6-26-2018

Privacy Regulation in the Age of Biometrics That Deal With a New World Order of Information

Michael Monajemi

PRIVACY REGULATION IN THE AGE OF BIOMETRICS THAT DEAL WITH A NEW WORLD ORDER OF INFORMATION

Before Sept. 11, the idea that Americans would voluntarily agree to live their lives under the gaze of a network of biometric surveillance cameras, peering at them in government buildings, shopping malls, subways and stadiums, would have seemed unthinkable, a dystopian fantasy of a society that had surrendered privacy and anonymity. - Jeffrey Rosen

Michael Monajemi

I. INTRODUCTION

With the iPhone X, getting into your phone is now so easy with Face ID—all you have to do is simply glance at your phone. Face ID is now a seamless way to use your unique face as authentication. With just one look at the camera, the sensor scans your face, matches it to the data on file, and unlocks your phone. However, it can also authorize purchases from the iTunes Store, App Store, and payments using Apple Pay.[1] It might seem interesting to use your face as a password, but does this raise any questions about privacy in the digital age?

As biometric technology is increasingly being used and accepted in the digital sphere, questions surrounding the privacy and security concerns are increasing. Because biometric data is stored on mobile devices, such as Apple's iPhone and Samsung's Galaxy, and in cloud-based biometric databases, inevitably questions arise as to how our personal data is being secured from the outside world. But it is not just in phones—biometric technologies are showing up in airports,[2] retail stores,[3] and schools.[4] Where is my data being

---

[1] *About Face ID Advanced Technology*, APPLE (Dec. 20, 2017), https://support.apple.com/en-us/HT208108.

[2] Ron Nixon, *Border Agents Test Facial Scans to Track Those Overstaying Visas*,N.Y. TIMES (Aug. 1, 2017), https://www.nytimes.com/2017/08/01/us/politics/federal-border-agents-biometric-scanning-system-undocumented-immigrants.html.

[3] Chris Frey, *Revealed: How Facial Recognition Has Invaded Shops – and Your Privacy*, THE GUARDIAN (Mar. 3, 2016), https://www.theguardian.com/cities/2016/mar/03/revealed-facial-recognition-software-infiltrating-cities-saks-toronto.

[4] *Biometrics in US Education Sector to See Significant Growth*, FINDBIOMETRICS (Aug. 14, 2015), https://findbiometrics.com/education-sector-biometrics-29142/.

stored? Who has access to it? How well is it protected? What regulation is in place to protect the privacy and security of biometric technology?

Private organizations and governments are readily acquiring an exorbitant amount of data on individuals on a day-to-day basis.[5] Everything we use these days on the internet requires us to log in with our email address, Facebook profile, or our telephone number.[6] The data that is then generated shows how long one spent on a site, what one buys, what websites are visited, etc.[7] All of this data is then disseminated through various channels on the information superhighway, which then treats data as a commodity—valuable information that the government and private organizations can use.[8] This is how companies like Facebook and Google make their money: they earn profits by collecting data on individuals and process that data instead of charging for using their services.[9] However, in recent years the

---

[5] Mary Madden & Lee Rainie, *Americans' Views About Data Collection and Security*, PEW RESEARCH CENTER (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-views-about-data-collection-and-security/.

[6] Fahmida Y. Rashid, *Signing into Websites with Google, Facebook is Good for Security*, PCMAG (May 21, 2015, 12:19 PM), https://www.pcmag.com/article2/0,2817,2484486,00.asp.

[7] Chris Hoffman, *The Many Ways Websites Track You Online*, HOW-TO GEEK (Sept. 28, 2016), https://www.howtogeek.com/115483/htg-explains-learn-how-websites-are-tracking-you-online/.

[8] *The World's Most Valuable Resource is No Longer Oil, But Data*, THE ECONOMIST (May 6, 2017), https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource.

[9] Greg McFarlane, *How Facebook, Twitter, Social Media Make Money from You*, INVESTOPEDIA, https://www.investopedia.com/stock-

technological evolution has produced new ways to identify individuals and collect data through biometric information.

Privacy in all its forms is of central importance to many systems of protecting one's fundamental rights. However, the right to privacy in most cases is unclear.[10] Moreover, evolution in the world of technology is not making it easy for courts or legislators to come up with a comprehensive way to deal with privacy rights.[11] Nevertheless, due to the technological revolution of the twenty-first century, certain countries are taking steps to expand the definition of privacy in terms of what information will be protected. One such example is the EU's upcoming General Data Protection Regulation ("GDPR"), which will become effective in May 2018 and will consider biometric data as a special category of personal data that calls for stricter rules on the processing of that data.[12] The GDPR will aim to provide harmonization

---

analysis/032114/how-facebook-twitter-social-media-make-money-you-twtr-lnkd-fb-goog.aspx (last visited Mar. 24, 2018).

[10] *See generally Privacy and Human Rights: An International Survey of Privacy Laws and Practice*, GLOBAL INTERNET LIBERTY CAMPAIGN (Mar. 24, 2018), http://gilc.org/privacy/survey/intro.html.

[11] Cameron F. Kerry, *The Law Needs to Keep Up with Technology But Not at the Expense of Civil Liberties*, FORBES (Nov. 6, 2014), https://www.forbes.com/sites/realspin/2014/11/06/the-law-needs-to-keep-up-with-technology-but-not-at-the-expense-of-civil-liberties/#739a2478cd14.

[12] *See* Commission Regulation 2016/679 of Apr. 27, 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) 87, https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en [hereinafter GDPR].

across the EU, as well as safeguard individual citizens' data rights in the increasingly technological world.[13]

The word "biometrics" makes one think of shows like Star Trek where the computer identified members of the crew based solely on their voice. But the use of "biometrics" for identification did not start in the twenty-fourth century. Fingerprints are one of the most commonly used biometric identification that police use to identify people.[14] But as biometric technology changes and becomes popular in both the private and public sectors, the use of the information by unauthorized parties raises privacy concerns.[15] Biometric identification systems that use certain physical traits such as fingerprint scans or facial recognition are becoming increasingly popular.[16] Cell phone companies have incorporated fingerprint scanners and facial recognition technologies into their devices to prevent unauthorized users from getting into another's device.[17] Because biometric systems play a role in distinguishing individuals through their personal data, there is concern that companies or the

---

[13] *Id.* at 1.

[14] *Fingerprints and Other Biometrics*, FEDERAL BUREAU OF INVESTIGATION, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics (last visited Mar. 24, 2018).

[15] *See generally* Brendan Collins, *Privacy and Security Issues in Social Networking*, FAST COMPANY (Oct. 3, 2008), https://www.fastcompany.com/1030397/privacy-and-security-issues-social-networking.

[16] Vikas Agrawal, *How Biometrics is Silently Becoming the New Normal*, ENGADGET (Jan. 10, 2017), https://www.engadget.com/2017/01/10/how-biometrics-is-silently-becoming-the-new-normal-infographic/.

[17] *Id.*

government can misuse such information.[18] This Note will discuss the European Union's forthcoming regulation known as the General Data Protection Regulation and regulations in the United States that refer to biometrics and their use. Part I of this Note will discuss the GDPR, what role it plays in privacy law in the EU, and some of the substantive requirements that must be met before data can be collected and used. Part II of this Note will discuss the landscape of the law in the United States as it relates to biometric legislation, with an overview of the laws in place that regulate their use, as well as some examples of cases in the US courts that reference biometric data. Part III will be the conclusion of this note, which will be my opinion on the biometric data protection in the EU and the US.

II. GENERAL DATA PROTECTION REGULATION BACKGROUND

A. WHAT IS THE GDPR?

The European Union's General Data Protection Regulation is the result of bringing the EU's data privacy protections into the twenty-first century.[19] The GDPR will replace the Data Protection Directive ("DPD") when it comes into effect in 2018 and will become the leading legislation regarding data protection in the EU.[20] The GDPR promises to

---

[18] JOSEPH N. PATO & LYNETTE I. MILLETT, NAT'L RES. COUNCIL, BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES 11, 108 (2010).

[19] Joe Curtis, *What is GDPR? Everything You Need to Know Before the 2018 Deadline*, ITPRO (Mar. 23, 2018), http://www.itpro.co.uk/it-legislation/27814/what-is-gdpr-everything-you-need-to-know-8.

[20] *Id.*

create more rights for data subjects, create obligations for controllers and processors, and create specific powers for supervisory authorities aimed at enforcing those new obligations.[21] The new legislation is intended to respond to the ever-evolving technological challenges and put in place a uniform law in place for the protection of personal data.[22] When the DPD was passed by the European Parliament in 1995, it was the first time that personal data protection was introduced as an autonomous right for the protection of individuals with regard to the processing of personal information.[23] In 2012, the EU made a new proposal for a more comprehensive Data Protection Regulation and stated that "rapid technological developments have brought new challenges for the protection of personal data," emphasizing the massive scale of data protection.[24] The GDPR will introduce larger penalties for organizations that do not comply with the regulations and will provide greater control for everyday citizens in the use of their data by private parties.[25]

The GDPR will go into effect for all EU member states on May 25, 2018, after the two-year transition period is over.[26]

---

[21] *Id.*

[22] *Id.*

[23] Council Directive 95/46, 1995 O.J. (L 281) 31, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:1995:281:TOC.

[24] *Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (Jan. 25, 2012), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN.

[25] Curtis, *supra* note 20.

[26] *Id.*

Because the GDPR is a regulation, it will apply to all EU members states as well as the UK[27] when it goes into effect—each member state will not need to pass a new legislative act.[28] The GDPR applies broadly to two specific groups of "people." Many of the obligations under the GDPR will fall on the "person" who is classified as the "Data Controller" who will determine the purpose and means of processing a data subject's personal data.[29] The second person is the "Processor," who is defined as a "natural or legal person, public authority, agency, or other body which processes personal data on behalf of a data controller."[30] Processing data is very broadly defined as carrying out "any operation or set of operations" including: collection, recording, storage, retrieval, use, erasure, destruction of data, and more.[31] For example, if Acme sells items to Wile-E-Coyote and uses Road Runner Inc. to email consumers on Acme's behalf and track their activities, then Acme would be the data controller and

---

[27] The GDPR will apply to the UK because Brexit will not take place until after the regulation is in effect. *See* Paul McClean, *Brexit Timeline: Key Dates in UK's Divorce with EU*, FINANCIAL TIMES (June 14, 2017), https://www.ft.com/content/64e7f218-4ad4-11e7-919a-1e14ce4af89b. However, the UK has planned to enact legislation that will mirror the GDPR requirements so that their businesses do not lose out in trade with the rest of the EU. *See* Warwick Ashford, *UK Legislation Will Mirror EU's GDPR, says Matt Hancock*, COMPUTER WEEKLY (Feb. 1, 2017), http://www.computerweekly.com/news/450412141/UK-legislation-will-mirror-EUs-GDPR-says-Matt-Hancock.

[28] Curtis, *supra* note 20.

[29] *See* GDPR, *supra* note 13, at art. 4(7), at 33.

[30] *Id.* at art. 4(8), 33.

[31] *Id.* at art. 4(2), 33.

Road Runner Inc. would be the data processor. This is important because the GDPR treats Controllers as the principal party responsible for collecting and managing the data it acquires and will hold Controllers accountable for violations.[32]

B. OBJECTIVES OF THE GDPR

The purpose of the GDPR is to give back citizens over their own personal information, while providing a simple framework for companies to look to.[33] In essence, the GDPR will "harmonize" the data privacy laws across Europe to a minimum set of standards for companies that handle EU citizens' data to safeguard the collection, storage, and movement of personal data—a one-stop shop.[34] The purpose of the one-stop shop in the GDPR is meant to provide for a lead authority when a controller or processor is in more than one member state.[35] This would allow for a single point of contact for people to complain and reach out to. The lead supervising authority will then take the appropriate legal action only after discussing with all other supervising authorities so that they may reach a consensus.[36] In this way, the investigation for handling complaints can be streamlined to provide support through mutual assistance by supervisory

---

[32] *Id.* at art. 24(1), 47.
[33] Daniel Wagner, *GDPR, the Law, and Virtual Terror*, HUFFPOST (Dec. 10, 2017), https://www.huffingtonpost.com/entry/gdpr-the-law-and-virtual-terror_us_5a2d2cc9e4b022ec613b8358.
[34] *Id.*
[35] *Id.*
[36] *See* GDPR, *supra* note 12, at art. 54(1)(a), 66.

authorities and conducting joint investigations.[37] This cooperation among member states and supervising authorities will likely introduce the consistency needed to establish a clear and concise operation for data protection violations.

Another important feature of the GDPR is the expansive role of Data Protection Officers.[38] The goal is to have a uniform entity that can make sure that the organizations are following the GDPR.[39] Under the GDPR, the EU has tried to reconcile the bureaucratic nightmare that the members states had under the DPD regarding their reporting requirements. Now, the GDPR requires DPOs to inform and advice regarding compliance with the GDPR and other member states' data protection laws; monitor the companies' compliance with the law and internal policies such as training; advise in areas of data protection; and to act as the point of contact between the company and the supervisory authority.[40] Organizations that must appoint a DPO include public authorities, controllers or processors whose main activity consists of processing data that they regularly monitor on a large scale, and controllers or processors whose core activities involve the processing of sensitive personal data on a large scale.[41] These DPOs cannot just be anyone—

---

[37] *See id.* at art. 55-56, 67-68.

[38] *See id.* at art. 35, 53-54; *see also* Marc Dautlich & Stephan Appt, *Data Protection Officers – Will EU Businesses Face an Obligation to Appoint One?*, OUT-LAW (Jan. 13, 2015), https://www.out-law.com/en/articles/2015/january/data-protection-officers--will-eu-businesses-face-an-obligation-to-appoint-one/.

[39] *See* GDPR, *supra* note 12, at art. 37-39, 55-56.

[40] *Id.* at art. 39, at 56.

[41] *Id.* at art. 37, at 55.

they must be experts in the field of data protection and be able to fulfil the requirements that are specified in the regulation such that the DPOs will be able to advise on the compliance of data protection rules and monitor the performance of the data protection impact assessments.[42] DPOs are meant to be an independent authority in the company, whose sole purpose is to be responsible for ensuring that the fundamental rights of privacy are respected by the institution, and who report to the highest person in management.[43]

The GDPR's take is revolutionary, as it would be one of the first truly global laws in place. However, the GDPR does acknowledge that data protection rights, like all rights, are not absolute. For example, the GDPR will not apply to the processing of personal data if the data falls outside the scope of EU law; is related to EU foreign or security policy; if the processing is by the authorities for prevention, investigation, or the prosecution of criminal offences; or if the processing is by a person who does something as a part of a "purely personal or household activity."[44]

C. BIOMETRIC DATA IN THE GDPR

The types of data that the GDPR protects are divided into two main categories: Personal Data and Sensitive Personal Data.[45] Personal Data is defined as "any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification

---

[42] *See id.* at art. 37(5), 38-39, 55, 55-56.
[43] *Id.* at art. 38(3), 56.
[44] *Id.* at art. 2(2)(c), 32.
[45] *See id.* at art. 4(1), 9, 33, 38-39.

number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity."[46] Personal data includes things such as name and address, ID number, location data, and even web data, like IP addresses.[47]

Sensitive Personal Data is classified as a "special category of personal data" in the GDPR and by definition require more protection than personal data.[48] The special categories include things such as health and genetic data, racial data, political data, sexual orientation data and biometric data.[49] One of the most revolutionary aspects of the GDPR is the fact that it regulates biometric data as a separate entity rather than trying to include it in an existing privacy scheme that does not take into account biometric data sensitivity. Specifically, biometric data is defined as "personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allows or confirms the unique identification of that natural personal, such as facial images or dactyloscopic data."[50] Biometric data is defined under very broad terms such that the GDPR seems to recognize that

---

[46] *Id.* at art. 4(1), at 33.

[47] *See id.*; *see also* Cour d'appel [App.] [Court of Appeal] Brussels, Third Chamber, Nov. 24, 2011, Case C-70/10 (Belg.) (holding IP addresses "are protected personal data because they allow [internet] users to be precisely identified").

[48] Regulation 2016/679, art. 9, (EU) of the European Parliament and of the Council on the Protection of Natural Persons with Regard to Processing of Personal Data and on the Free Movement of Such Data, *available at* http://eurlex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=en.

[49] *Id*.

[50] *Id*. at art. 4(13), 9.

biometric data will continue to evolve, both the way it is collected but also what data points will be able to be collected. As such, the GDPR seems to be in a good position to apply to many different types of biometric data that will arise through the development of technology. The GDPR is looking forward and trying to make sure that it is in line with technological changes so that the law can keep up with the ever-advancing technologies.

The definition of biometrics recognizes two separate categories of biometric information.[51] The first is information that relates to a person's physical or physiological trait. This category is what most people would think biometrics data is, fingerprints, iris scans, etc. The second category is behavioral information such as what hand you hold your phone in, how long does it take you to shop in the supermarket, etc. In scope, any behavioral information could be used to uniquely identify someone and be considered biometric data. However, the GDPR is unclear how it will narrowly regulate this category as it has no nexus to the "normal" definition of biometrics as it relates to body information.

One critical impact of the GDPR's treatment of biometric data as sensitive personal data is that controllers will need to conduct Privacy Impact Assessments (PIA) for many forms of biometric data processing.[52] The GDPR now formalizes the need to for controllers to conduct an assessment of the possible impact of processing operations under certain conditions. Article 35 address two specific instances where controllers would need to incorporate a PIA

---

[51] *Id*. at art. 4(14).
[52] *Id*. at art. 35.

into their practice. The first is the processing of biometric data in situations where processing of biometric data will involve the use of new technologies.[53] Although biometric technology in one shape of form has been used for some time, new and evolving uses are being found due to the new technologies and the GDPR wants to make sure that controllers are prepared for them. The second is biometric data that is being processed to uniquely identify a natural person when the processing is being done on a large scale.[54] But many forms of existing biometric data processing will attach the GDPR's mandatory PIA requirement because it is foreseeable that the data processing will be conducted on a large scale, employ automated processing, and in some applications systematically monitor publicly accessible areas. Therefore, controllers will need to identify risks that processing data presents to the data subjects and implement protocols that will mitigate activities that form a high risk for the rights and freedoms of persons which in turn will influence how new privacy technology will be developed.

D. CONSENT IN THE GDPR

One of the directives of the GDPR is that organizations must get the consent of individuals when they plan to collect or store the persons data.[55] The GDPR defines consent as ""any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by

---

[53] *Id*. at art. 35(1).
[54] *Id*. at art. 35(3)(b).
[55] *Id*. at art. 18; *Id*. at art. 4(11).

statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[56]Consent must be active and affirmative by the person whose data is to be collected, "ticking a box when visiting an internet website, choosing technical settings… or by any other statement or conduct which clearly indicates… subject's acceptance… silence, pre-ticked boxes or inactivity should therefore not constitute consent."[57] The subject needs to be properly informed about the use of their personal data including how it will be processed and about their rights regarding their data. This is to make sure that people are specifically aware of what information they are giving up and not just blindly accepting the terms and conditions of something without understanding what they are giving up.[58] Article 7 then goes on to describe the conditions for consent being valid. Article 7 explains that the consent must be a written declaration that is distinguishable from other matters[59] in the declaration and it must be intelligible, easily accessible and be in clear and plain language, it must be free

---

[56] *Id*. at art. 4(11).

[57] Regulation 2016/679, Recital 32, (EU) of the European Parliament and of the Council on the Protection of Natural Persons with Regard to Processing of Personal Data and on the Free Movement of Such Data, http://eurlex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=en

[58] Joe Curtis, *Does your organisation comply with the new data protection rules?*, IT PRO (Mar. 23, 2018), *available at* http://www.itpro.co.uk/it-legislation/27814/what- is-gdpr- everything-you- need-to- know-8. The EU is moving towards a clear and concise opt-in policy where any privacy information that you are going to be giving away will need to be explicitly said and you must agree to it.

[59] The consent can't be tied up in with language for something else, it must appear explicitly on its own face.

of legalese so that anyone could understand what they are participating in.[60]

E. INDIVIDUAL RIGHTS IN THE GDPR

Individuals will have a stronger "right of erasure."[61] Individuals have the right to have their data erased in certain situations – effectively when the processing does not satisfy the GDPR. This first came to light when the CJEU ruled against Google and needed them to remove search results against a Spanish national when Google had no legal basis to process such information.[62] The right will apply when the data is no longer necessary for the purpose to which it was collected, or when a subject withdraws their consent and there is no other legal justification for the processing of the data.[63] However, this right is not an absolute and only applies in narrow cases where the controller has no legal ground for processing the information, such as in the case of Google.[64]

---

[60] The burden is on the Controller to show that the consent was legally was as the "controller shall bear the burden of proof for the data subject." This highlights the importance of record keeping that the GDPR want's companies to keep, especially important due to the new standard on violations of the GDPR.

[61] Regulation 2016/679, *supra* note 57, at art. 17; *see also* Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, ECLI:EU:C:2014:131/12.

[62] *Id.*

[63] Regulation 2016/679, *supra* note 57, at art. 1. (In practice, organizations will need to usually have unambiguous consent, process the information as necessary for the performance of the contract to which the data subject consented to, processing is necessary to follow a legal obligation to which the controller is subject and processing is necessary to uphold the legitimate interest of the controller or the third party).

[64] *Id.*

But what could be considered worrisome in the GDPR unlike the DPD is that data could be "unlawfully" processed for a variety of reasons[65] which would then make the controller in violation and the data then must be erased under the GDPR. The DPD left some more room for interpretation when the data must be deleted, so here it will be up to the states to make exceptions so that the "unlawfully" processed data does not become too onerous on themselves.

The data subjects also have the ability to request access to their data by asking the controllers whether personal data is being processed and how it is being used. Interestingly, they can also get a copy of the personal data that was collected by the controlling organization.[66] The GDPR emphasizes the right of the individual citizen to control what information is collected and stored about them.[67] Citizens also have the right to withdraw their consent of data collection at any time and the organization must stop unless they can demonstrate a "compelling legitimate ground,"[68] essentially shifting the burden to the organization to show that there is a specified and legitimate reason to collect the information, not just

---

[65] Such as the data is inaccurate or some of the information notice may not have been provided to the data subject.

[66] Regulation 2016/679, *supra* note 57, at art. 15; *see also* art. 13. (The controller must give the following information: The purpose of the processing, the categories of personal data concerned, the recipients to whom the personal data will be disclosed, the timeframe of the storage of the data, right to request erasure of personal data, who the supervising authority is and if there exists an automated decision-making program).

[67] FBI, *Fingerprints and Other Biometrics*, FBI, https://www.fbi.gov/services/cjis/fingerprints-and- other-biometrics.

[68] Curtis, *supra* note 19.

because they want to. However, public authorities are unable to rely on "compelling legitimate ground"[69] to legitimize their data processing activities. If they rely on such a ground, they will need to identify another legal way to process the data, for example, processing of such data is in the exercise of official authority.

F. IMPLEMENTING DATA PROTECTION BY DESIGN AND BY DEFAULT

The GDPR now makes it a legal requirement for companies to create "data protection by design and by default."[70] Data protection by design requires taking data protection risks into account throughout the process of designing a new process, product or service, rather than treating it as an afterthought.[71] This means assessing carefully and implementing appropriate technical and organizational measures and procedures from the outset to ensure that processing complies with GDPR and protects the rights of the data subjects.[72] One of the new ways which the GDPR treats data protection by design is through the use of a

---

[69] Recitals give examples of what kind of processing could be considered a "legitimate interest", it includes the transmission of personal data for internal administrative purposes, or processing data to ensure network security such as preventing unauthorized access to electronic networks.

[70] *Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, COM (2012).

[71] *Id*.

[72] Through the use of a PIA a controller will be able to demonstrate the results and prove that an assessment has taken place.

pseudonymisation. Pseudonymisation is when the processing of personal data is done in such a way that it can no longer be tied to a specific data subject without more information. Privacy by design will help shape technologies into privacy-friendly objects for the end users because organizations must implement their designs in a certain way, for example by automatically deleting biometric data after a matching procedure.[73] "Data protection by default" requires ensuring mechanisms are in place within the organization to ensure that, by default, only personal data which are necessary for each specific purpose are processed.[74] This obligation includes ensuring that only the minimum amount of personal data is collected and processed for a specific purpose; the extent of processing is limited to that necessary for each purpose; the data is stored no longer than necessary and access is restricted to that necessary for each purpose. If true pseudonymisation could be achieved then a lot of privacy concerns could be relieved, however, with biometric data that is unlikely since the purpose of biometrics is to uniquely identify an individual for the purposes of authentication.

---

[73] Google for instance says they do this in the new feature of matching your selfie to a piece of art. They collect the selfie and give a notification that your picture will only be used to match and will not be stored or used for any other purpose.

[74] *Id.*

G. IMPLICATIONS OF THE GDPR FOR COMPANIES OUTSIDE OF THE EU

The GDPR is especially important for companies and organizations outside of the EU who deal with EU data subjects because the regulation has extraterritorial reach.[75] Since the regulations and penalties that are put in place are more expansive than the DPD, companies must be aware of how it will affect them. Non-EU established organizations are subject to the GDPR when the processing of personal data of data subjects in the EU is by a controller or processor that is not in the EU where the intent relate to either "[t]he offering of goods or services irrespective of whether a payment of the data subject is required to such data subjects in the Union, or the monitoring of their behavior as far as that behavior takes place in the Union."[76]

For the offering of goods and services, more than just accessibility is needed within the EU, the organizations must predict that their activities will be directed towards EU data subjects.[77] To establish what directed means, the CJEU has examined when something is directed towards EU member states. Some of the aspects that the CJEU will look toward if this is ever discussed in the courts will be things such an organizations paying money for search engine optimization to facilitate access to their website, or the context of what the organization is targeting, for example tourist destinations in member countries, domain names, or even if a website

---

[75] Nixon, *supra* note 2; Economist, *supra* note 8.
[76] *See* GDPR, *supra* note 12, at art. 3 sec. 2, art. 44.
[77] *Id*.

mentions that they have an international presence.[78] However, the GDPR does not make it clear whether Non-EU organizations who are "offering goods or services" to business in the EU would be subject to the scope of the regulation as listed in Article 3, since the regulation applies to the processing of personal data only.[79]

I believe the more common way that Non-EU organizations will be subject to the GDPR will be when they monitor EU data subject's behavior. This includes things like tracking individuals online and creating profiles and using that profile to predict certain behaviors and attitudes. Thus, it does not matter if a person buys something from a company not based in the EU if the intent was to target the customer. For instance, this could apply in cases where Facebook places cookies on a EU citizens computer for tracking their usage history to provide personal advertisements to them.[80] It seems that one of the major purposes of the evolution of the GDPR in terms of data subject's privacy is meant to deter companies

---

[78] Case C-585/08 and C-144/09, Pammer v. Reederei Karl Schluter GmbH & Co KG and Hotel Alpenhof Gesmb v. Heller, 2010 Reg. (E.C.) No. 44/2001.

[79] The GDPR does not make it clear if you target businesses as opposed to individuals how you will be affected when it comes to the disclosure and consent requirements that are the objective of the GDPR. This is specific to the offerings and does not include the monitoring aspect of the GDPR

[80] Facebook which is a US company that handles a massive amount of data from EU data subjects is going to have to essentially retool multiple business processes to comply with the new rules. They make most of their revenue on ads which are personalized because they do monitor offline behavior by their users. However, they have been working on retooling their systems for a while now to make sure that they are in compliance with the GDPR.

from overreaching their grasp on individual consumers.[81] The extra-territorial scope of the GDPR will make the EU a pioneer in data protection and most likely force privacy standards all over the world to rise up to a set standard. It will be interesting to see the changing legislation in privacy law in the next few years in countries such as the US and China because of the GDPR on their business.

H. ARTICLE 9 DISCUSSION OF COUNTRY DIFFERENCES

As opposed to a directive, the GDPR will go into effect in each member state without the need for each state to pass the same legislation. However, under Article 9, the GDPR does allow every member state to impose their own conditions related to the storage and collection of sensitive personal data like biometric data.[82] Although the GDPR will support a uniform standard across the EU, some member states have existing approaches to regulate sensitive personal data and those differences will be kept. This would mean that member states can still enact different procedural and substantive requirements to govern certain data which ultimately defeats a fundamental purpose of this regulation which is to provide a truly universal law throughout the European Union. As such, companies who seek to do business in the EU must also be aware of the individual member states regulations as well since they could impose other obligations on the collection and processing of biometric data which are not included in the GDPR. If companies are not aware then they will be in violation of the GDPR and the subsequent

---

[81] *See* GDPR, *supra* note 12, at art. 22.
[82] *See id.* at art. 9 sec. 4.

member states regulation which could penalize organizations even further, then they would be under the GDPR.

I. PENALTIES ASSOCIATED WITH A VIOLATION OF THE GDPR

In comparison to the DPD, the GDPR increases penalties for non-compliance.[83] Supervisor authorities have investigative powers and can issue warnings for non-compliance, perform audits, and need companies to meet deadlines.[84] The supervising authorities watch the data controllers and processors to make sure that they met the demands of the GDPR.[85] If a supervising authority finds that an organization has been in violation then they have the power to put sanctions on companies that have failed to follow with the Regulation.[86] Instead of being fined a specific number, the GDPR will base sanctions on the affected company's revenue.[87] If companies do not follow with certain GDPR regulations then the fines that are imposed may be up to 4% of the annual income for a corporation.[88]

III. PRIVACY REGULATIONS IN THE UNITED STATES

Unlike the EU and other jurisdictions, the United States does not have a centralized or dedicated data protection laws in place, instead data protection is regulated through a sector-

---

[83] *See id*. at art. 58, art. 83.
[84] *See id*. at art. 51.
[85] *See id*. at art. 58.
[86] *See id*. at art. 83.
[87] *Id.*
[88] *Id.*

specific approach.[89] There are many actors in the privacy law paradigm in the United States at the state and federal level. At the federal government, the regulatory scheme seems to depend on what kind of law is being implicated. If it references healthcare then the Department of Health and Human Services is responsible for the enforcement of the Health Insurance Portability and Accountability Act (HIPAA) against entities.[90] However, outside of any specific organization, the Federal Trade Commission (FTC) is primarily responsible for regulating privacy in the United States.[91] Section 5 of the FTC Act applies generally to consumer protection law and that is how the FTC enforces privacy in the US.[92] But if we look to the states we see that it is usually the Attorney Generals who bring about enforcement actions to enforce any specific violation of state privacy laws. However, due to the hodgepodge of regulation and enforcement, definitions of privacy vary in the United States. The FTC for instance defines personal data as data that can be used to contact or distinguish a person, such as IP addresses, and phone numbers.[93] The definition of sensitive personal data also varies across the US but includes things

---

[89] Daniel J. Solove, *The Growing Problems with the Sectoral approach to Privacy Law*, PRIVACY AND SECURITY BLOG (Nov. 13, 2015), https://teachprivacy.com/problems-sectoral-approach-privacy-law/.

[90] OFFICE FOR CIVIL RIGHTS, *Enforcement* Process, HEALTH INFORMATION PRIVACY (June 7, 2017), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html.

[91] *See generally* F.T.C., *Protecting Consumer Privacy*, FEDERAL TRADE COMMISSION, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy.

[92] 15 U.S.C. § 45 (2012).

[93] *See* F.T.C, *supra* note 91.

such as personal health data, consumer report information and children's information.

A. US FEDERAL APPROACH

Like the DPD and the GDPR, the US at one point tried to pass a comprehensive privacy reform bill in the 1970's to allow for the processing of personal data by both public and private entities.[94] Instead, Congress decided to not to pass the original bill and instead proposed a new bill where there was no oversight by any single committee or organization and only applied the law to the public sector, which in turn became the Privacy Act of 1974.[95] The Privacy Act of 1974 regulates the collection, use, dissemination, and maintenance of personal information (only) by federal government agencies.[96] In general strokes, the Act gives certain rights to individuals who provides any personal information to the government and then places restrictions and responsibilities on the handling of such data to a collector or agency.[97]

The Act tries to balance the governments need to collect information on subjects with an individual's right to privacy, specifically in to prevent unjustified use of personal information about the individual. In part, the Act restricts agencies from disclosing personally identifiable records that are maintained by the agencies, requires agencies to establish safeguards to protect the security of the data and allows individuals rights to access information on themselves and to

---

[94] Nadezhda Purtova, *Property Rights in Personal Data: A European Perspective* , 2 EUR. J. OF LEG. STUD, 3, 3 (2010).
[95] *Title 5 – Government Organization and Employees*, 5 U.S.C. § 552 (1974).
[96] *Id.* at sec. a.
[97] *Id.*

amend their records if somehow inaccurate.[98] The act establishes the minimum standards that must be complied with on a federal level by public agencies. Similar to the GDPR, the Privacy Act does not allow for information to be disclosed without consent.[99] The Act prohibits an agency from "disclosing any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains."[100] Also like the GDPR, the act has twelve exceptions to the rule some of which are the "Routine Use", "Intra-Agency Need to Know", or "Judicial" exception.[101]

However, regulations have been put into place to try and regulate some aspects of private data collection. In 2012, President Obama released a memo called "Consumer Privacy Bill of Rights," which later given to the FTC who then recommended to Congress to establish some minimum standards.[102] However, Congress has still not passed a bill that would be legally binding to establish a comprehensive minimum framework. Most states are not equipped to handle the evolution of technology that biometrics and other developments of the technological age have brought us with the current laws in place. As of January 2018, it is still legal in

---

[98] *Id.* at sec. e.
[99] *Id.* at sec. a.
[100] *Id.*
[101] 5 U.S.C § 552a(b)(1)-(12).
[102] The White House Washington, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, WHITE HOUSE ARCHIVES (Feb. 2012), https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf.

most of the United States for facial recognition software to identify a person using images taken without their consent while in public.[103] However, some states like Illinois, and Texas do not allow that technology to be used for a commercial purpose such as targeting individuals.[104] The problem with technology like Facial Recognition is that is can be performed without a person's consent and without an individual actually providing any information, all they have to do is step outside. Some shops already use facial recognition software to identify customers that misuse the stores policies on returns or to tag potential shoplifters.[105] The downside of the sectoral approach in the US as opposed to the current and future regulation in the EU is that the regulations are context-specific which leave many gaps in the regulatory framework. Those gaps make it hard to understand with and comply with the changing regulations.

There is no federal law in place to regulate biometrics, however, the FTC has given recommendations for best practices for companies. Specifically, about facial recognition technology the FTC published a memo in 2012 to give guidance to companies that seek to use facial recognition

---

[103] April Glaser Security, *Biometrics are Coming, Along with Serious Security Concerns*, WIRED (Mar. 9, 2016), https://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/.

[104] *Id.*

[105] Will Oremus, *Forget Security Cameras. Stores are Using Face Recognition to See if You're a Shoplifter*, SLATE (Nov. 25, 2015), http://www.slate.com/blogs/moneybox/2015/11/24/stores_are_using_face_recognition_to_catch_shoplifters.html

technology.[106] The FTC guidance seems to mirror both BIPA as well as the DPD and other EU privacy laws in place during that time. The first thing the FTC recommends is for companies to implement a privacy by design system by maintaining reasonable data security protections for biometric information, establish the correction deletion requirements for information and for companies to consider the sensitivity of the data in facial recognition technologies. In many ways, the FTC puts guidance on making things more transparent, or giving consumers a clear choice to opt-out of the collection of data, all things either the state laws provide for or are similar to laws in the EU. Although the FTC guidance is merely that and it not in effect for any type of enforcement action, the FTC has commented that if companies engage in unfair or deceptive business practices while using facial recognition technology, they will bring enforcement under Section 5 of the FTC act.[107]

B. STATE LAW APPLYING BIOMETRIC INFO

Currently there are three states that have statutes explicitly regulating the storage and use of biometric data: Illinois, Washington and Texas. In 2008, Illinois passed the first biometric act in the United States known as the Biometric

---

[106] *Facing Facts: 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.

[107] *Id.* at 2, n.6.

Information Privacy Act (BIPA).[108] Texas[109] passed a similar law in 2009 and recently Washington[110] passed a biometric privacy bill in 2017. All three bills are fundamentally similar with a few exceptions. All three state bills explicitly restrict the collection and storage of "biometric identifiers," which means an iris scan, fingerprint, scan of face geometry and a voiceprint.[111] BIPA also defines "biometric information" as "any information that is based on an individual's biometric identifier used to identify an individual regardless of how that information is captured, converted, stored, or shared."[112] However, in Texas, the law only applies to biometric identifiers and not the broader biometric information.[113]All three states also require that employers give notice and obtain explicit consent before they collect and store any biometric data. BIPA requires the employers to obtain "written" consent but the other bills do address whether consent must be in writing.[114]

However, the law differs in Washington in a few important ways. The first is that HB1493 focuses on the "enrollment" of biometric identifiers which is data used to identify an individual that is generated by automatic measurements of an individual's biological characteristic.[115] This includes things such as Fingerprints, iris scans,

---

[108] Ill. Biometric Info. Privacy Act, § 740 ILCS 14 (2008).
[109] Tex. Bus. & Com. Code Ann. § 503.001 (2009).
[110] Wash. H.B. 1493 (2017).
[111] Ill. Biometric Info. Privacy Act, *supra* note 108.
[112] *Id.*
[113] *Id.* at sec. 31:30.20. Applies to Iris scans, fingerprints, voiceprints and hand or face geometry.
[114] Ill. Biometric Info. Privacy Act, *supra* note 189.
[115] Wash. H.B., *supra* note 110.

voiceprint and other unique biological patterns or characteristics.[116] 1493's scope because it limits the enrollment of biometric identifiers or information in a database that is for a commercial purpose and further sale or disclosure of the information instead of broadly requiring affirmative consent for almost all collection and disclosure of biometric information. Under Washington law, biometric information may also be collected without a person's consent but cannot be made into a reference template that will then allow for a matching of identity without consent. Washington also does not include photographs, video or audio recordings or facial geometry as biometric identifiers. This is a response to the number of class action lawsuits that stem from companies violating Illinois BIPA statute. These lawsuits have put companies like Shutterfly and Google into the news since they allow users to group or tag their photos by automatically recognizing faces. Furthermore, Washington's consent requirements are laxer as they are "context-dependent" as opposed to BIPA which needs written notice and written release prior to collection of data.

Washington also provides a specific exception that BIPA and Texas do not; that the law's notice and consent do not apply if the biometric data is to be collected and stored for "security purposes," which is defined as data that is stored for "the purpose of preventing shoplifting, fraud, or any other misappropriation or theft of a thing of value."[117] All three states also require similar to the GDPR that the organizations exercise "reasonable care" to protect the biometric data,

---

[116] However, there are exceptions for physical or digital photographs, health care information and video or audio recordings.

[117] Wash. H.B., *supra* note 110, at sec. 3.

however, the states do differ in some respects in how they define reasonable care. In Illinois, it is specified that organizations should use "reasonable standard of care within the industry, and in a manner that is the same as or more protective than the manner in which the business stores, transmits, and protects other confidential information.[118] In Texas, the law allows for employers to protect the data from disclosure using reasonable care in the same way that organizations would protect other confidential data.[119] Finally, in Washington it requires organizations to just take reasonable care to prevent unauthorized access to the data.[120] The statute don't govern exactly how the companies will achieve this, just that they are required to do it.

Each state also has different policies when it comes to how the biometric information must be destroyed. BIPA is the strictest and directs the companies to set up written, publicly available policies that discuss the timeframe for storing the biometric data and the way that they will "permanently" destroy the information.[121] Illinois also requires that the data be destroyed if the purpose for the collection of the data has been fulfilled or three years have passed since the last interaction of the individual with the employer.[122] Texas allows for employers to destroy any biometric data "within a reasonable time," but not until one year after the data is no

---

[118] Ill. Biometric Info. Privacy Act, *supra* note 108.
[119] Tex. Bus. & Com. Code Ann., *supra* note 109.
[120] Wash. H.B., *supra* note 110, at sec. 2.
[121] Ill. Biometric Info. Privacy Act, *supra* note 109.
[122] *Id*. In addition, Illinois requires that business in possession of biometric data have a publicly available, written policy which states their rules regarding the destruction of data.

longer needed.[123] Washington is the most lenient with the requirements as it allows the employers to keep the data "no longer than it is reasonable necessary" to comply with the law.[124]

But what cause of action does plaintiffs have if they felt that their rights were being violated. Although all three states allow for civil damages for organizations that violate the law, Illinois is the only state to allow for a private right of action that allows plaintiffs to sue and recover damages.[125] The statute hold that any person who is "aggrieved by a violation" of BIPA and who can demonstrate that a private entity was negligent with respect to implementing a provision of BIPA may recover for each violation damages of $1,000 or the amount of actual damages, whichever is greater.[126] However, if the entity has been found to intentionally violate the statute, the aggrieved may recover up to $5,000.[127] But recently the court has held that for an aggrieved party to get damages through a violation of the statute, they must allege an actual injury or adverse effect, and not just a technical violation of the statute.[128] Interestingly, Google in an abundance of caution as seemed to disable a new feature in their Arts & Culture app regarding selfies and matching to a museum

---

[123] Tex. Bus. & Com. Code Ann., *supra* note 110.
[124] Wash. H.B., *supra* note 111.
[125] Ill. Biometric Info. Privacy Act, *supra* note 109.
[126] *Id.*
[127] *Id*.
[128] *See Spokeo Inv v. Robins*, 136 S. Ct 1540, (2016) (Holding that the complaints failed to show that the plaintiffs suffered any harm related to BIPA's protections for the collection or sharing of data. The Court held that the harm has to more than just pecuniary).

painting.[129] Google recently updated their Arts & Culture app to compare a selfie to a database of works of art and match the selfie to a painting. Seemingly, Google has disabled such a feature due to the regulations in Illinois and Texas regarding the collection and use of biometric information.[130] Google is facing a class action that alleges that Google Photos, their cloud-based photo sharing system violated BIPA but automatically uploading photos and scanning them to create unique faceprints to tag photos without the users consent.[131] Although the app requires explicit consent before you can take a selfie, it seems that Google is being very careful as they do not want to face a new class action in case this app is in violation as well.

In Washington and Texas, only the State Attorney General can bring a suit to enforce the laws. This is the reason Illinois is at the forefront of the biometric privacy debate, it allows anyone to raise complaints. Furthermore, like the GDPR, all three states prohibit a business from selling the data it collects unless of course an exception applies such as the individual giving consent to the disclosure for instance. The restrictions also apply to third parties that have access to the data.

Recently the courts have gotten involved in interpreting the relevant state statutes. In Vigil v. Take-Two

---

[129] Jeffrey Neuburger, *Google App Disables Art-Selfie Biometric Comparison Tool in Illinois and* Texas, NEW MEDIA AND TECH. LAW Blog (Jan. 18, 2018), https://newmedialaw.proskauer.com/2018/01/18/google-app-disables-art-selfie-biometric-comparison-tool-in-illinois-and-texas/

[130] *Id.*

[131] *Rivera v. Google Inc.*, 338 F. Supp 3d 1088, 1091 (N.D. Ill. 2017) (Google moved to dismiss and the court denied the motion).

Interactive Software[132], the U.S. Court of Appeals for the Second Circuit rejected the privacy claims made under BIPA. This case dealt with the facial scans that the video games like NBA 2K16 used to allow users to create a custom basketball player that has a 3-D model of the gamers face, more commonly known as an "avatar."[133] The avatar is created when the human player uses a camera to scan his face to put it in the game.[134] The video game prompts the gamer to agree to the conditions onscreen which state that "Your face scan will be visible to you and others you play with and may be recorded or screen captured during gameplay."[135] The court concluded that the aggrieved failed to present any material risk that the game companies violations have resulted in the plaintiffs data being used without their consent.[136] In essence, the court said that the plaintiffs have not shown they were injured. BIPA was just a static bill until 2015 when a multiple class action suits were filed alleging that against Facebook and Shutterfly for their use of collecting and storing facial features.[137] Facebook lost its first battle in consolidated class actions claiming the company's Tag Suggestions program

---

[132] *Vigil v. Take-Two Interactive Software, Inc.*, 235 F. Supp. 3d 499, 505 (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).

[133] *Vigil, supra* note 132, at 506.

[134] *Id.*

[135] *Id* at 505.

[136] *Id.* at 516

[137] *See Norberg v. Shutterfly, Inc.,* 152 F. Supp. 3d 1103, 1104 (N.D. Ill. 2015) (where the plaintiff claims' that Shutterfly's collection, and storage of its "face templates" from individuals whose images are submitted to Shutterfly, some of which are not users of the service, violate BIPA's consent requirements).

violates BIPA's notice and consent requirements when it applies facial recognition to uploaded photos.[138]

C. INDIVIDUAL CONTROL OF INFORMATION IN THE US

Unlike the EU, the privacy law in the United States does not give much control to an individual. In some of the regulated sectors, subjects are given limited control over the use of their information. For example, under the Federal Credit Reporting Act (FCRA), individuals can opt out of certain reporting agencies affiliates having access to their information.[139] Unlike the EU which works under an opt-in policy, the US privacy laws rely on the use of individuals opting out instead. However, much like the EU and the GDPR, the law in the US is that organizations must use the information they collect in a way that is consistent with the reasons stated in the privacy notice that one receives.[140] If an organization wants to use the information for a new purpose that was not disclosed nor consistent with the notice, then the companies would be required to obtain a new opt-in notice.[141] Due to the current climate on security regulation from recent data security hacks, many have tried to put some plan in place for a wider adoption of security protection when it comes to

---

[138] *In re Facebook Biometric Information Privacy Litig*., 185 F. Supp. 3d 1155, 1166, 1170-72 (N.D. Cal. 2016).
[139] *See generally* 15 U.S.C. § 1681, et seq (1970).
[140] *How to Comply With the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act*, FEDERAL TRADE COMMISSION (2002), https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm#obligations.
[141] *Id*.

general data security. There are a number of bills currently being proposed in Congress to that effect. One such bill is the Consumer Privacy Protection Act of 2017, S2124, which was introduced by Senator Patrick Leahy (D-VT) in response to the Equifax breach.[142] The bill would put in place safeguards for the protection of sensitive personally identifiable information and impose punitive punishments for the failure to notify consumers in a timely manner of the security breach.[143] What is important about the bill is that it includes a definition of "sensitive personally identifiable information," that is akin to the European definition of "sensitive identifiable information."[144] The definition specifically includes "unique biometric data, such as faceprint, fingerprint, voice print, a retina or iris image, or any other unique physical representation."[145] This is at least a step in the right direction by the Federal Government to try and start to think about regulating biometric information much the same way it does with other types of private information.

IV. CONCLUSION

While the future of biometric privacy is still unclear in most of the states, the laws passed in both the United States and the EU, although they mean well, still have problems when trying to keep up with the evolution of technology. Whether we are considering the law under the proposed

---

[142] Consumer Privacy Protection Act of 2017, § 2124, 115th Cong. (2017).
[143] *Id.* It seems that the idea behind the bill is to start mirroring some aspects of the GDPR by holding companies accountable for their actions and making them pay when they don't follow the rules.
[144] *Id.* at sec. 11.
[145] *Id.*

GDPR or the law in Illinois, they seem to be too broad in scope. The law can expose companies like Google, Facebook, Shutterfly, Twitter and the like to civil liability even when there is no risk to one's data. Biometrics is constantly evolving and the law is unlikely to keep up to achieve its goal. For example, authentication is more than just putting a finger on a scanner, it is more than just an image. Companies are using systems that will make sure that the person is present and living, not just a mere photograph of a person's face. If a burglar really wants to get into your house, a simple door lock will not stop him. The same is true about biometric information, if a criminal wants to get access to your data, they won't be stopped if biometric access can be gained simply from using a photo of a person to request access.[146] Companies are developing systems to protect the personal and sensitive data using new innovations to manage the risks. However, since biometric jurisprudence is still in its infancy in the US and the GDPR has not gone into effect yet, companies employing technologies using biometric identifiers and biometric information should err on the side of caution. Unfortunately, a concern related to biometric data is that the public is becoming desensitized through the widening use of this data. People freely give away biometric data because it is easy or it makes some tasks simpler, and as such do not recognize the data privacy risks that they might be subjected to later in life. Moreover, although companies might make data subjects opt-in to certain programs, it is

[146] Furthermore, in the case of a breach of data relating to a single biometric identifier it is highly unlikely that any company would continue to use either the same identifier or the identifier alone in allowing access to sensitive data.

more than likely that people will accept its usage without being fully informed since it makes life easier.

However, it is still up to the regulators to try and prevent or set rules in place to protect people's private information. For cautious businesses, regulators should even go further and devise an opt-in scheme like the GDPR, rather than the more common opt-out scheme used in the US for your technologies using biometric information. As the wider application of biometrics becomes more clear throughout the world, it will be easier for regulators to focus on what really needs to be done to ensure that the laws are not too broad, and to ensure that laws will address the changing security risks. It is too early to tell what the effects of the GDPR will be until it goes into effect in May 2018. However, for both the EU and the US companies who deal with biometric information, the only thing they can do is watch the developing landscape, err on the side of caution, and ensure that they have adequate consent processes. But at the end of the day, protection of biometric data is up to the end user. The law is simply not ready to discuss the issues surrounding biometrics in the long run, and slowly it will catch up in the next few years when biometrics comes to the forefront of technology. Although biometric systems represent a big step forward, we should realize that it is up to the users to accept it or to not accept it. The way technology is changing, users are more likely to accept these systems without understanding what they mean for their privacy. Although the GDPR, BIPA and its related state laws are a good starting point, only time will tell how biometric data will play a role in the evolution of privacy.