all regulate the collection, retention and use of biometric data. Entities collecting biometric data must notify the subject that biometric data is being collected and the subject must in turn consent to such collection. The three statutes, however, differ in four keys respects: (i) definitions, (ii) scope, (iii) procedural requirements and (iv) availability of a private cause of action. This creates potential uncertainty for collectors of biometric data from people across the U.S. Rather than worry about violating state laws, these companies may simply geo-fence the availability of their applications.[24]

(i) Definition of Biometric Data

The definition of biometric data in the three statutes includes retina or iris scans, voiceprints and fingerprints. Texas and Illinois, additionally, specifically call out "hand or face geometry" (i.e. facial scanning).[25] Washington (the most recent statute) does not

---

Legislatures, on Security Breach Notification Laws, available at: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

[22] Respectively, the Illinois Biometric Information Privacy Act ("BIPA") (740 ILCS 14) (hereinafter referred to as "Illinois"); Section 503.001 of the Texas Business and Commercial Code (hereinafter referred to as as "Texas"); and House Bill 1493 on Biometric Identifiers, passed in Washington on March 2, 2017 (hereinafter referred to as "Washington").

[23] *See e.g* Alaska (HB 72) (prohibiting the collection of biometric data without proper notice and consent and requiring timely disposal when the data is no longer needed), available at http://www.akleg.gov/basis/Bill/Detail/30?Root=HB%20%2072; Connecticut (HB 5522) (preventing retailers from using facial recognition software for marketing purposes), available at https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&bill_num=HB-5522; Arizona (SB 1373) (limiting the collection of biometric data by schools without consent), available at https://legiscan.com/AZ/bill/SB1373/2017; Illinois (HB 2411) (an amendment to the existing Illinois statute preventing companies from collecting biometric data as a condition for the provision of goods or services, with the exception of background checks and security protocols), available at http://www.ilga.gov/legislation/BillStatus.asp?DocTypeID=HB&DocNum=2411&GAID=14&SessionID=91&LegID=103118; California (SB 327) (requiring smart phones and other devices to inform users when biometric data is being collected beyond ways expected for known functionality), available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327; Massachusetts (SB 95) (adding "biometric indicators" to the definition of personal information under state data security law), available at https://malegislature.gov/Bills/190/S95 and New Hampshire (HB 523) (regulating collection of biometric data with a private right of action similar to the Illinois statute), available at https://legiscan.com/NH/text/HB523/id/1456913.

[24] *See* Section III.B.

[25] *See* Texas §503.001 (a) ("retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry"); Illinois §10 ("retina or iris scan, fingerprint, voiceprint, or scan of hand or face

regulate the collection of hand or face geometry and contains some language that is ambiguous:

> "Biometric identifier" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual. *"Biometric identifier" does not include a physical or digital photograph, video or audio recording or data generated therefrom*, or information collected, used, or stored for health care treatment, payment, or operations under the federal health insurance portability and accountability act of 1996.[26]

While Washington expressly excludes "a physical or digital photograph" from its scope, the statute could be interpreted as applying to data generated *from* "a physical or digital photograph" (for example, data generated by applying facial recognition to a photograph in one's smartphone library).[27] This ambiguity raises issues that may prove problematic for AR companies, which prefer certainty when rolling out facial recognition features in each state.

(ii) Scope – commercial or any purposes?

The Illinois statute is not limited to a particular type of use. It applies to *any* collection of biometric data, both commercial and non-commercial.[28] Washington and

---

geometry"); Washington 1493 §3 ("data generated by automatic measurements of an individual's biological characteristics, such as fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns of characteristics that is used to identify a specific individual"). Interestingly, the Montana (HB 518), which died in standing committee, went even further, defining biometric data as including both "gait" and "vein" recognition. If future bills borrow this broad definition of "biometric data", it is unclear whether VR's body tracking technology may become precise enough to be considered collection of a person's manner of walking (gait).

[26] *See* Washington §3 (emphasis added). 42 U.S.C.A. § 1320d (West).

[27] *Id.* The definition of "biometric identifier" does not include "a physical or digital photograph, video or audio recording *or data generated therefrom*" (emphasis added). The wording "or data generated therefrom," at the end of the sentence, appears to apply only to "audio recordings," not "physical or digital photograph." This may be interpreted in two ways: (1) "physical or digital photographs" are completely excluded from the definition of biometric data, including any data generated therefrom; or (2) as the qualifier "or data generated therefrom," attaches to "audio recordings" only, data generated from "physical or digital photographs" *is* covered by the statute. This issue, if brought before a court and resolved in favor of a broad interpretation, would present a risk for AR developers marketing facial recognition applications in Washington that either scan users' faces or generate data from existing photographs. Note that in Illinois, a judge has already made clear that BIPA covers "scans of facial geometry", no matter how they are created. *See* Rivera v. Google Inc., 238 F. Supp. 3d 1088 (N.D. Ill. 2017).

[28] The Illinois statute applies to the collection of biometric data for both private and commercial purposes. *See* Illinois §15(c) ("No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it [meets the consent and disclosure requirements set out in the statute]").

Texas, in contrast, regulate only the more narrow collection of biometric data for "commercial purposes."[29] While Texas does not define "commercial purposes," Washington limits "commercial purposes" to a:

> "purpose in furtherance of the sale or disclosure to a third party of a biometric identifier for the purpose of marketing of goods or services when such goods or services are *unrelated to the initial transaction in which a person first gains possession of an individual's biometric identifier.*"[30]

The statute is triggered only where biometric data is being collected at least in part to sell to third parties. Collection related solely to the functionality of the application or product appears, therefore, to remain unregulated. This carve out is significant for AR/VR companies looking merely to improve their product's effectiveness, and not otherwise market the data collected.[31]

(iii) Procedural requirements

Illinois imposes specific procedural requirements for obtaining a subject's consent. A private entity cannot collect or obtain any biometric data unless it first (1) informs the subject that a "biometric data identifier" is being collected;[32] (2) informs the subject of the specific purpose and length of term for which the biometric identifier is being collected, stored and used;[33] and (3) the entity receives a *written* release executed by the subject.[34] Texas and Washington, in contrast, have not specified a particular process for providing notice or obtaining consent. Washington expressly provides particular flexibility, as the exact notice and type of consent required is "context dependent".[35]

---

[29] *See* Texas, §503.001 (c) ("person who possesses a biometric identifier of an individual that is captured for a *commercial* purpose") and Washington §2 ("A person may not enroll a biometric identifier in a database for a *commercial* purpose") (emphasis added).

[30] Washington §2 (emphasis added). The statute also excludes "security or law enforcement purposes" for "commercial purposes".

[31] By way of example, a "My Super Bowl" application using facial recognition for the sole purpose of overlaying the colors of a user's favorite football team over his or her face during the Super Bowl, would be excluded form the scope of the Washington statute.

[32] Illinois §15(b)(1) ("informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored.")

[33] *Id.* §15(b)(2) ("informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identified or biometric information is being collected, stored, and used.")

[34] *Id.* §15(b)(3) ("receives a written released executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.") Note that a written release is defined as "informed written consent or, in the context of employment, a release executed by an employee as a condition of employment." *Id*. at §10.

[35] Washington §2(2). Washington gives companies the option to select between giving notice, obtaining consumer notice or providing a "mechanism to prevent subsequent" commercial uses before collecting the information.

(iv) Private Right of action

A private right of action exists only in Illinois.[36] Texas and Washington opted to restrict legal action to the state's attorney general.[37] The availability of a private cause of action in Illinois, as discussed further below, has already led to multiple actions being filed under that statute against companies using facial recognition technologies.

Overall, the Washington statute, which came into force in 2017 is more favorable to biometric data collectors than its predecessors. This, and the differences outlined above, may be attributed to the decade that separates the Illinois/Texas and Washington legislative efforts. The main impetus for the Illinois and Texas statutes was the introduction of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias.[38] These statutes were part of the government's earlier efforts to coordinate biometric data use and therefore best left for the government to regulate.[39] Knowledge of biometric data collection has since evolved. The Washington statute explicitly recognizes that citizens of Washington disclose biological information not just for commerce and security but "convenience" as well.[40] Moreover, the procedural flexibility included in the latest statute may also reflect legislative sensitivity to the fact that Washington is home to a number of companies heavily involved in AR and potentially VR, including Amazon and Microsoft.

B. Regulation in the EU

In stark contrast to the disparate development of biometric data collection regulation in the US, data collection in Europe is well-established and closely regulated. The Data Protection Directive was adopted in 1995 to regulate the processing of personal data within the European Union.[41] On 25 May 2018, the new GDPR will apply across all

---

[36] Illinois §20 ("Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party.")

[37] *See* Texas §503.001 (3)(d) ("The attorney general may bring an action to recover the civil penalty") and Washington § 3(d) ("This chapter may be enforced solely by the attorney general under the consumer protection act.")

[38] *See e.g.* 740 Ill. Comp. Stat. Ann. 14/5 ("BIPA") ("Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions"); Annemaria Duran, *Understanding the Texas Privacy Law as an Employer* (Dec. 29, 2017), https://www3.swipeclock.com/understanding-texas-biometric-privacy-law-employer/ ("In 2007, Pay By Touch first introduced biometric technology and a promise to change the world of payments. Customers linked their credit cards, bank accounts, rewards programs and other information to their fingerprint.").

[39] For more information on the history of biometrics, *see* Stephen Mayhew, *History of Biometrics* (Jan. 14, 2015) http://www.biometricupdate.com/201501/history-of-biometrics ("2008 – U.S. Government begin coordinating biometric database use").

[40] Washington §1.

[41] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement*

28 EU Member States. Its key objective is to "protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy".[42] One mechanism by which the GDPR achieves this is the provision of a new framework for the processing of "special categories of personal data"[43], which include biometric data.[44]

This new framework imposes onerous obligations on data controllers collecting biometric data from data subject within the EU[45], namely:

(1) **Consent**. Processing of data will be lawful only to the extent that the data subject has given affirmative consent to the processing of his or her personal data for one or more specific purposes.[46] Silence, pre-ticked boxes or inactivity are not considered consent[47]. The burden is on the data controller to show that the data subject has consented to the data processing, which the data subject can withdraw at any time.

(2) **Freely given.** Consent is not deemed freely given if the contract was conditional on consent to the processing of personal data that was not necessary for the performance of the contract.[48]

---

of such data, 1995 O.J. (L 281), available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046.

[42] *See* website of the GDPR, https://www.eugdpr.org/. Note that the GDPR applies to all companies processing and holding the personal data of data subjects residing in the EU, regardless of the company's location. A California based company collecting biometric data from a user residing in Italy, for example, will be caught by the GDPR.

[43] *Id.* at Article (9).

[44] *Id.* at Article 4(14) ("'biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.") The very broad EU definition, capturing any kind of behavioral data that could enable unique identification of a person, stands in marked contrast to the more narrowly defined language in the Washington, Illinois and Texas statutes. *See supra* note 25.

[45] *Id*. at Article 4(7) ("'controller' 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.")

[46] *Id.* at Article 6 (2)(a) ("the data subject has given consent to the processing of his or her personal data for one or more specific purposes").

[47] *See* Article 32 ("Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent.")

[48] *See* also Article 4(11) ("'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by

(3) **Record of processing activities.** Data controllers will have a positive obligation to maintain a written record of collected data, including (a) the purpose for collection, (b) a description of categories of data subjects and personal data, (c) the categories of recipients to whom the personal data have been or will be disclosed, and (d) a general description of technical and organization security measures taken by the controller.[49]

(4) **Designation of a representative**. All non-EU data controllers will have to designate a representative to act on behalf of the data controller and monitor the controller's behavior in the EU, unless the collection is "occasional" and "unlikely to result in a risk to the rights and freedom of natural persons, taking into account the nature, context, scope and purpose of the processing or if the controller is a public authority or body."[50]

(5) **72-hour notification period**. All operators will have to notify a supervisory authority within 72 hours of becoming aware of a personal data breach.[51]

Data collectors must show compliance with the GDPR, including the framework outlined above, by 25 May 2018, at which point, the GDPR will automatically come into force at a domestic level. Many Member States, including the UK, France and the Netherlands have started preparing companies for the GDPR's effective date.[52] Over the course of 2017, a number of non-EU countries also addressed the collection of biometric data, whether by legislation or the issuance of best practices.[53]

---

a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.").

[49] *Id.* at Article (13)(1).

[50] *Id*. at Article (85).

[51] *Id.* at Article (33).

[52] Government organizations across the EU are shepherding stakeholders into compliance with the GDPR, such as the Data Protection Authority in the UK (Brexit does not affect the implementation of the GDPR) or the *Commission Nationale de l'Informatique et des Libertés* (CNIL) in France. *See Biometric data and the General Data Protection Regulation*, GEMALTO (Dec. 14, 2017), https://www.gemalto.com/govt/biometrics/biometric-data.

[53] *See e.g*. Japan (definition of personal data expanded to include biometrics), *Significant changes to Japanese data protection law*, LEXOLOGY (Feb. 15, 2017), https://www.lexology.com/library/detail.aspx?g=380d104a-2434-4b0e-8e01-4bf021fb5f67; Israel (approval of biometric database law), *Israeli Parliament Approves Biometric Database Law*, ISRAEL DEFENSE (Mar. 13, 2017), http://www.israeldefense.co.il/en/node/28828; India (India's supreme court ruled in August that any law seeking to restrict privacy, including those related to India's biometric database, would now have to be measured against article 21 of the Indian Constitution, which safeguards an individual's "life and liberty"), Michael Safi, *Indian court rules privacy a 'fundamental right' in battle over national ID cards*, THE GUARDIAN (Aug. 24, 2017), https://www.theguardian.com/world/2017/aug/24/indian-court-rules-privacy-a-fundamental-right-in-battle-over-national-id-cards; and, Russia (guidance issued by Russian data protection authority recommending that privacy policies disclose all collection of biometric data),

III. Impact of Biometric Statutes

A. Increasing Class Actions

Nearly forty biometric privacy lawsuits were filed in 2016-2017 against tech giants including Google,[54] Facebook,[55] Snapchat,[56] Shutterfly[57] and a number of companies and facilities that have incorporated biometric scanning in their employee time-clock process.[58]

While most class actions are still pending, one court of appeals has already dismissed a lawsuit brought under the Illinois Biometric Information Privacy Act

---

Roskomnadzor publishes privacy guidelines for data operator, (Aug. 17, 2017), http://www.privacy-ticker.com/roskomnadzor-publishes-privacy-guidelines-for-data-operator/.

[54] Google was accused of violating BIPA by collecting "face prints" without people's consent in conjunction with its cloud-based Google Photo service. U.S. District Court Judge Edmond Chang refused to grant Google's motion to dismiss, despite Google's argument that requiring it and other photo services to abide BIPA would "unconstitutionally burden interstate commerce." Google's request for immediate appeal to the 7th Circuit was denied, but the possibility of authorizing a future appeal was left open. *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088 (N.D. Ill. 2017). *See also* Wendy Davis, *Google Can't Take 'Faceprint' Battle To Appellate Court*, DIGITAL NEWS (Jun. 29, 2017), https://www.mediapost.com/publications/article/303714/google-cant-take-faceprint-battle-to-appellate.html.

[55] A number of class action lawsuits have been brought against Facebook alleging that it violates BIPA with its photograph tagging suggestion feature. *See e.g.* Pezen v. Facebook Inc., 1:15-cv-03484 (N.D. Ill. filed 04/21/15), Licata v. Facebook Inc., 1:15-cv-04022 (N.D. Ill. filed 5/5/15), Patel v. Facebook Inc., 1:15-cv- 04265 (N.D. Ill. file 5/14/15), and Gullen v. Facebook Inc., 1:15-cv-07861 (N.D. Ill. filed 8/31/15). Facebook's motion to dismiss was denied in 2016. *See In re Facebook Biometric Info. Privacy Litig.,* 185 F. Supp. 3d 1155, 1170 (N.D. Cal. 2016).

[56] See e.g. Jose Luis Martinez, et al. v. Snapchat Inc., No. 2:16-CV-05182, C.D. Calif. (class action filed under BIPA against Snapchat for collecting and storing "face templates" – highly detailed geometric maps of the face – of millions of individuals using facial recognition technology that extracts and analyzes data from the points and contours of users' faces when they use Snapchat's "Lenses" feature). Note that the lead plaintiffs filed a notice of voluntary dismissal in California federal court on August 30, 2016, agreeing to pursue their claim against Snapchat via arbitration. *See* https://www.lexislegalnews.com/articles/10898/snapchat-biometrics-class-complaint-dismissed-in-favor-of-arbitration.

[57] Norberg v. Shutterfly, Inc., No. 15-05351 (N.D. Ill. filed June 17, 2015). The case has since been settled. *See* Rebecca Campbell, *Shutterfly settles Illinois privacy class action over facial recognition tech*, COOK COUNTY RECORD (May 9, 2016, 4:03pm), https://cookcountyrecord.com/stories/510723060-shutterfly-settles-illinois-privacy-class-action-over-facial-recognition-tech.

[58] These lawsuits allege that employers using timeclocks that scan employee fingerprint, retinas and irises to track hours or work have failed to notify employees in writing about the collection and storage of biometric data and obtain proper consent. *See e.g.* Baron v. Roundy's Supermarkets, Inc., No. 17-03588 (N.D. Ill. filed May 11, 2017) (employees allege that the Roundy's chain of grocery store has been scanning employee fingerprints without properly obtaining the written executed release and making the required disclosures concerning the collection, storage, use or destruction of biometric identifiers or information).

("BIPA")[59] for lack of standing.[60] The case arose from the "MyPlayer" feature of video games like "NBA 2K15", developed by Take-Two, which allows gamers to create a personalized basketball player that displays a realistic 3D rendition of the gamer's face (or "avatar"). To create an avatar, the gamer must first agree to the terms and conditions displayed on the screen, which include the disclosure that, by proceeding, the user agrees to having his or her face scanned.[61] Gamers then hold their faces 6 to 12 inches of the camera and slowly turn their head 30 degree to the left and right during the scanning process.[62]

The Second Circuit Court of Appeals found that such click-to-agree process was sufficient to meet the disclosure requirements of BIPA. The fact that the disclosure omitted the word "geometry", as used in the statute, did not render the disclosure inadequate.[63] Moreover, despite Take-Two's failure to inform gamers of the duration that it would hold the biometric data, the plaintiffs had not alleged that Take-Two lacked such protocols, or that its policies were inadequate. Rejecting the plaintiff's attempt to "manufacture an injury", the court concluded there was no material risk that Take-Two's procedural violations had resulted in the plaintiffs' biometric data being "compromised".[64]

While this summary order has no precedential effect,[65] it may nonetheless influence later courts in deciding whether mere procedural breaches of BIPA are insufficient to confer Article III standing.

B. Increasing pressure on AR/VR companies

Outside of the courtroom, biometric privacy legislation already appears to have affected at least one company's geographic roll-out of its application. In January 2018, Google released an application that matches selfies with historical artwork look-alikes (Google's Arts & Culture application). The application requires a user's consent to proceed after displaying a disclosure that "Google won't use data from your photo for any other purpose and will only store your photo for the time it takes to search for

---

[59] 740 ILCS 14/1.

[60] *Santana v. Take-Two Interactive Software, Inc.*, No. 17-303, 2017 WL 5592589, at *1 (2d Cir. Nov. 21, 2017).

[61] *Id.* at *1.

[62] *Id.*

[63] *Id* at *3. BIPA requires that private entities be informed that a "biometric identifier" is being collected or stored and defines a "biometric identifier," among other things, as a "scan of… face *geometry*" (emphasis added). To the extent that Take-Two departed from BIPA's requirements, it only did so insofar as it omitted the term, "geometry."

[64] *Id.* at *4 ("While it is true that BIPA's legislative findings identify consumers' withdrawal from biometric-facilitated transactions as a problem, they clarify that this issue arises only where a consumer's biometric has been "compromised," *i.e.*, collected or disclosed without his or her authorization.)

[65] *Id*. ("RULINGS BY SUMMARY ORDER DO NOT HAVE PRECEDENTIAL EFFECT.")

matches."[66] Millions of users downloaded the application. The selfie functionality, however, was not available for users located in Illinois and Texas at the time of download.[67] Those in Washington, however, were able to download and use the selfie tool.[68] While Google did not make a statement either way,[69] the comparatively greater breadth and scope of the Illinois and Texas statues, combined with Google's continuing litigation under BIPA, suggest that Google may be proceeding cautiously in states with broadly defined biometric privacy laws.[70]

Other companies have previously displayed similar caution in rolling out biometric data collection functionalities dependent on consumer location, but in Europe. A 2016 study by the Information Systems Audit and Control Association (ISACA), notably, found that the majority of surveyed European companies were hesitant to implement AR for business purposes in the EU due to privacy regulations.[71] In November of 2016, John Hanke, the founder of Niantic, Inc. (the company behind Pokémon Go), echoed these concerns before Congress, calling for greater clarity with European colleagues about the ambiguous interplay between AR and privacy in the EU.[72] Despite Google's silence on its decision not to make its art selfie application available in Illinois and Texas, the message is clear: the ambiguity and hesitation is no longer confined to Europe.[73]

---

[66] *See* Karen Hao, *No, Google's Arts & Culture app isn't secretly evil*. QUARTZ (Jan. 19, 2018), https://qz.com/1183296/googles-arts-culture-app-is-not-secretly-being-used-for-facial-recognition-training/.

[67] Jack Nicas, *Why Google's New App Won't Match Your Face to Art in Some States*, THE WALL STREET JOURNAL (Jan. 18, 2018), https://www.wsj.com/articles/why-google-wont-search-for-art-look-alike-in-some-states-1516194001.

[68] Note that while Washington excludes "a digital or physical photograph" from the scope of its biometric statute, an argument may be made that digital data generated *from* such photographs is regulated by the statute. *See supra* note 26. If so, a similar application that uses existing photographs rather than selfies could be caught by the Washington statute.

[69] The only response to date has been a tweet from Google: "This mobile experiment is currently available in parts of the US. Stay tuned as we try to improve and expand!" (Jan. 15, 2018), available at https://twitter.com/googlearts/status/952957246106951682 .

[70] Tobii, the company bringing eye-tracking technology to VR, has openly stated that application developers should seek explicit consent before any type of eye tracking. *See* VOICES OF VR (March 11, 2017) http://voicesofvr.com/514-tobii-recommends-explicit-consent-recording-eye-tracking-data/ ("From Tobii's side, we should be really, really cautious about using eye tracking data to spread around. We separate using eye tracking data for interaction… it's important for the user to know that's just being consumed in the device and it's not being sent. But if they want to send it, then there should be user acceptance.")

[71] *See e.g. Study: European companies hesitant to implement augmented reality*, IAPP (Nov. 14, 2016), https://iapp.org/news/a/study-european-companies-hesitant-to-implement-augmented-reality-citing-privacy-concerns/.

[72] Author's personal notes from hearing, Washington D.C., Nov. 16, 2017.

[73] The ambiguity in the US is compounded by the possibility of right of publicity statutes being interpreted as encompassing biometric data. The plaintiffs in *Santana* tried this approach in their first hearing before the New York District Court, arguing that Take-Two had misappropriated their facial scans to their detriment, and thereby invaded their privacy. The judge dismissed the plaintiff's "creative theory" as incompatible with their own allegation that they agreed to have

IV. Conclusion

AR and VR can no longer be dismissed as passing trends. Last year witnessed remarkable technological advancements in both AR and VR. It also saw a surge of state biometric data bills and legislation, exposing AR and VR companies to private and state actions. As courts continue to make their way through the biometric privacy cases, the actual requirements and impact of these statutes will become clearer. Until then, AR and VR companies are expected to consider the location of their consumers and tailor their activities accordingly.

In doing so, developers may wish to consider adopting the most demanding standard: the GDPR. On the one hand, complying with the GDPR may require upfront investment in drafting privacy policies and training employees. But it will (a) decrease the likelihood of running afoul the varying levels of regulations within the US, and (b) lay the groundwork at an early stage for a more seamless transition into the European market. On the other hand, following the GDPR may stifle certain innovation, which U.S. companies will reject. Assessing companies' risk tolerance versus their desire to leverage biometric data in the face of the growing body of state laws is key to helping them make good decisions for their businesses.

Adequate biometric data disclosures, moreover, may also serve a greater reputational interest. The AR/VR market is booming, with companies everywhere seeking to establish themselves as leaders in these industries. Achieving recognition as both a cutting-edge *and* responsible developer may be a critical step in securing the consumer vote necessary to do so, and may have the added benefit of slowing down the spread of additional state biometric data laws.

Edward Klaris is Managing Partner and Alexia Bedat is an Associate at Klaris Law, which is based in New York and focuses on media, entertainment and intellectual property.

---

their faces scanned, highlighting that this branch of the privacy doctrine is designed to protect a person from having his name or image used for commercial purposes *without consent*. Moreover, any value obtained by Take-Two from the scans would be irrelevant, so long as the action did not diminish the plaintiff's likeness. The judge also rejected the existence of a "right to biometric privacy". *See Vigil v. Take-Two Interactive Software, Inc.,* 235 F. Supp. 3d 499, 516 (S.D.N.Y. 2017), aff'd in part, vacated in part, remanded sub nom. Santana v. Take-Two Interactive Software, Inc., No. 17-303, 2017 WL 5592589 (2d Cir. Nov. 21, 2017).