


2020

Consent, Appropriation by Manipulation, and the 10-Year Challenge: How an Internet Meme Complicated Biometric Information Privacy

Michael J. Slobom

Follow this and additional works at: <https://open.mitchellhamline.edu/mhlr>

 Part of the [Privacy Law Commons](#), and the [Science and Technology Law Commons](#)

Recommended Citation

Slobom, Michael J. (2020) "Consent, Appropriation by Manipulation, and the 10-Year Challenge: How an Internet Meme Complicated Biometric Information Privacy," *Mitchell Hamline Law Review*: Vol. 46 : Iss. 5 , Article 5.

Available at: <https://open.mitchellhamline.edu/mhlr/vol46/iss5/5>

This Article is brought to you for free and open access by the Law Reviews and Journals at Mitchell Hamline Open Access. It has been accepted for inclusion in Mitchell Hamline Law Review by an authorized administrator of Mitchell Hamline Open Access. For more information, please contact sean.felhofer@mitchellhamline.edu.

© Mitchell Hamline School of Law

CONSENT, APPROPRIATION BY MANIPULATION, AND THE 10-YEAR CHALLENGE: HOW AN INTERNET MEME COMPLICATED BIOMETRIC INFORMATION PRIVACY

Michael J. Slobom *

ABSTRACT

In 2019, a viral Internet meme called the “10-Year Challenge” flooded social-media newsfeeds, asking users the question: “How hard did aging hit you?” Users responded by sharing side-by-side photographs of themselves from 2009 and 2019 with their followers. While the challenge spread across social-media platforms, commentators began speculating about the challenge’s origins after a writer for Wired magazine published an op-ed questioning whether Facebook used the challenge to train its facial recognition technology. The op-ed argued that the challenge, while seemingly harmless, could provide Facebook with a sufficient dataset to train its facial recognition technology on age progression. While Facebook denied playing a role in generating the challenge, the op-ed poignantly observes the chilling possibility of tech companies using manipulative tactics to compel disclosure of otherwise private information.

This Article examines the potential remedies available to consumers who have been manipulated into surrendering their biometric data. Using the 10-Year Challenge as a test case, this Article assesses the viability of the causes of actions currently available to consumers who have surrendered their biometric data as a result of manipulative, or at least less-than-forthright, data-collection tactics and concludes that neither common-law tort claims nor recently enacted biometric privacy laws at the state level provide adequate protection from campaigns designed to manipulate consumers into surrendering their private information. Congress must address these types of tactics when crafting broader federal privacy legislation; this Article proposes a legislative starting point.

I. INTRODUCTION.....	1153
A. An Overview of Biometrics and Facial Recognition Technology	1157
II. PRIMARY FUNCTIONS OF BIOMETRIC TECHNOLOGY	1158

*J.D., Penn State’s Dickinson Law, 2019. I thank Professor Anne Toomey McKenna for encouraging me to pursue publishing this Article, Olivia Phillips for providing me with helpful feedback, and others who shared their knowledge of biometric technologies with me. Many thanks to Josh Numainville and the editors of the *Mitchell Hamline Law Review* for their editorial assistance. The views expressed in this Article are the author’s own.

<i>A. Identification and Verification</i>	1158
<i>B. Categorization</i>	1161
<i>C. Current Uses and Value of Biometrics</i>	1163
III. THE RIGHT TO PRIVACY.....	1169
<i>A. Origins and Common Law Claims</i>	1169
<i>B. Privacy and the Constitution</i>	1171
1. <i>Early Foundations: Griswold v. Connecticut</i>	1171
2. <i>Katz and Its Progeny</i>	1172
<i>a. The Reasonable-Expectation-of-Privacy Test</i>	1172
<i>b. The Third-Party Doctrine</i>	1174
3. <i>Fourth Amendment Privacy and Advancements in</i> <i>Technology</i>	1175
<i>a. Maryland v. King</i>	1175
<i>b. Birchfield v. North Dakota</i>	1176
<i>i. Breath Test</i>	1177
<i>ii. Blood Draw</i>	1179
<i>c. Carpenter v. United States</i>	1179
<i>i. Distinctions from Public Movement Cases</i>	1182
<i>ii. Carpenter's Application of the Third-Party</i> <i>Doctrine</i>	1184
<i>d. Fourth Amendment Privacy and Advancements in</i> <i>Technology Redux</i>	1186
IV. CURRENT PRIVACY CLAIMS AND BIOMETRIC PRIVACY.....	1189
<i>A. Privacy in Tort</i>	1189
1. <i>Appropriation and Facebook's Facial Recognition</i> <i>Techniques</i>	1190
<i>a. Name or Likeness</i>	1190
<i>b. Commercial or Other Value</i>	1191
<i>c. Use or Benefit</i>	1193
<i>d. Consent</i>	1193
2. <i>Appropriation by Manipulation</i>	1196
<i>B. Biometric Privacy in State Statutory Law</i>	1197
1. <i>Statutory Protections at the State Level</i>	1197
<i>a. Illinois</i>	1197
<i>i. Overview of BIPA</i>	1197
<i>ii. Attacks on BIPA and Recent Litigation</i>	1199
<i>b. Texas</i>	1202
<i>c. Washington</i>	1202
2. <i>Applicability of State Statutes to the 10-Year Challenge</i>	1204
V. PROPOSED SOLUTION.....	1205
VI. CONCLUSION.....	1212

I. INTRODUCTION

Internet memes have emerged as a primary method of communication in the age of social media.¹ Social-media users create and share memes to evoke humor or irony, to spread political messages, and to participate in online challenges, among other purposes.² In January 2019, a new viral meme flooded social-media newsfeeds. What later became known as the “10-Year Challenge” asked social-media users to answer the question “How hard did aging hit you?” by sharing side-by-side photographs of themselves from 2009 and 2019.³ Over 5.2 million users participated in the challenge, with some users providing their audiences with helpful context behind the photos, such as the dates and locations of when and where the photos were taken.⁴

Speculation over the challenge’s origins quickly arose when Kate O’Neill, a writer for *Wired* magazine, published an op-ed questioning whether Facebook engineered the challenge.⁵ O’Neill argued that the challenge, while seemingly harmless, could provide Facebook with a clean dataset sufficient to train its facial recognition technology on age progression:

Imagine that you wanted to train a facial recognition algorithm on age-related characteristics and, more specifically, on age progression (e.g., how people are likely to look as they get older). Ideally, you’d want a broad and rigorous dataset with lots of people’s pictures. It would help if you knew they were taken a fixed number of years apart—say, 10 years.

Sure, you could mine Facebook for profile pictures and look at posting dates or EXIF data. But that whole set of profile pictures could end up generating a lot of useless noise. People don’t reliably upload pictures in chronological order, and it is not

¹ Perry Kostidakis, *The Evolution of Memes*, COMPLEX (Mar. 13, 2019), <https://bit.ly/2D6anMw> [<https://perma.cc/2TNE-V6VF>].

² See *This Is Where Internet Memes Come From*, MIT TECH. REV. (June 11, 2018), <https://bit.ly/349tT75> [<https://perma.cc/YA3D-52VK>] (noting Internet memes have also been used “to spread aggressive or racist messages and to incite hatred”).

³ See Rebecca Jennings, *Why You’re Seeing the 10-Year Challenge Everywhere*, VOX (Jan. 16, 2019), <https://bit.ly/2QStyOp> [<https://perma.cc/2YFJ-GM3R>].

⁴ Nicole Martin, *Was the Facebook ‘10 Year Challenge’ A Way to Mine Data for Facial Recognition AI?*, FORBES (Jan. 17, 2019), <https://bit.ly/2GJSPZZ> [<https://perma.cc/B8R6-J46M>].

⁵ See Kate O’Neill, *Facebook’s ‘10 Year Challenge’ Is Just a Harmless Meme—Right?*, WIRED (Jan. 15, 2019), <https://bit.ly/2CmCK8L> [<https://perma.cc/PDN9-VNT6>].

uncommon for users to post pictures of something other than themselves as a profile picture.⁶

O’Neill’s piece quickly gained traction. Within days, various media outlets, including *NPR*, *The New York Times*, *Forbes*, and *Vox*, also ran pieces questioning Facebook’s use of the challenge.⁷ The *Forbes* piece even quoted one scholar who characterized the challenge as a “perfect storm for machine learning.”⁸

While Facebook denied playing a role in generating the challenge,⁹ O’Neill’s theory does not fall outside the realm of possibility given Facebook’s history of surreptitiously exploiting its users’ data.¹⁰ And even if the challenge was not an attempt at social engineering, O’Neill’s op-ed poignantly observes the chilling possibility of tech companies—such as Facebook with its more than two billion users¹¹—using seemingly harmless campaigns as pretext for compelling the disclosure of otherwise private information.¹²

⁶ *Id.* EXIF stands for Exchangeable Image File Format. EXIF data is information that is recorded and stored within an image file when a photograph is taken and contains details about when, where, and how the photo was taken. See Thomas Germain, *How a Photo’s Hidden ‘Exif’ Data Exposes Your Personal Information*, CONSUMER REP. (Dec. 6, 2019), <https://bit.ly/2XJEJjK> [<https://perma.cc/6EUA-MXS9>]. Critics questioned O’Neill’s premise, arguing that because Facebook already has access to the photos it does not need to manipulate users into re-posting the images. See Kate O’Neill (@kateo), TWITTER (Jan. 13, 2019, 9:46 AM), <https://bit.ly/2DIGphT> [<https://perma.cc/W76Z-NTP2>] (“Most common rebuttal in my mentions: ‘That data is already available. Facebook’s already got all the profile pictures.’”). In response, O’Neill pointed out that many Facebook users do not upload photos immediately after the photos were taken and many users’ profile pictures display images not of themselves, but of cartoons and animals. See Martin, *supra* note 4.

⁷ Amanda Morris, *Could The 10-Year Challenge Be Putting Your Data At Risk?*, NAT’L PUB. RADIO (Jan. 20, 2019), <https://n.pr/2RF4eAJ> [<https://perma.cc/LQC4-8SUZ>]; Jacey Fortin, *Are ‘10-Year Challenge’ Photos a Boon to Facebook’s Facial Recognition Technology?*, N.Y. TIMES (Jan. 19, 2019), <https://nyti.ms/2X4pSgY> [<https://perma.cc/H3ZY-FYUC>]; Martin, *supra* note 4; Jennings, *supra* note 3.

⁸ Martin, *supra* note 4.

⁹ Facebook (@facebook), TWITTER (Jan. 16, 2019, 3:08 PM), <https://bit.ly/2MfytZ4> [<https://perma.cc/JP9C-VUP9>] [hereinafter Facebook Response].

¹⁰ See Elizabeth Dwoskin et al., *Facebook Allegedly Offered Advertisers Special Access to Users’ Data and Activities, According to Documents Released by British Lawmakers*, WASH. POST (Dec. 5, 2018), <https://wapo.st/2X2HI3T> [<https://perma.cc/5LFF-SXKS>] (describing internal Facebook emails that suggest Facebook used users’ data as a bargaining chip to attract advertisers).

¹¹ See Fortin, *supra* note 7.

¹² Similar concerns arose again in July 2019 when FaceApp, an app that can edit photos of people’s faces to show younger or older versions of themselves, went viral. See Thomas Brewster, *FaceApp: Is The Russian Face-Aging App A Danger To Your Privacy?*, FORBES (July 17, 2019), <https://bit.ly/2KRsdag> [<https://perma.cc/PL5G-ER2G>]. While the majority

These concerns underscore the cries of information privacy law scholars for federal legislation recognizing a right to privacy in one's own biometric data.¹³ Biometric identifiers are intrinsic physical and behavioral human characteristics, such as fingerprints, DNA, iris patterns, voice, gait, and facial geometry.¹⁴ Both state and private actors collect and store biometric information in databases designed to assist with identifying or verifying peoples' identities.¹⁵ Facebook, for example, has collected and stored facial biometrics using facial recognition technology since 2010.¹⁶ Facial recognition technology measures the curves of a person's face on a sub-millimeter scale and then matches the measurements to other images stored in a database or on a device.¹⁷ Common measurements include the distance between eyes, width of the nose, depth of the eye sockets, shape of the cheekbones, and length of the jaw line.¹⁸ According to Facebook's Deputy Chief Privacy Officer, Facebook uses the data strictly for improving user experience (i.e., making the "tagging" feature more user friendly, preventing online impersonation, and assisting people with visual

of concerns initially raised proved untrue, FaceApp's viral moment nevertheless demonstrated "how quickly millions of faces could be gathered up for nefarious purposes." Chip Brownlee, *How Worried Should You Be About FaceApp?*, SLATE (July 18, 2019), <https://bit.ly/2qvQXhN> [<https://perma.cc/5C6L-MJL8>].

¹³ See, e.g., Hannah Zimmerman, *The Data of You: Regulating Private Industry's Collection of Biometric Information*, 66 KAN. L. REV. 637, 656-71 (2018); Carra Pope, Note & Comment, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data*, 26 J.L. & POL'Y 769, 797-802 (2018); Yana Welinder, *A Face Tells More than a Thousand Posts: Developing Face Recognition Privacy in Social Networks*, 26 HARV. J.L. & TECH. 165, 197 (2012) ("Federal legislation is more desirable . . ."); Lisa J. McGuire, Comment, *Banking on Biometrics: Your Bank's New High-Tech Method of Identification May Mean Giving Up Your Privacy*, 33 AKRON L. REV. 441, 476-80 (2000).

¹⁴ *Biometrics*, ELECTRONIC FRONTIER FOUND., <https://bit.ly/2TJoUES> [<https://perma.cc/78LW-RJAT>].

¹⁵ See *id.*

¹⁶ See Camila Domonoske, *Facebook Expands Use of Facial Recognition to ID Users in Photos*, NAT'L PUB. RADIO (Dec. 19, 2017), <https://n.pr/2Bmdkdt> [<https://perma.cc/C9UF-NL92>]. In September 2019, Facebook announced that it would no longer automatically collect its users' facial biometrics and would instead turn on its facial recognition technology only when a user opts in. See Srinivas Narayanan, *An Update About Face Recognition on Facebook*, FACEBOOK NEWSROOM (Sept. 3, 2019), <https://bit.ly/2QKyDMv> [<https://perma.cc/TX2T-AHP2>].

¹⁷ See Kevin Bonsor & Ryan Johnson, *How Facial Recognition Systems Work*, HOWSTUFFWORKS, <https://bit.ly/2jqAbZQ> [<https://perma.cc/PL67-NCPT>]; *Facial Recognition*, FIND BIOMETRICS, <https://bit.ly/2t8z5qB> [<https://perma.cc/D6UA-TW48>] [hereinafter *Facial Recognition*]. For a discussion of facial recognition technology, as well as other biometric technology, see *infra* Part I.

¹⁸ Bonsor & Johnson, *supra* note 17.

impairments).¹⁹ Meanwhile, critics have pointed out that Facebook also uses facial recognition “to support its research into artificial technology, which Facebook hopes will lead to new platforms to place more focused targeted ads.”²⁰

While the U.S. government has acknowledged the highly sensitive, private nature of biometric data,²¹ no federal statute currently regulates its collection or use by private actors.²² Thus, absent state statutory protections,²³ consumers are left to resort to common-law claims. Even still, actors who profit from collecting consumers’ biometric data can arguably dodge liability by simply disclosing their data-collection practices in well-drafted terms-of-service agreements²⁴—even when consumers have surrendered their data as a consequence of an actor’s manipulative tactics.²⁵

This Article examines the potential remedies currently available to consumers manipulated into surrendering their biometric data to interested data collectors. Using the 10-Year Challenge as a test case, this Article assesses the viability of the most relevant common-law and statutory causes of actions as well as the state statutory protections that do not afford private rights of action. This Article argues that neither common-law tort claims, nor state biometric privacy laws adequately protect consumers against campaigns designed to manipulate disclosure of biometric information.

¹⁹ See Rob Sherman, *Hard Questions: Should I Be Afraid of Face Recognition Technology?*, FACEBOOK NEWSROOM (Dec. 19, 2017), <https://bit.ly/2AtZq3T> [<https://perma.cc/MTQ2-TCL6>].

²⁰ Jared Bennett, *Saving Face: Facebook Wants Access Without Limits*, CTR. FOR PUB. INTEGRITY (July 31, 2017), <https://bit.ly/2BuTb3a> [<https://perma.cc/CRB8-YX5F>].

²¹ See OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, OMB MEM. NO. 07-16, SAFEGUARDING AGAINST AND RESPONDING TO THE BREACH OF PERSONALLY IDENTIFIABLE INFORMATION 1 n.1 (2007), <https://bit.ly/2I9a8G1> [<https://perma.cc/AVL4-XJDR>] [hereinafter OMB MEMO] (including “biometric records” in the category of “personally identifiable information”).

²² See *Biometric Data and the General Data Protection Regulation*, GEMALTO (Aug. 20, 2018), <https://bit.ly/2SrudI3> [<https://perma.cc/QSK4-7CYE>] [hereinafter *Biometric Data*].

²³ *Id.* Currently, only Illinois, Washington State, and Texas have passed laws regulating the collection of biometric information. Of the three states that have passed such laws, only Illinois provides individuals with the right to sue for damages. Jason P. Stiehl et al., *New Biometric Information Privacy Cases Reveal Breadth of Potential Exposure for Companies*, LEXOLOGY (Mar. 5, 2018), <https://bit.ly/2URU9xu> [<https://perma.cc/9NUU-3MZB>].

²⁴ For instance, Facebook discloses its use of facial recognition technology to create facial recognition templates in its data policy. See *Data Policy*, FACEBOOK, <https://bit.ly/1wYGJjt> [<https://perma.cc/QS6G-399J>]. Agreeing to Facebook’s data policy is a precondition to using Facebook’s products. See *Terms of Service*, FACEBOOK, <https://bit.ly/1mAamz3> [<https://perma.cc/49CR-K3PY>].

²⁵ See *infra* Section III.A.2, III.B.2.

This Article then argues that future federal privacy legislation must address these types of tactics.

Part I of this Article first provides an overview of biometric technologies, including the technologies' primary functions. It then discusses how private entities use biometric technologies and the value of collecting, storing, and distributing individuals' biometric traits.²⁶ Part II overviews the right to privacy, including its origins and the common-law tort claims that emerged therefrom. Part II also provides a brief overview of constitutional privacy protections, focusing primarily on the intersection of Fourth Amendment privacy interests and modern technology. Using the 10-Year Challenge as a test case, Part III assesses the viability of causes of action currently available to consumers who have suffered privacy injuries as a result of private companies' manipulative data-collection tactics, which this Article refers to as "appropriation by manipulation." Section III.A examines the most pertinent privacy tort—appropriation of name or likeness²⁷—and demonstrates how that tort provides an insufficient safeguard against appropriation by manipulation in the biometric-data context. Section III.B briefly overviews existing state biometric privacy statutes and demonstrates how those statutes, in current form, do not adequately protect consumers against appropriation by manipulation in the biometric-data context. Finally, Part IV proposes a starting point for addressing these concerns through broader federal biometric privacy legislation.

A. An Overview of Biometrics and Facial Recognition Technology

"Biometrics" is a term used to refer to either characteristics or processes.²⁸ As characteristics, biometrics refers to a person's "measurable biological (anatomical and physiological) or behavioral aspects . . . that can be used for automated recognition."²⁹ As processes, biometrics refers to

²⁶ This author does not claim to be an expert in biometric technologies. Instead, Part I's overview of biometric technologies is based on research and discussions with people familiar with the technology.

²⁷ Although there is an argument to be made for addressing the applicability of the intrusion upon seclusion tort, see Carmen Aguado, Comment, *Facebook or Face Bank?*, 32 LOY. L.A. ENT. L. REV. 187, 215–16 (2011), it is not sufficiently strong enough to warrant consideration in this Article. The intrusion upon seclusion tort focuses on the "solitude or seclusion of another or his private affairs or concerns." RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1977). By posting photographs to Facebook, users remove information from the private sphere into the public sphere, thus making the information public.

²⁸ NAT'L SCI. & TECH. COUNCIL, *PRIVACY & BIOMETRICS: BUILDING A CONCEPTUAL FOUNDATION* 4 (2006).

²⁹ *Id.*

“automated methods of recognizing an individual based on” those characteristics.³⁰ “Biometric technologies” are the technologies that perform the biometric processes.³¹

II. PRIMARY FUNCTIONS OF BIOMETRIC TECHNOLOGY

A. Identification and Verification

Biometric technologies perform two main functions: identification and verification.³² Biometric identification is the process of comparing an individual’s biometric data to a number of biometric “templates” stored in a database,³³ with the goal of answering the question “Who are you?”³⁴ For instance, Facebook’s now-abolished “Tag Suggestions” feature³⁵ used facial recognition technology to identify its users. The technology first analyzed a single face appearing in a photograph and then compared the facial

³⁰ *Id.*

³¹ See *The Future of Biometric Technology: Convenience or Privacy?*, THOMSON REUTERS (June 2, 2017), <https://tmsnr.rs/2qkpoHt> [<https://perma.cc/VYC6-2F9S>].

³² See NAT’L SCI. & TECH. COUNCIL, *supra* note 28, at 11. In addition to these primary functions, biometric technologies also perform a “categorization” function. See *infra* Section I.A.2. The categorization function is less common.

³³ ARTICLE 29 DATA PROT. WORKING PARTY, OPINION 3/2012 ON DEVELOPMENTS IN BIOMETRIC TECHNOLOGIES 5 (2012), <https://bit.ly/2nzLzbf> [<https://perma.cc/MPT5-2L92>] [hereinafter DPWP MARCH 2012 OPINION]. Identification is referred to as “one-to-many” or “1:N” identification because the single dataset is compared to many different biometric templates linked to many different individuals. See *The Difference Between 1:N, 1:1, and 1:Few and Why It Matters in Patient ID*, RIGHTPATIENT (Sept. 23, 2015), <https://bit.ly/2nxF74y> [<https://perma.cc/EE7M-54KZ>] [hereinafter *The Difference Between 1:N, 1:1, and 1:Few*].

³⁴ See Ian E. Muller, *Identification vs Verification: What’s the Difference?*, VERIDIUM (July 12, 2018), <https://bit.ly/2mFE02H> [<https://perma.cc/6R5X-N7N4>].

³⁵ In September 2019, Facebook announced its plan to replace the Tag Suggestions feature with a broader “face recognition setting.” See Narayanan, *supra* note 16. The Tag Suggestions setting was enabled by default and used facial recognition technology to automatically suggest tagging other users in photos posted to Facebook’s platform. See *id.* The new face recognition setting requires users to “opt in” to Facebook’s use of facial recognition technology and provides additional services. See *id.* In addition, Facebook claims that if a user chooses to disable the face recognition setting, then Facebook will delete that user’s face template from its database. See *What Is the Face Recognition Setting on Facebook and How Does It Work?*, FACEBOOK HELP CTR., <https://bit.ly/37H5eJc> [<https://perma.cc/JK4C-CXS9>] [hereinafter *Facebook Face Recognition*]. Facebook implemented the change after the Federal Trade Commission imposed a \$5 billion fine on the company, citing Facebook’s practice of enabling the Tag Suggestions feature by default while suggesting to consumers that Facebook’s facial recognition technology was opt in. See Blake Montgomery, *Facebook Makes Facial Recognition Opt-In Instead of Automatically Scanning Users’ Faces*, DAILY BEAST (Sept. 3, 2019), <https://bit.ly/2MN2UIh> [<https://perma.cc/2PW8-NMNR>].

biometrics with *all* previously stored facial biometrics to determine the identity associated with the face in the photograph.³⁶

Biometric verification, on the other hand, verifies a person's identity by comparing his or her biometric data with a *single* biometric template stored in a database or on a device.³⁷ Much like a PIN or password, biometric verification is used to answer the question "Are you who you say you are?"³⁸ For instance, Apple's "Touch ID" allows iPhone users to unlock their iPhones and authorize iTunes Store purchases by verifying the users' identities using a fingerprint reader built into the phone's home button.³⁹

A short overview of a typical biometric system's data-collection, data-storage, and data-comparison processes demonstrates how these functions work. Generally, three components of a typical biometric system perform the collection and storage processes:

1. A sensor that *observes* characteristics and *converts* the observations into data that can be stored in electronic form.
2. Signal processing algorithms that perform quality control activities on the collected data and develop [a] *biometric template* [of the subject]
3. A *data storage* component that manages all of the data collected, including data from the initial and all future collections and processing.⁴⁰

By way of example, facial recognition technology uses sensors to capture images of a person's face and identify numerous, distinguishable "landmarks," such as points on the chin, nose, and cheekbones (i.e., the observation phase).⁴¹ After capturing the images, which can be gathered through both 2D images, such as photos and videos, and 3D facial scans,⁴²

³⁶ *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1268 (9th Cir. 2019) (discussing the mechanics of Facebook's Tag Suggestions feature); see also April Glaser, *Facebook Will Tell You How to Turn Off Facial Recognition. Why Wait?*, SLATE (Sept. 3, 2019), <https://bit.ly/2munKlm> [<https://perma.cc/H9YM-CVPR>] ("By recognizing faces and suggesting users tag their friends and themselves in uploaded photos, the company has built what could be the largest name-to-face database in the world."). Although not much information regarding Facebook's new face recognition setting has been made available, the new setting likely uses the same processes, consistent with other facial recognition technology. *Accord* Bonsor & Johnson, *supra* note 17.

³⁷ See DPWP MARCH 2012 OPINION, *supra* note 33, at 6.

³⁸ See Muller, *supra* note 34.

³⁹ See *Use Touch ID on iPhone or iPad*, APPLE, <https://apple.co/1ZVD2Jf> [<https://perma.cc/PSY7-36XM>].

⁴⁰ NAT'L SCI. & TECH. COUNCIL, *supra* note 28, at 4 (emphasis added).

⁴¹ See Bonsor & Johnson, *supra* note 17; Steve Symanovich, *How Does Facial Recognition Work?*, NORTON, <https://nr.tn/2GGM0W7> [<https://perma.cc/4PPN-E2C8>].

⁴² See Bonsor & Johnson, *supra* note 17.

the technology measures various distances between the landmarks (i.e., the conversion phase).⁴³ The system then aggregates those measurements into a numerical code that comprises a person's "faceprint" (i.e., the biometric template component).⁴⁴ The system then stores the subject's faceprint in a database (i.e., the data storage component) that it later accesses to compare with new images.⁴⁵

The identification and verification functions occur at the comparison stage. Generally, two components of a typical biometric system perform the comparison process: (1) "[a] matching algorithm that compares the new biometric template to one or more templates that may already be stored"; and (2) "a decision process (either automated or human-assisted) that uses the results from the matching component to make a system-level decision."⁴⁶ A system verifying a person's identity compares the person's new biometric template to a previously stored biometric template associated with that individual (i.e., a "one-to-one" comparison), while a system that identifies a person compares that person's new biometric template to many previously stored biometric templates associated with many different individuals (i.e., a "one-to-many" comparison).⁴⁷ A match between the new template and the previously stored template completes the identification or verification process.⁴⁸

Today's biometric technologies use various physiological and behavioral characteristics to perform identification and verification processes. The most implemented and studied biometric modalities⁴⁹ are fingerprint, facial, iris, voice, signature, and hand-geometry recognitions.⁵⁰ These modalities nevertheless vary in accuracy and efficiency. For instance, facial recognition is a relatively efficient method of identifying and verifying

⁴³ See *id.*; Symanovich, *supra* note 41.

⁴⁴ Bonsor & Johnson, *supra* note 17; Symanovich, *supra* note 41.

⁴⁵ The process of storing an individual's faceprint in a biometric database for the first time is known as "enrollment." ARTICLE 29 DATA PROT. WORKING PARTY, OPINION 02/2012 ON FACIAL RECOGNITION IN ONLINE AND MOBILE SERVICES 2 (2012), <https://bit.ly/2o7vWrT> [<https://perma.cc/6C7B-EG4U>].

⁴⁶ NAT'L SCI. & TECH. COUNCIL, *supra* note 28, at 4-5.

⁴⁷ *Id.* at 7-10; *The Difference Between 1:N, 1:1, and 1:Few*, *supra* note 33.

⁴⁸ See NAT'L SCI. & TECH. COUNCIL, *supra* note 28, at 4-5.

⁴⁹ The term "biometric modalities" refers to categories of biometric systems based on the biometric trait used to recognize an individual. See *Biometrics - Modalities*, TUTORIALSPPOINT, <https://bit.ly/2N8P56P> [<https://perma.cc/3N6Y-PSK3>]. Biometric modalities fall under three types: physiological, such as fingerprint recognition; behavioral, such as gait or signature recognition; and a combination of both physiological and behavioral, such as voice recognition. *Id.*

⁵⁰ See Danny Thakkar, *Top Five Biometrics: Face, Fingerprint, Iris, Palm and Voice*, BAYOMETRIC, <https://bit.ly/2OKNnq1> [<https://perma.cc/CH94-2H8H>].

individuals, with technologies that allow users to capture the initial image using a standard digital camera even at relatively far distances.⁵¹ However, facial recognition technology has proven to be less accurate than other biometric modalities due to different variables that can corrupt the biometric template (e.g., sunglasses, poor lighting, and low-resolution images).⁵² Iris recognition technology, on the other hand, provides quite accurate results—it can even differentiate two genetically identical individuals.⁵³ Nonetheless, iris recognition also has its limitations. For instance, current iris recognition technology cannot meet its objectives from great distances and requires the subject's cooperation to obtain the data necessary to build the biometric template.⁵⁴

Some biometric systems employ a “multi-modal” approach to cure these accuracy defects.⁵⁵ Multi-modal biometric systems collect multiple biometric traits belonging to a single person and consolidate those results to perform the identification or verification functions.⁵⁶ For instance, a system that combines both facial recognition and fingerprint recognition can be considered a multi-modal biometric system.⁵⁷ By tying more traits to an individual's identity, the system becomes more likely to accurately and efficiently recognize that person.⁵⁸

B. Categorization

Biometric technologies, and facial recognition technologies in particular, have been used increasingly to perform another function: categorization.⁵⁹ The European Union's Data Protection Working Party has

⁵¹ *Id.*

⁵² *Id.*

⁵³ *Id.*

⁵⁴ *Id.* For instance, the subject often must look directly into the camera capturing the iris image. *Id.*

⁵⁵ DPWP MARCH 2012 OPINION, *supra* note 33, at 6, 17; *see also* Waleed Dahea & HS Fadewar, *Multimodal Biometric System: A Review*, 4 INT'L J. RES. ADVANCED ENGINEERING & TECH. 25, 26 (2018). “In addition, multimodal biometric system can effectively deal with a variety of issues such as noisy data, intra-class variations, limited degrees of freedom, non-universality, spoof attacks, and unacceptable error rates which may be caused by unimodal biometric systems.” *See Multimodal Biometrics—A More Accurate Identification System*, IRITECH, INC. (Apr. 30, 2015), <https://bit.ly/2nfTZ4f> [<https://perma.cc/RMR8-7VQU>] [hereinafter *A More Accurate Identification System*].

⁵⁶ Dahea & Fadewar, *supra* note 55, at 26; DPWP MARCH 2012 OPINION, *supra* note 33, at 6.

⁵⁷ *See A More Accurate Identification System*, *supra* note 55.

⁵⁸ *See id.*; Dahea & Fadewar, *supra* note 55, at 26.

⁵⁹ *See* DPWP MARCH 2012 OPINION, *supra* note 33, 5–6; *see also* Derek Hawkins, *Researchers Use Facial Recognition Tools to Predict Sexual Orientation. LGBT Groups*

defined biometric categorization as “the process of establishing whether the biometric data of an individual belongs to a group with some predefined characteristic in order to take a specific action.”⁶⁰ Biometric categorization aims not to identify a person or verify a person’s identity but rather to place biometric data into categories, such as age and gender.⁶¹ The data can then be stored, analyzed, and used to predict whether other people belong in that same category.⁶²

A controversial 2018 study conducted by researchers at Stanford University suggested that facial recognition technology can predict an individual’s sexual orientation more accurately than humans can.⁶³ The researchers fed more than 35,000 photographs of roughly 15,000 self-identified gay and heterosexual men and women into an algorithm that analyzed the subtle differences in the faces appearing in the images.⁶⁴ The researchers then showed photographs of new faces to the software and asked it to predict each person’s sexual orientation.⁶⁵ According to the researchers, the results showed that the software accurately distinguished between gay and heterosexual men eighty-one percent of the time and between gay and heterosexual women seventy-one percent of the time.⁶⁶

Aren’t Happy., WASH. POST (Sept. 12, 2017), <https://wapo.st/2ffzvVC> [<https://perma.cc/QPV6-J4QB>]; Daniel Thomas, *The Cameras that Know if You’re Happy—or a Threat*, BBC (July 17, 2018), <https://bbc.in/2P41MP4> [<https://perma.cc/K3TD-EFHB>].

⁶⁰ DPWP MARCH 2012 OPINION, *supra* note 33, at 6.

⁶¹ *See id.*

⁶² *See id.*; *see also* Hawkins, *supra* note 59; Thomas, *supra* note 59.

⁶³ *See* Yilun Wang & Michal Kosinski, *Deep Neural Networks Are More Accurate Than Humans at Detecting Sexual Orientation from Facial Images*, 114 J. PERSONALITY & SOC. PSYCHOL. 246 (2018). The study faced significant backlash, with some criticizing the study for its methodology, the conclusions that the researchers drew from results, and some of the basic assumptions underlying those conclusions. *See* Jeremy Howard, *Can Neural Nets Detect Sexual Orientation? A Data Scientist’s Perspective*, FAST.AI (Sept. 13, 2017), <https://bit.ly/2JnRtEA> [<https://perma.cc/K5DU-G6S9>]. LGBTQ rights groups also criticized the study, claiming the study was based on “flawed research” and could be used by brutal regimes across the world to persecute people believed to be gay. *See* Drew Anderson, *GLAAD and HRC Call on Stanford University & Responsible Media to Debunk Dangerous & Flawed Report Claiming to Identify LGBTQ People Through Facial Recognition Technology*, GLAAD (Sept. 8, 2017), <https://bit.ly/31UFUuR> [<https://perma.cc/9E2M-G8N5>]. This author expresses no view on the validity of the study but cites the study only to demonstrate the ways in which facial recognition technology has been used to attempt to categorize people.

⁶⁴ Wang & Kosinski, *supra* note 63, at 248–49.

⁶⁵ *Id.*

⁶⁶ *Id.* at 250.

Some biometric technologies have categorized people based on other, less-controversial characteristics.⁶⁷ For instance, some technology companies now claim to possess the ability to detect a person's mood using facial recognition technology.⁶⁸ Market-research agencies have begun using this technology to assess consumers' reactions to television advertisements.⁶⁹ In 2012, Walmart filed a patent application signaling the company's intent to use facial-recognition technology to detect customers' moods.⁷⁰ The Walmart technology would reportedly monitor customers' facial expressions attempting to identify dissatisfied customers at the checkout lines.⁷¹

C. Current Uses and Value of Biometrics

The ever-growing use of biometrics and biometric technology has already begun changing the ways in which society operates. Private companies have begun replacing traditional methods of verification with biometric technologies,⁷² and these shifts come with certain advantages. A person might forget or share a password or PIN, or an unauthorized person might find a key or token and use it to gain access to a person's sensitive information. With biometrics, these problems do not exist: people are unlikely to lose or share fingerprints and, absent significant advances in 3D-

⁶⁷ See, e.g., Mehedi Hassan, *Which Is the Most Reliable Biometric Modality?*, M2SYS BLOG, <https://bit.ly/364rxHK> [<https://perma.cc/7VHM-DQWM>] (discussing biometric technology's unique ability to identify people by observing behavioral and physical attributes); Wang & Kosinski, *supra* note 63 (positing that people lack the ability to detect and interpret certain revealing facial traits that machines can detect and interpret).

⁶⁸ See Thomas, *supra* note 59 (discussing facial recognition technology that is designed to detect dissatisfied customers); George Anderson, *Walmart's Facial Recognition Technology Would Overstep Boundaries*, FORBES (July 27, 2017), <https://bit.ly/33X3HMg> [<https://perma.cc/5FZB-FSUF>] (discussing Walmart's application for a patent on facial recognition technology designed to detect dissatisfied customers). Amazon has touted its facial recognition service, which is part of a larger suite of image-analysis features called Rekognition, for its ability to detect emotions using facial recognition technology and then placing those emotions into several categories, including "happy," "sad," "angry," "surprised," "disgusted," "calm," "confused," and, most recently, "fear." Tom Simonite, *Amazon Says It Can Detect Fear on Your Face. You Scared?*, WIRED (Aug. 18, 2019), <https://bit.ly/2JkdSTs> [<https://perma.cc/SA64-B5EG>].

⁶⁹ See, e.g., Thomas, *supra* note 59.

⁷⁰ See Hayley Peterson, *Walmart Is Developing a Robot that Identifies Unhappy Shoppers*, BUS. INSIDER (July 19, 2017), <https://bit.ly/35VTtFQ> [<https://perma.cc/U5LN-9KBF>].

⁷¹ *Id.*

⁷² See Thakkar, *supra* note 50 ("[Biometric] technology [has] been successfully implemented in various real-life applications such as forensics, government agencies, banking and financial institutions, enterprise identity management and other identification and recognition purposes.").

printing technology, would-be identity thieves are unlikely to duplicate a person's facial geometry.⁷³ Even biometric identification technology provides some advantages. For instance, biometric identification technology has been used to recover missing persons and identify criminal suspects.⁷⁴ Other potential advantages of this type of technology include the arguable benefit of consumer convenience and shoplifting prevention.⁷⁵

But a darker, and perhaps more insidious, side of biometrics exists. Mobile software applications and the tech companies behind them collect massive amounts of information about consumers each day;⁷⁶ online search engines, such as Google, and social-media sites covertly gather and store

⁷³ It should be noted, however, that at least one reporter has used a 3D-printed replica of his own head to successfully unlock several Android phones. See Thomas Brewster, *We Broke into a Bunch of Android Phones with a 3D-Printed Head*, FORBES (Dec. 13, 2019), <https://bit.ly/2JLXzW1> [<https://perma.cc/U2UZ-T2KM>]. The reporter could not break into Apple's iPhone. See *id.*

⁷⁴ See Anthony Cuthbertson, *Indian Police Trace 3,000 Missing Children in Just Four Days Using Facial Recognition Technology*, INDEP. (Apr. 24, 2018), <https://bit.ly/2JjuUAZ> [<https://perma.cc/HQW2-H8K4>]; Jon Schuppe, *How Facial Recognition Became a Routine Policing Tool in America*, NBC NEWS (May 11, 2019), <https://nbcnews.to/2Pjo1n0> [<https://perma.cc/UJ8Y-H9Y6>]. This use of facial recognition technology also has its downsides. For instance, the technology's false-match rates disproportionately impact women and people of color. See Steve Lohr, *Facial Recognition Is Accurate, if You're a White Guy*, N.Y. TIMES (Feb. 9, 2018), <https://nyti.ms/2BZ9Z2d> [<https://perma.cc/64ZL-VLWT>]. The ACLU of Massachusetts recently conducted a test using Amazon's facial recognition technology to determine the technology's accuracy. See *Facial Recognition Technology Falsely Identifies Famous Athletes*, ACLU MASS. (Oct. 21, 2019), <https://bit.ly/2Wb0beB> [<https://perma.cc/MS97-ZUVV>]. According to the ACLU, Amazon's technology mistakenly matched 27 professional athletes' faces to criminal mugshots. See *id.* Some states have begun introducing legislation that would prohibit police from using facial recognition technology in conjunction with body cameras. See Chris Mills Rodrigo, *California Blocks Police Body Cameras from Using Facial Recognition*, HILL (Oct. 9, 2019), <https://bit.ly/2BEJlv5> [<https://perma.cc/65QY-UBPQ>].

⁷⁵ See Leticia Miranda, *Thousands of Stores Will Soon Use Facial Recognition, and They Won't Need Your Consent*, BUZZFEED NEWS (Aug. 17, 2018), <https://bit.ly/2JpEEJS> [<https://perma.cc/YQ5S-3WTY>]; Jeff John Roberts, *Walmart's Use of Sci-fi Tech to Spot Shoplifters Raises Privacy Questions*, FORTUNE (Nov. 9, 2015), <https://bit.ly/3IPYxAm> [<https://perma.cc/6ZCN-R5EF>].

⁷⁶ See Nicole Perlroth & Nick Bilton, *Mobile Apps Take Data Without Permission*, N.Y. TIMES: BITS (Feb. 15, 2012), <https://nyti.ms/2MOg081> [<https://perma.cc/8XFP-9XF8>] ("Companies that make many of the most popular smartphone apps for Apple and Android devices . . . routinely gather the information in personal address books on the phone and in some cases store it on their own computers.").

hundreds of millions of consumers' facial biometrics;⁷⁷ and the motives underlying these practices go beyond consumer convenience.⁷⁸

The federal government currently classifies biometric data as “personally identifiable information” (PII).⁷⁹ PII is loosely defined as any information that can be used to trace a person's identity.⁸⁰ In addition to

⁷⁷ *Cf.* Aguado, *supra* note 27, at 192 (“By 2009, there were more than thirty publicly available databases for facial recognition analysis. Today, applications such as Google's Picasa, Apple iPhoto, Sony's Picture Motion Browser, Windows Live Photo Gallery, and Facebook, all use facial recognition technology.”).

⁷⁸ *See* Anne T. McKenna, *Pass Parallel Privacy Standards or Privacy Perishes*, 65 RUTGERS L. REV. 1041, 1067 (2013) (“[C]ollected, stored, and accessible biometric data provides vast potential for financial gain for international, national, and local private entities.”).

⁷⁹ *See, e.g.*, 2 C.F.R. § 200.82 (2019) (defining “protected” PID); 34 C.F.R. § 99.3 (2019) (defining PII in the education context); 6 C.F.R. § 37.3 (2019) (defining PII in the identification-card context); 41 C.F.R. § 105-64.001 (2019) (defining PII under the General Services Administration rules under the Privacy Act of 1974); *cf.* 6 C.F.R. pt. 5, app. C (71) (2019); *see also* OMB MEMO, *supra* note 21, at 1 n.1 (including “biometric records” in the category of “personally identifiable information”).

⁸⁰ *See, e.g.*, 2 C.F.R. § 200.79 (2019) (“PII means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.”); 32 C.F.R. § 329.3 (2019) (defining PII as “[i]nformation about an individual that identifies, links, relates, or is unique to, or describes him or her . . . [or] which can be used to distinguish or trace an individual's identity which is linked or linkable to a specified individual”). PII is the central concept upon which information privacy law rests. *See* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1816 (2011). The United States' sectoral approach to privacy law has generally focused on privacy protections of information that can be used to link information to a person's identity. In turn, most federal privacy statutes protect narrowly defined classes of PII. *See* Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g(b)(2) (2018) (“No funds shall be made available under any applicable program to any educational agency or institution which has a policy or practice of releasing, or providing access to, any personally identifiable information in education records”); Cable Communications Policy Act, 47 U.S.C. § 551(a)-(b) (requiring cable operators to provide consumers with notice regarding the PII collected and prohibiting collection of PII without prior written consent); Video Privacy Protection Act, 18 U.S.C. § 2710(b)(1) (2018) (“A video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person”); *cf.* Fair Credit Reporting Act, 15 U.S.C. § 1681b(1) (2018) (providing protections relating to “consumer reports,” which the statute defines as “any . . . communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness . . . [or] personal characteristics” when used to establish the consumer's eligibility for credit, insurance, or for other defined purposes). Despite PII's central importance to information privacy, no uniform definition of the term exists in the United States. Shwartz & Solove, *supra*, at 1819. Moreover, the American concept of PII, and the law's reliance on PII for protecting individuals' privacy, has come under attack in recent years, as the digital era has proven that even non-PII can be de-anonymized and transformed into PII. *See id.* at 1816 (“Increasingly,

biometric identifiers, some of the most common examples of PII include a person's name, social security number, date of birth, and address.⁸¹ Ultimately, PII can be used to tie information relating to an otherwise anonymous individual to that individual's identity.⁸² For example, an online retailer might have a record of a user's transaction history. With that record alone, the retailer could not determine who made the purchases in question. But when the record is attached to an address, date of birth, social security number, or name, the retailer can readily determine the identity of the purchaser.⁸³

The value of PII increases demonstrably within the context of the data brokerage industry. While there is no statutory definition for the term "data brokers,"⁸⁴ the Federal Trade Commission has defined the term as follows: "Data brokers are companies that collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information to their customers for various purposes, including verifying an individual's identity, differentiating records, marketing products, and preventing financial fraud."⁸⁵ These entities often

technologists can take information that appears on its face to be non-identifiable and turn it into identifiable data."); Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1704 (2010) ("Today, this debate centers almost entirely on squabbles over magical phrases like 'personally identifiable information' (PII) or 'personal data.' Advances in reidentification expose how thoroughly these phrases miss the point."). In response to a Federal Trade Commission call for comments on privacy issues associated with new technologies and business models, "several consumer and privacy groups elaborated on the privacy concerns associated with supposedly anonymous data and discussed the decreasing relevance of the personally identifiable information ('PII') label." FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 18 (2012), <https://bit.ly/3cD7Blx> [<https://perma.cc/F6NX-DBK7>] [hereinafter FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY].

⁸¹ See, e.g., 2 C.F.R. § 200.82 (2019); 34 C.F.R. § 99.3 (2019); 6 C.F.R. § 37.3 (2019); 41 C.F.R. § 105-64.001 (2019).

⁸² Accord FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY, *supra* note 80, at 18-22.

⁸³ See Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), <https://nyti.ms/2Wf1HfC> [<https://perma.cc/XRM6-9CUY>] (discussing how Target's "Guest ID" links an individual's transaction history and demographic information to the individual's identity).

⁸⁴ STAFF OF S. COMM. ON COMMERCE, SCI. & TRANSP., 113TH CONG., A REVIEW OF THE DATA BROKER INDUSTRY: COLLECTION, USE, AND SALE OF CONSUMER DATA FOR MARKETING PURPOSES 1 (2013) [hereinafter A REVIEW OF THE DATA BROKER INDUSTRY].

⁸⁵ FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY, *supra* note 80, at 68. Data brokers have operated for years. "Long before the advent of the Internet, e-mail, or the mobile economy, data brokers developed expertise in compiling consumer data to facilitate targeted outreach to consumers through direct mail." A REVIEW OF THE DATA BROKER

operate in the shadows, with consumers unaware of the types of information being collected, the methods used to do so, and to whom it is sold.⁸⁶ In fact, the scope of information that data brokers gather is quite broad, largely due to the decisions people now make using the Internet.⁸⁷ Each day, “millions of consumers . . . [use] computers, smart phones, and tablets to make purchases, plan trips, and research personal financial and health questions, among other activities. These digitally recorded decisions provide insights into the consumer’s habits, preferences, and financial and health status.”⁸⁸ With consumers increasingly expanding their digital footprints and technological advances facilitating access to the information generated, data brokers have expanded the types of information they collect, store, and sell.⁸⁹

Data brokers’ customers range from financial lending institutions making credit decisions on a particular borrower to employers making hiring decisions to retailers determining how, and to whom, to target their advertising efforts.⁹⁰ A *New York Times Magazine* profile on the data-broker industry found that retailers can purchase a wide swath of information about consumer habits based on peoples’ online activities, including:

data about your ethnicity, job history, the magazines you read, if you’ve ever declared bankruptcy or got divorced, the year you bought (or lost) your house, where you went to college, what kinds of topics you talk about online, whether you prefer certain brands of coffee, paper towels, cereal or applesauce, your political leanings, reading habits, charitable giving and the number of cars you own.⁹¹

INDUSTRY, *supra* note 84, at 1. However, the data broker industry has grown significantly in the wake of the digital era. *Id.* at 2.

⁸⁶ FED. TRADE COMM’N, PROTECTING CONSUMER PRIVACY, *supra* note 80, at 68.

⁸⁷ A REVIEW OF THE DATA BROKER INDUSTRY, *supra* note 84, at 1-2.

⁸⁸ *Id.* at 2 (footnote omitted).

⁸⁹ *See id.* at 1-2; FED. TRADE COMM’N, PROTECTING CONSUMER PRIVACY, *supra* note 80, at 68.

⁹⁰ A REVIEW OF THE DATA BROKER INDUSTRY, *supra* note 84, at i, 8. Data brokers have a wide range of customers. The types of customers include financial institutions, hotel chains, wireless telephone service providers, cable companies, jewelry stores, and other data brokers and resellers. *Id.* at 29.

⁹¹ Duhigg, *supra* note 83. To aid this effort, data brokers offer “predictive scoring products” that predict a consumer’s behavior. Companies that purchase these products use them to “assess[] which customers will receive special offers, or [to] look[] at credit risks associated with certain mortgage applications.” A REVIEW OF THE DATA BROKER INDUSTRY, *supra* note 84, at 8.

Those retailers then analyze the data both to better market products to consumers and to predict how consumers will behave in the future.⁹²

The data collected and sold by data brokers would be meaningless without the links that PII provides. PII provides data brokers and interested data collectors with the identities behind online activities.⁹³ A search query or online purchase may be linked to an IP address; that IP address is linked to a name, email address, or street address; and that name or address is linked to the consumer. Armed with this information, retailers can analyze the information connected to a consumer's identity and then determine how to capitalize on what they know about that person.

Biometrics exacerbates the concerns associated with these practices. Consider the Walmart patent application discussed above.⁹⁴ Theoretically, Walmart could use the same technology to instantaneously determine each customer's preferences by using facial biometrics to access the customer's purchase history and then use that information to provide targeted ads or coupons at point of sale.⁹⁵ Indeed, some retailers have already begun using facial recognition technology for that very purpose, surveilling and tracking consumers from the moment they walk into the store.⁹⁶ And while social

⁹² Duhigg, *supra* note 83; *see also* A REVIEW OF THE DATA BROKER INDUSTRY, *supra* note 84, at 8, 12-13. This information is gathered from a range of data, including consumers' purchase and transaction information and social-media activity. *See* A REVIEW OF THE DATA BROKER INDUSTRY, *supra* note 84, at 13-14. Data brokers gather this information from a range of sources, including "government records and other public data; purchase or license from other data collectors; cooperative agreements with other companies; self-report by consumers, often through surveys, questionnaires, and sweepstakes; and social media." A REVIEW OF THE DATA BROKER INDUSTRY, *supra* note 84, at 15.

⁹³ *See* Duhigg, *supra* note 83.

⁹⁴ *See supra* notes 70-71 and accompanying text.

⁹⁵ The Federal Trade Commission has raised similar concerns:

In the future, digital signs and kiosks placed in supermarkets, transit stations, and college campuses could capture images of viewers and, through the use of facial recognition software, match those faces to online identities, and return advertisements based on the websites specific individuals have visited or the publicly available information contained in their social media profiles. Retailers could also implement loyalty programs, ask users to associate a photo with the account, then use the combined data to link the consumer to other online accounts or their in-store actions. This would enable the retailer to glean information about the consumer's purchase habits, interests, and even movements, which could be used to offer discounts on particular products or otherwise market to the consumer.

FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY, *supra* note 80, at 45.

⁹⁶ *See* Miranda, *supra* note 75; Nick Tabor, *Smile! The Secretive Business of Facial-Recognition Software in Retail Stores*, INTELLIGENCER (Oct. 20, 2018), <https://nym.ag/2Wgo709> [<https://perma.cc/LD6L-TZWR>]. Many retailers use this technology for security purposes. For instance, the facial recognition software in many retail stores captures images of customers' faces and compares the scanned images against a database of known shoplifters. *See* Miranda, *supra* note 75. The cameras used to capture

security numbers can be changed, email accounts deleted, and birth records sealed, it is much more difficult, if not impossible, to discard and replace a person's fingerprints, facial landmarks, or iris patterns. Biometrics can, therefore, provide the inescapable means by which private entities can trace limitless personal information back to a consumer in real time, regardless of whether the consumer knows it is happening.

III. THE RIGHT TO PRIVACY

The right to privacy stands as a pillar of individual liberty that intersects with many distinct aspects of American jurisprudence. As a constitutional right, the right to privacy prohibits the government from unreasonably intruding into one's private affairs.⁹⁷ Outside the constitutional context, the right protects against private actors who encroach on one's ability to be left alone. This section provides a brief overview of the right to privacy's origins, the common-law tort claims that emerged therefrom, and the Supreme Court's endeavors to parse Fourth Amendment privacy interests within the context of modern technology.

A. *Origins and Common Law Claims*

In 1890, Samuel Warren and Louis Brandeis published the seminal article *The Right to Privacy*,⁹⁸ which has been widely credited as the catalyst for American privacy law.⁹⁹ The article opens with an acknowledgement of

the images are not only the security cameras placed near ceilings but also cameras stored inside digital signs and kiosks. *See* Tabor, *supra*. The latter type of camera has been used to determine whether customers are paying attention to advertisements. *Id.* The advent of "smart shelves" may further the capabilities of this technology. Smart shelves are expected to replace current supermarket shelves and, more importantly, the labels that appear on them. Instead of the normal paper label containing information about a product's price, smart shelves will be equipped with sensors that interact with customers' mobile devices. *See* Lana Bandoim, *How Smart Shelf Technology Will Change Your Supermarket*, FORBES (Dec. 23, 2018), <https://bit.ly/2pPTkLv> [<https://perma.cc/X6U7-7G9G>]. The technology will sift through the information associated with that individual—including his or her purchasing habits, Internet search history, and demographic information—and create personalized advertisements that immediately appear on a screen on the shelf. *See id.* It would not be far-fetched to imagine smart-shelf technology employing facial recognition technology to perform the same tasks and, in turn, produce far more efficient and detailed results.

⁹⁷ *See* *Griswold v. Connecticut*, 381 U.S. 479 (1965) (identifying a constitutionally protected right to privacy).

⁹⁸ Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

⁹⁹ *See* Benjamin E. Bratman, *Brandeis and Warren's The Right to Privacy and the Birth of the Right to Privacy*, 69 TENN. L. REV. 623 (2002) (crediting *The Right to Privacy* as the

the common law's ability to progress and "grow[] to meet the demands of society."¹⁰⁰ Warren and Brandeis set forth several historic instances in which common-law rights have evolved with societal change to protect the underlying interests attached to those rights.¹⁰¹

Citing "[r]ecent inventions and business methods," Warren and Brandeis argued that recent societal developments necessitated new legal recognitions to preserve the "protection of the person"—namely, the recognition of the "right 'to be left alone.'"¹⁰² The "right to privacy," they argued, did not constitute a *new* right but rather an unspoken protection preserved by then-existing sources of law.¹⁰³ And like most rights, they found, the right to privacy was not absolute.¹⁰⁴ Warren and Brandeis outlined six limitations to the right, which included—importantly for this Article—the right's cessation upon the rightholder's publication of private facts or consent thereto.¹⁰⁵

The right to privacy quickly gained traction, with Georgia becoming the first state to recognize a common-law cause of action for invasion of privacy in 1905.¹⁰⁶ Today, most states recognize four torts that collectively comprise the "invasion of privacy" cause of action:¹⁰⁷ (1) intrusion upon

motivating force behind the recognition of the right to privacy by several state courts and state legislatures).

¹⁰⁰ Warren & Brandeis, *supra* note 98, at 193.

¹⁰¹ *Id.* at 193–95.

¹⁰² *Id.* at 195.

¹⁰³ *Id.* at 205–06. As Warren and Brandeis note:

These considerations lead to the conclusion that the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone. It is like the right not to be assaulted or beaten, the right not to be imprisoned, the right not to be maliciously prosecuted, the right not to be defamed. In each of these rights, as indeed in all other rights recognized by the law, there inheres the quality of being owned or possessed—and (as that is the distinguishing attribute of property) there may be some propriety in speaking of those rights as property. But, obviously, they bear little resemblance to what is ordinarily comprehended under that term. The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality.

Id. at 205 (footnote omitted).

¹⁰⁴ *See id.* at 214 (contemplating limitations to the right to privacy).

¹⁰⁵ *See id.* at 218.

¹⁰⁶ DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 12 (6th ed. 2018); *see also* Pavesich v. New England Life Ins. Co., 50 S.E. 68, 81 (Ga. 1905) ("So thoroughly satisfied are we that the law recognizes within proper limits, as a legal right, the right of privacy . . . that we venture to predict that the day will come when the American bar will marvel that a contrary view was ever entertained . . .").

¹⁰⁷ SOLOVE & SCHWARTZ, *supra* note 106, at 28.

seclusion;¹⁰⁸ (2) public disclosure of private facts;¹⁰⁹ (3) false light;¹¹⁰ and (4) appropriation of name or likeness.¹¹¹ Scholars attribute this four-tort conception to William Prosser,¹¹² whose article *Privacy*¹¹³ provided the first attempt to describe invasion of privacy in tort law. In Prosser's view, which later informed the *Restatement (Second) of Torts*' approach,¹¹⁴ privacy torts protect against a narrow class of harm that includes mental harm and distress,¹¹⁵ reputational harm,¹¹⁶ and proprietary harm.¹¹⁷

Prosser's four-tort conception persists today, as courts continue to limit their recognition of privacy-tort claims to the four torts enumerated in Prosser's article and the narrow interests those torts purportedly protect.¹¹⁸ Some scholars argue that this limited approach to the right to privacy has lost touch with the times,¹¹⁹ explaining that such a confined view of the protected interests fails to account for modern technology and therefore leaves many injuries unremedied.¹²⁰

B. Privacy and the Constitution

1. Early Foundations: *Griswold v. Connecticut*

While the U.S. Constitution does not explicitly reference a right to privacy, the Supreme Court has nevertheless found the right's subsistence through other constitutional guarantees. *Griswold v. Connecticut*¹²¹ marked the Court's first express recognition of a constitutionally protected privacy

¹⁰⁸ See RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1977).

¹⁰⁹ See *id.* § 652D.

¹¹⁰ See *id.* § 652E.

¹¹¹ See *id.* § 652C.

¹¹² See, e.g., Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1809 (2010).

¹¹³ William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383 (1960).

¹¹⁴ See RESTATEMENT (SECOND) OF TORTS §§ 652C–652E.

¹¹⁵ See Prosser, *supra* note 113, at 392 (concluding intrusion upon seclusion protects a “mental” interest).

¹¹⁶ See *id.* at 398 (finding the public disclosure of private facts tort protects “reputation” interests); see also *id.* at 400 (positing the false light tort protects “reputation” interests).

¹¹⁷ See *id.* at 406 (concluding the tort of appropriation protects “proprietary” interests more than “mental” interests).

¹¹⁸ Citron, *supra* note 112, at 1824 (“Prosser’s privacy taxonomy now permeates case law.”). For a discussion of the elements comprising the appropriation of name or likeness tort, see *infra* Section III.A.1.

¹¹⁹ See Citron, *supra* note 112, at 1824–31.

¹²⁰ See *id.*

¹²¹ *Griswold v. Connecticut*, 381 U.S. 479 (1965).

right.¹²² *Griswold* involved a state law that criminalized both the use and prescription of contraception methods.¹²³ The Court, by a 7-to-2 vote, invalidated the law on the grounds that the law unconstitutionally intruded on the “privacy surrounding the marriage relationship.”¹²⁴ Writing for the majority, Justice Douglas explained that although the Constitution does not explicitly protect an individual’s privacy, the express protections contained in the Bill of Rights create “zones of privacy” that are necessary to ensure the Constitution’s explicit protections.¹²⁵ The First Amendment, Justice Douglas explained, protects privacy in group association; the Third Amendment in one’s home; the Fifth Amendment’s Self-Incrimination Clause in one’s personal information.¹²⁶ Justice Douglas also observed the protections contained in the Fourth Amendment, suggesting a right to privacy in one’s person, houses, papers, and effects;¹²⁷ and in the Ninth Amendment, suggesting privacy protections in areas not specifically addressed in the other amendments.¹²⁸

2. *Katz and Its Progeny*

a. *The Reasonable-Expectation-of-Privacy Test*

The Supreme Court’s Fourth Amendment jurisprudence provides the most robust probe into the constitutional protections of privacy rights. Two years after *Griswold*, the Court decided *Katz v. United States*,¹²⁹ which set forth the modern test for analyzing the Fourth Amendment’s applicability to privacy interests. The “reasonable expectation of privacy test,” articulated in Justice Harlan’s concurring opinion, provides the standard by which

¹²² See Arthur E. Brooks, *Doe and Dronenburg: Sodomy Statutes Are Constitutional*, 26 WM. & MARY L. REV. 645, 662 (1985) (noting *Griswold* was the “first major privacy decision.”).

¹²³ See *Griswold*, 381 U.S. at 480.

¹²⁴ *Id.* at 485–86 (“Would we allow the police to search the sacred precincts of marital bedrooms for telltale signs of the use of contraceptives? The very idea is repulsive to the notions of privacy surrounding the marriage relationship.”).

¹²⁵ *Id.* at 484 (“[S]pecific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create zones of privacy.” (citation omitted)).

¹²⁶ *Id.*

¹²⁷ *Id.* In pertinent part, the Fourth Amendment provides: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.” U.S. CONST. amend. IV.

¹²⁸ *Griswold*, 381 U.S. at 484. The Ninth Amendment provides: “The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.” U.S. CONST. amend. IX.

¹²⁹ *Katz v. United States*, 389 U.S. 347 (1967).

courts determine whether a “search” occurred within the meaning of the Fourth Amendment.¹³⁰ Under the test, a search occurs when the government violates a person’s “reasonable expectation of privacy.”¹³¹ A violation occurs if: (1) the person had an “actual (subjective) expectation of privacy”; and (2) the expectation is “one that society is prepared to recognize as ‘reasonable.’”¹³² Thus, a person’s reasonable expectation of privacy is determined by a combination of subjective and objective inquiries.

Since *Katz*, the Court has routinely applied the reasonable-expectation-of-privacy test to determine the Fourth Amendment’s applicability to government conduct. On the one hand, the Court has found a reasonable expectation of privacy in one’s home¹³³ and its curtilage,¹³⁴ a lawfully possessed rental vehicle,¹³⁵ the contents of a passenger bag¹³⁶ or suitcase;¹³⁷ the results of a diagnostic urine sample;¹³⁸ and the contents of films.¹³⁹ On the other hand, the Court has found no reasonable expectation of privacy in a vehicle in which a person has no ownership or possessory

¹³⁰ *See id.* at 361 (Harlan, J., concurring) (setting forth a two-prong test for assessing the Fourth Amendment’s application).

¹³¹ *See id.* at 360 (Harlan, J., concurring) (“I join the opinion of the Court, which I read to hold only . . . that an enclosed telephone booth is an area where, like a home and unlike a field, a person has a constitutionally protected reasonable expectation of privacy . . .” (citations omitted)).

¹³² *Id.* at 361.

¹³³ *Steagald v. United States*, 451 U.S. 204, 213–14 (1981) (holding the Fourth Amendment requires a judicial determination of probable cause before police may search a home without a search warrant); *Payton v. New York*, 445 U.S. 573, 589 (1980) (stating the zone of privacy is most clearly defined by the “unambiguous physical dimensions of an individual’s home”).

¹³⁴ *Florida v. Jardines*, 569 U.S. 1, 6–7 (2013) (“We therefore regard the area ‘immediately surrounding and associated with the home’—what our cases call the curtilage—as ‘part of the home itself for Fourth Amendment purposes.’” (quoting *Oliver v. United States*, 466 U.S. 170, 180 (1984))).

¹³⁵ *Byrd v. United States*, 138 S. Ct. 1518, 1524 (2018) (holding as a general rule a person in lawful possession of a rental car has a reasonable expectation of privacy even if that person is not listed on the rental agreement).

¹³⁶ *Bond v. United States*, 529 U.S. 334, 339 (2000) (holding the Fourth Amendment protects a traveler’s carry-on bag from unreasonable physical manipulation).

¹³⁷ *Arkansas v. Sanders*, 442 U.S. 753, 766 (1979) (holding the Fourth Amendment’s warrant requirement applies to personal luggage taken from a vehicle).

¹³⁸ *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (“The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent.”).

¹³⁹ *Walter v. United States*, 447 U.S. 649, 654 (1980) (“[T]he unauthorized exhibition of the films constituted an unreasonable invasion of their owner’s constitutionally protected interest in privacy.”).

interest;¹⁴⁰ the numbers dialed from a telephone;¹⁴¹ open fields;¹⁴² plainly observable areas of one's yard, including those observable by aerial surveillance;¹⁴³ and trash left for collection.¹⁴⁴

b. The Third-Party Doctrine

Under the “third-party doctrine,” individuals possess no reasonable expectation of privacy in information they voluntarily convey to a third party, “even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.”¹⁴⁵ In *United States v. Miller*,¹⁴⁶ the Court held that a bank depositor did not maintain a reasonable expectation of privacy in financial information voluntarily conveyed to a bank in the ordinary course of business.¹⁴⁷ The Court found that because the depositor assumed the risk that the bank would reveal his information to the Government, he could not reasonably expect that information to remain private.¹⁴⁸

The Court reaffirmed its holding in *Miller* three years later in *Smith v. Maryland*,¹⁴⁹ where the Court found a person had no reasonable expectation of privacy in the phone numbers he dialed because he voluntarily conveyed those numbers to the phone company by using the phone. Citing *Miller*, the Court in *Smith* found the defendant assumed the risk that the telephone company would reveal the call-log information to the police.¹⁵⁰ The Court found that the defendant's privacy claim fell flat under the objective prong

¹⁴⁰ *Rakas v. Illinois*, 439 U.S. 128, 148-49 (1978) (holding Petitioners' claims failed because they “made no showing that they had any legitimate expectation of privacy in the glove compartment or area under the seat of the car in which they were merely passengers”).

¹⁴¹ *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979) (stating a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties).

¹⁴² *Oliver v. United States*, 466 U.S. 170, 178 (1984) (“[A]n individual may not legitimately demand privacy for activities conducted out of doors in fields, except in the area immediately surrounding the home.”).

¹⁴³ *Florida v. Riley*, 488 U.S. 445, 449-51 (1989) (holding the Fourth Amendment was not violated when police view from an aircraft revealed marijuana growing on the defendant's property); *California v. Ciraolo*, 476 U.S. 207, 215 (1986) (holding the Fourth Amendment does not require law enforcement traveling in public airways to get a warrant to see what is visible with the naked eye).

¹⁴⁴ *California v. Greenwood*, 486 U.S. 35, 40-41 (1988) (stating exposing garbage to the public by placing it on the curb defeats any Fourth Amendment protection).

¹⁴⁵ *United States v. Miller*, 425 U.S. 435, 443 (1976); see also *Smith*, 442 U.S. at 743-46.

¹⁴⁶ *Miller*, 425 U.S. at 442-43.

¹⁴⁷ *Id.*

¹⁴⁸ *Id.* at 443.

¹⁴⁹ *Smith*, 442 U.S. at 744-75.

¹⁵⁰ *Id.*

of the *Katz* test because, in part, the public knows the telephone company's facilities are capable of tracking and storing the phone numbers a person dials.¹⁵¹

3. *Fourth Amendment Privacy and Advancements in Technology*

In recent years, rapid advancements in technology have challenged the Fourth Amendment's precepts. Certain technological advancements provide new means for collecting and storing information; others make new types of information available. Accordingly, the Court has been forced to grapple with privacy concerns implicated in not only the methods of collection but also the types of information collected. This section briefly overviews three cases in which the Court was forced to confront these issues.

a. *Maryland v. King*

In *Maryland v. King*,¹⁵² the Court held that using a cheek swab to take and analyze an arrestee's DNA for identification purposes following a lawful arrest does not violate the Fourth Amendment.¹⁵³ While the Court acknowledged that using a cheek swab to obtain a DNA sample constitutes a search,¹⁵⁴ the Court found that the circumstances of the case—namely, the swab was conducted incident to arrest and the sample was used strictly for identification purposes—rendered the search reasonable.¹⁵⁵ Importantly, the Court acknowledged that the lawfulness of performing such a search on the average citizen fell outside the scope of the Court's opinion “because unlike the search of a citizen who has not been suspected of a wrong, a detainee has a reduced expectation of privacy.”¹⁵⁶

The Court paid little attention to the type of information gathered but instead focused on the method by which the police gathered the DNA information.¹⁵⁷ The Court observed that the cheek swab at issue “involve[d]

¹⁵¹ *Id.* at 742 (“All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial”).

¹⁵² *Maryland v. King*, 569 U.S. 435 (2013).

¹⁵³ *See id.* at 465–66 (“When officers make an arrest supported by probable cause . . . , taking and analyzing a cheek swab of the arrestee's DNA is, like fingerprinting and photographing, a legitimate police booking procedure that is reasonable under the Fourth Amendment.”).

¹⁵⁴ *See id.* at 446 (“It can be agreed that using a buccal swab on the inner tissues of a person's cheek in order to obtain DNA samples is a search.”).

¹⁵⁵ *See id.* at 461–65. The Fourth Amendment only protects against “*unreasonable* searches and seizures.” U.S. CONST. amend. IV (emphasis added).

¹⁵⁶ *King*, 569 U.S. at 463.

¹⁵⁷ *See id.* at 463–64 (“[A] buccal swab involves an even more brief and still minimal intrusion. A gentle rub along the inside of the cheek does not break the skin, and it ‘involves virtually no risk, trauma, or pain.’”).

an even more brief and still minimal intrusion” than other approved incident-to-arrest search procedures.¹⁵⁸ While the Court acknowledged early in the opinion that DNA samples can reveal significant information about a person,¹⁵⁹ it found the Maryland statute, which authorized such searches, provided adequate safeguards against police misuse such that the authorized procedures did “not amount to a significant invasion of privacy.”¹⁶⁰

b. Birchfield v. North Dakota

Issues of privacy and the Government’s use of technology confronted the Court again in 2016. *Birchfield v. North Dakota*¹⁶¹ asked the Court to decide whether so-called “implied consent laws” violated the Fourth Amendment’s prohibition on unreasonable searches.¹⁶² In an effort to combat drunk driving, states enacted implied consent laws requiring drivers suspected of drunk driving to submit to blood-alcohol-concentration (BAC) tests.¹⁶³ These laws provide that drivers impliedly consent to BAC testing by driving on public roads.¹⁶⁴ The laws at issue in *Birchfield*, however, made it a crime to refuse to submit to a BAC test after being lawfully arrested for impaired driving.¹⁶⁵

Birchfield involved three separate cases of individuals from different states who refused to submit to BAC testing. The disposition of each case turned on the type of BAC testing at issue: breath test or blood draw. In the case of Danny Birchfield, Birchfield was criminally prosecuted under North Dakota law for, and ultimately pleaded guilty to, refusing to submit to a blood draw following his arrest for driving while impaired.¹⁶⁶ Robert Bernard, Jr. was criminally prosecuted under Minnesota law for refusing to

¹⁵⁸ *Id.* at 463–64.

¹⁵⁹ *Id.* at 442–43.

¹⁶⁰ *Id.* at 464–65. Specifically, the Court referenced statutory language that barred government officials from using the DNA samples “for information that does not relate to the identification of individuals.” *Id.* at 465 (quoting MD. CODE ANN., PUB. SAFETY § 2-512(c) (LexisNexis 2019)). The Court also noted earlier in the decision that the statute also prohibits “[t]ests for familial matches.” *Id.* at 444 (citing MD. CODE ANN., PUB. SAFETY § 2-506(d) (LexisNexis 2019)).

¹⁶¹ *Birchfield v. North Dakota*, 136 S. Ct. 2160 (2016).

¹⁶² *Id.* at 2166–67.

¹⁶³ *Id.*

¹⁶⁴ See Robert B. Voas et al., *Implied-Consent Laws: A Review of the Literature and Examination of Current Problems and Related Statutes*, 40 J. SAFETY RES. 77, 79 (2009) (“[I]mplied-consent laws [are] based on the principle that driving is a privilege, not a right, and in accepting a drivers license, an individual is deemed to have given consent to a chemical test.” (citation omitted)).

¹⁶⁵ *Birchfield*, 136 S. Ct. at 2170–72.

¹⁶⁶ *Id.* at 2170–71.

submit to a breath test following his arrest for driving under the influence, but the state trial court dismissed the charge, finding the Fourth Amendment prohibited the warrantless breath test.¹⁶⁷ Finally, Steve Michael Beylund's driver's license was suspended in an administrative proceeding after he submitted to a blood test.¹⁶⁸ Beylund's submission to the blood test came after a police officer told Beylund that North Dakota law required his submission.¹⁶⁹ The North Dakota Supreme Court found Beylund voluntarily consented to the blood draw and therefore affirmed the suspension.¹⁷⁰

Because the testing in each case occurred after a lawful arrest, the Court constructed its analytical framework around the "search-incident-to-arrest" doctrine,¹⁷¹ which categorically permits police officers to search, without a warrant, the person and surrounding area of an arrestee following a lawful arrest.¹⁷² The justification for the exception to the warrant requirement is based on officer safety and preservation of evidence.¹⁷³ After canvassing the history of the exception, the Court acknowledged that BAC testing, while not an entirely "new" phenomenon, was not contemplated in the Founding era; accordingly, the Court examined the specific BAC testing methods at issue, balancing the "degree to which it intrudes upon an individual's privacy and . . . the degree to which it is needed for the promotion of legitimate governmental interests."¹⁷⁴

i. Breath Test

The Court found binding precedent permitted the breath tests, stating, "Years ago we said that breath tests do not 'implicat[e] significant privacy concerns.' That remains so today."¹⁷⁵ Acknowledging the diminished

¹⁶⁷ *Id.* at 2171.

¹⁶⁸ *Id.* at 2171–72.

¹⁶⁹ *Id.* at 2172.

¹⁷⁰ *Id.*

¹⁷¹ *Id.* at 2174 ("In the three cases now before us, the drivers were searched or told that they were required to submit to a search after being placed under arrest for drunk driving. We therefore consider how the search-incident-to-arrest doctrine applies to breath and blood tests incident to such arrests.").

¹⁷² *See id.* at 2179 ("[T]he legality of a search incident to arrest must be judged on the basis of categorical rules.").

¹⁷³ *See id.* at 2176 ("The authority to search the person incident to a lawful custodial arrest, while based upon the need to disarm and to discover evidence, does not depend on what a court may later decide was the probability in a particular arrest situation . . ." (quoting *United States v. Robinson*, 414 U. S. 218, 235 (1973))).

¹⁷⁴ *Id.* at 2174–76 (quoting *Riley v. California*, 573 U.S. 373, 385 (2014)).

¹⁷⁵ *Id.* at 2176 (quoting *Skinner v. R Labor Executives' Ass'n*, 489 U.S. 602, 626 (1989)) (citation omitted).

expectation of privacy one holds following an arrest,¹⁷⁶ the Court based its reasoning on three grounds. First, breath tests do not involve significant *physical* intrusion. The breath test at issue in Bernard's case, the Court explained, lasted for a short time and involved no pain.¹⁷⁷ And while the breath test required a sample of "deep lung" air,¹⁷⁸ the Court found that humans have never asserted a "possessory interest in or any emotional attachment to *any* of the air in their lungs."¹⁷⁹

Second, the Court found that breath tests reveal only negligible information about the test's subject. Contrasting the information obtained through breath tests in this case—"the amount of alcohol in the subject's breath"¹⁸⁰—with the information obtained through the cheek swab in *King*—the subject's DNA—the Court found that breath tests involve only minimal revelations about persons subjected to such tests.¹⁸¹ Importantly, however, this comparison seemingly reinforces the narrowness of the holding in *King*: post-arrest cheek swabs, for *identification* purposes only, do not run afoul of the Fourth Amendment.¹⁸²

Finally, the Court found that breath tests do not exacerbate the inherent embarrassment of an arrest. Noting that breath tests are usually administered in "private," the Court found blowing into a straw for several seconds is not inherently embarrassing.¹⁸³

Following an assessment of the Government's interest in public safety, the Court ultimately concluded that the Fourth Amendment does not

¹⁷⁶ *See id.* at 2177 ("Moreover, once placed under arrest, the individual's expectation of privacy is necessarily diminished.").

¹⁷⁷ *Id.*

¹⁷⁸ Typically, there is more alcohol present in the deeper portions of the lungs (i.e., the "alveolar sacs") than in other portions of the lung. *See State v. Brayman*, 751 P.2d 294, 297 (Wash. 1988). Thus, most breath test machines are designed to test the last portion of a person's breath. *Id.*

¹⁷⁹ *Birchfield*, 136 S. Ct. at 2177.

¹⁸⁰ *Id.*

¹⁸¹ *Id.*

¹⁸² *See id.* The Court explained:

[Breath tests] contrast sharply with the sample of cells collected by the swab in *Maryland v. King*. Although the DNA obtained under the law at issue in that case could lawfully be used only for identification purposes, the process put into the possession of law enforcement authorities a sample from which a wealth of additional, highly personal information could potentially be obtained. A breath test, by contrast, results in a BAC reading on a machine, nothing more. No sample of anything is left in the possession of the police.

Id. (citation omitted).

¹⁸³ *See id.*

require police to obtain a warrant before conducting a breath test incident to arrest.¹⁸⁴

ii. Blood Draw

The Court found important distinctions between blood draws and breath tests that rendered warrantless blood draws unreasonable. Examining blood-draw procedures, the court found that blood draws implicate significant privacy interests for two reasons. First, unlike breath tests, blood draws require a physical intrusion into the subject's body by piercing of the skin.¹⁸⁵ Second, and unlike the finding in *King*, the Court found the potential for misuse raised grave concerns.¹⁸⁶ Specifically, the Court found that preserved blood samples can reveal information about a person beyond the levels of alcohol contained in the subject's blood.¹⁸⁷ And even if police were precluded from using the sample for other purposes, the Court noted, "the potential [for misuse] remains and may result in anxiety for the person tested."¹⁸⁸

On balance, the Court found, the privacy interests at stake in blood-draw cases outweigh states' interests in public safety.¹⁸⁹ Thus, the Court concluded, a warrantless blood draw performed incident to arrest violates the Fourth Amendment.¹⁹⁰

c. Carpenter v. United States

The Court's most recent opportunity to address modern technology's implications on Fourth Amendment privacy arose in *Carpenter v. United States*.¹⁹¹ In June 2018, the Court issued its decision in *Carpenter*, which held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through" cell-site location information (CSLI).¹⁹² CSLI refers to time-stamped location records

¹⁸⁴ *See id.* at 2184.

¹⁸⁵ *See id.* at 2178.

¹⁸⁶ *See id.*

¹⁸⁷ *See id.*

¹⁸⁸ *Id.*

¹⁸⁹ *See id.* at 2184–85.

¹⁹⁰ *See id.*

¹⁹¹ *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

¹⁹² *See id.* at 2217. While the plain words of the Court's express holding appeared to establish significant, broad-sweeping precedential value, *see id.*, the majority seemed to leave room for scaling back some of the decision's most important protections by peppering its opinion with qualifying statements. For instance, while the Court's broad statement suggests that warrantless government access to an individual's CSLI constitutes a search, the Court included a footnote suggesting that its holding was limited to the seven days of CSLI gathered

generated from a cell phone's communications with nearby cell towers.¹⁹³ As the Court in *Carpenter* explained:

Cell phones continuously scan their environment looking for the best signal, which generally comes from the closest cell site. Most modern devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features. Each time the phone connects to a cell site, it generates time-stamped records known as [CSLI].¹⁹⁴

The petitioner in *Carpenter*—Timothy Carpenter—was arrested and convicted on five firearm counts in connection with a series of robberies after a suspect identified Carpenter as an accomplice.¹⁹⁵ Based on the information provided by the suspect, prosecutors applied for court orders under the Stored Communications Act¹⁹⁶ to compel Carpenter's wireless carriers to disclose CSLI linked to Carpenter's phone during the four-month period in which the robberies occurred.¹⁹⁷ After obtaining the orders, prosecutors obtained CSLI records from Carpenter's wireless carriers covering one-hundred and twenty-seven days of Carpenter's location information and disclosing nearly 13,000 location points cataloging

by police in that case. *See id.* at 2217 n.3 (“It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.”). In fact, despite the sweeping language of the Court's holding, the Court later described its decision as “a narrow one” and limited its application to historical—as opposed to real-time—CSLI. *See id.* at 2220.¹⁹³ *See Cell Site Location Information*, ELECTRONIC FRONTIER FOUND., (Mar. 28, 2019), <https://bit.ly/2B89YZi> [<https://perma.cc/SCZ2-34QV>]. CSLI is the information that cell phones convey to nearby cell towers. *Id.* Cell phones constantly search for nearby cell towers in order to locate the tower providing the strongest signal. *Id.* The tower with the strongest signal provides the cell phone with the fastest service. *Id.* When the cell phone connects to a tower, the person's wireless provider records the time and duration of the connection. *Id.* Wireless providers store two types of CSLI: historical and prospective. *Id.* Historical CSLI is used to track a person's past movements. *Id.* Prospective CSLI allows for tracking in real time. *Id.* The Court in *Carpenter* addressed the use of historical CSLI and expressly refused to address the propriety of prospective CSLI. *See Carpenter*, 138 S. Ct. at 2220 (“We do not express a view on matters not before us: real-time CSLI or ‘tower dumps’ . . .”).

¹⁹⁴ *Carpenter*, 138 S. Ct. at 2211.

¹⁹⁵ *Id.* at 2212–13.

¹⁹⁶ Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2018). The Stored Communications Act (SCA) permits the Government “to compel the disclosure of certain telecommunications records when it ‘offers specific and articulable facts showing that there are reasonable grounds to believe’ that the records sought ‘are relevant and material to an ongoing criminal investigation.’” *Carpenter*, 138 S. Ct. at 2212 (quoting 18 U.S.C. § 2703(d)). Thus, in order to obtain an order to compel those records under the SCA, the Government need not satisfy the same requirements for obtaining a warrant—specifically, the requirement of probable cause.

¹⁹⁷ *Carpenter*, 138 S. Ct. at 2212.

Carpenter's movements.¹⁹⁸ Carpenter moved to suppress the CSLI prior to trial, but the district court denied his motion.¹⁹⁹

The U.S. Court of Appeals for the Sixth Circuit affirmed the district court's ruling, holding Carpenter lacked a reasonable expectation of privacy in his location information.²⁰⁰ The Sixth Circuit found the third-party doctrine rendered Carpenter's expectation of privacy in his movements unreasonable because Carpenter had voluntarily conveyed his location information to his wireless carriers in the ordinary course of business.²⁰¹ Citing *Smith v. Maryland*,²⁰² the Sixth Circuit concluded that Carpenter's CSLI constituted voluntarily disclosed business records not entitled to Fourth Amendment protection.²⁰³

The Supreme Court's opinion in *Carpenter* opened with an observation of the pervasiveness of cell phones in modern America and the near-constant stream of data sent to wireless carriers, "even if the owner is not using one of the phone's features."²⁰⁴ The Court noted that "[w]ireless carriers collect and store CSLI" primarily for business purposes, but the Court also acknowledged "wireless carriers often sell aggregated location records to *data brokers*, without individual identifying information of the sort at issue here."²⁰⁵ Recent advancements in technology, the Court observed, have made it possible for "modern cell phones [to] generate increasingly vast amounts of increasingly precise CSLI."²⁰⁶

After surveying the Fourth Amendment's history and its guiding principles,²⁰⁷ the Court found the expectation of privacy in one's CSLI lies "at the intersection of two lines of cases": (1) those addressing the expectation of privacy in one's physical location and movements; and (2)

¹⁹⁸ *Id.*

¹⁹⁹ *Id.*

²⁰⁰ *Id.* at 2213.

²⁰¹ *Id.* For a discussion of the third-party doctrine, see *supra* Section II.B.2.b.

²⁰² *Smith v. Maryland*, 442 U.S. 735 (1979). For a brief discussion of *Smith v. Maryland*, which reaffirmed the third-party doctrine's general precepts, see *supra* Section II.B.2.b.

²⁰³ *Carpenter*, 138 S. Ct. at 2212.

²⁰⁴ *Id.* at 2211.

²⁰⁵ *Id.* at 2212 (emphasis added).

²⁰⁶ *Id.*

²⁰⁷ In particular, the Court acknowledged two "basic guideposts" that applied to the case in *Carpenter*. First, the Court noted, the Fourth Amendment "seeks to secure 'the privacies of life' against 'arbitrary power.'" *Id.* at 2214 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)). The Court then noted that "a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'" *Id.* (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)). For further implications of the Court's survey of the Court's Fourth Amendment jurisprudence, see *infra* Section II.B.3.d.

those in which the Court applied the third-party doctrine.²⁰⁸ Ultimately, these two lines of cases formed the path to the Court's holding in *Carpenter*.

i. Distinctions from Public Movement Cases

The CSLI technology in *Carpenter* presented the Court with unique circumstances that fit somewhere between the two poles of the first line of cases. On the one hand, the Court explained, the Court previously held that people do not have a reasonable expectation of privacy in their travels on public roads, even when law enforcement uses “augmented” visual surveillance.²⁰⁹ In *United States v. Knotts*,²¹⁰ the Court held that a search did not occur when police planted a beeper in a container carried on the defendant's vehicle and used the beeper's signal to track the defendant to his final destination.²¹¹ The Court in *Knotts* focused not on the use of the monitoring technology but rather on the defendant's use of public roads.²¹² The Court in *Knotts* found that the use of technology to augment the “sensory faculties bestowed upon [officers] at birth” does not constitute a search when the police could have otherwise lawfully monitored the suspect's movements without the technology.²¹³

On the other hand, the Court in *Carpenter* noted, the Court has also held that planting a GPS tracking device on the undercarriage of a person's vehicle and using the GPS to conduct surveillance constitutes a search.²¹⁴ In *United States v. Jones*,²¹⁵ the Court found that such use of technology constitutes a search, but it did not reach this conclusion based on the defendant's reasonable expectation of privacy. Instead, the Court in *Jones* found that a search occurred because the police had physically trespassed onto the person's property when they placed the device on the vehicle's undercarriage.²¹⁶ Because the police carried out the trespass for the purpose of monitoring the defendant's movements, a search had occurred.²¹⁷

²⁰⁸ See *Carpenter*, 138 S. Ct. at 2214-15.

²⁰⁹ *Id.* at 2215 (citing *United States v. Knotts*, 460 U.S. 276, 280-81 (1983)).

²¹⁰ *United States v. Knotts*, 460 U.S. 276 (1983).

²¹¹ See *id.* at 282-85.

²¹² See *id.* at 282 (“Visual surveillance from public places . . . would have sufficed to reveal all [relevant] facts to the police. The fact that the officers in this case relied not only on visual surveillance, but also on the use of the beeper . . . does not alter the situation.”).

²¹³ *Id.*

²¹⁴ See *Carpenter*, 138 S. Ct. at 2215 (citing *United States v. Jones*, 565 U.S. 400, 404-05 (2012)).

²¹⁵ *United States v. Jones*, 565 U.S. 400 (2012).

²¹⁶ *Id.* at 404-05.

²¹⁷ *Id.*

The Court in *Carpenter* ultimately noted that, much like the GPS monitoring in *Jones*, CSLI is “detailed, encyclopedic, and effortlessly compiled.”²¹⁸ But the *Carpenter* Court found that CSLI produced far more information about the subject of the search than the GPS monitoring in *Jones*. Focusing heavily on the technology’s ability to “achieve near perfect surveillance,” the Court observed two interconnected aspects of the technology: (1) its precision; and (2) the breadth of information it can reveal about a person.²¹⁹ The Court noted that cell phones have become “almost a ‘feature of human anatomy,’” tracking “nearly exactly the movements of its owners.”²²⁰ Unlike the beeper in *Knotts* or the GPS in *Jones*, the Court explained, cell phones follow their owners beyond public roads and into areas of life that historically have been deemed private, such as homes, doctors’ offices, and political headquarters.²²¹ The Court further noted that CSLI’s precision has rapidly improved in recent years, now enabling wireless carriers to identify users’ locations with increasing accuracy.²²² Importantly, the Court expressed significant concern regarding future advancements in CSLI technology and how those advancements could lead to increasingly more accurate surveillance.²²³

With respect to the breadth of the information, the Court noted that CSLI’s ability to calculate a phone’s location implicates privacy concerns that strike at the core of the Fourth Amendment’s protections.²²⁴ The places that a person visits, the Court explained, can reveal significant details about that person, including “not only [a person’s] particular movements, but through them [his or her] ‘familial, political, professional, religious, and sexual associations.’”²²⁵ These associations, the Court noted, have been

²¹⁸ *Carpenter*, 138 S. Ct. at 2216.

²¹⁹ *Id.* at 2217–18.

²²⁰ *Id.* at 2218.

²²¹ *Id.*

²²² *Id.* at 2218–19 (“[T]he rule the Court adopts ‘must take account of more sophisticated systems that are already in use or in development.’” (quoting *Kyllo v. United States*, 533 U.S. 27, 36 (2001))).

²²³ *See id.* at 2219. Specifically, the Court noted:

While the records in this case reflect the state of technology at the start of the decade, the accuracy of CSLI is rapidly approaching GPS-level precision. As the number of cell sites has proliferated, the geographic area covered by each cell sector has shrunk, particularly in urban areas. In addition, with new technology measuring the time and angle of signals hitting their towers, wireless carriers already have the capability to pinpoint a phone’s location within 50 meters.

Id.

²²⁴ *See id.* at 2217–18 (“Mapping a cell phone’s location over the course of 127 days provides an *all-encompassing record* of the holder’s whereabouts.” (emphasis added)).

²²⁵ *Id.* at 2217.

characterized as the “privacies of life.”²²⁶ And because cell phones travel with a person nearly everywhere he or she goes, while generating increasingly more accurate information, CSLI data provides an “intimate window into a person’s life” that directly implicates the expectations of privacy, which the drafters of the Fourth Amendment sought to protect.²²⁷

ii. Carpenter’s Application of the Third-Party Doctrine

The third-party doctrine’s application to the CSLI in *Carpenter* presented somewhat of a square peg/round hole dilemma.²²⁸ The Government in *Carpenter* argued that even though a person might have a reasonable expectation of privacy in his or her movements when surveilled by GPS monitoring, CSLI data falls within the ambit of the third-party doctrine because the data amounted to business records obtained by wireless carriers.²²⁹ While Justice Kennedy agreed with the Government’s position,²³⁰ the majority did not.

At face value, the third-party doctrine, as it existed pre-*Carpenter*, arguably encompassed CSLI: third-party businesses collected the data; Carpenter knowingly shared the data with those third parties; and Carpenter arguably shared the data voluntarily pursuant to the wireless carriers’ terms-of-service agreements.²³¹ For the majority, however, that position “fail[ed] to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter’s location but also everyone else’s, not for a short period of time but for years and years.”²³²

In what some have deemed a “carve out” to the third-party doctrine,²³³ the Court found that the CSLI data in *Carpenter*, unlike the bank records

²²⁶ *Id.* (quoting *Riley v. California*, 573 U.S. 373, 403 (2014)).

²²⁷ *Id.* at 2217–19.

²²⁸ See Jordan M. Blanke, *Carpenter v. United States Begs for Action*, 2018 U. ILL. L. REV. 260, 260 (2018).

²²⁹ *Carpenter*, 138 S. Ct. at 2219.

²³⁰ See *id.* at 2226–30 (Kennedy, J. concurring).

²³¹ See *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979) (“This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.”) (discussing the third-party doctrine).

²³² *Carpenter*, 138 S. Ct. at 2219.

²³³ See Trevor Burrus & James Knight, *Katz Nipped and Katz Cradled: Carpenter and the Evolving Fourth Amendment*, 17 CATO SUP. CT. REV. 79, 87 (2018) (“[I]nstead of reassessing the Court’s entire Fourth Amendment jurisprudence to judge whether this deviation is justified, [Chief Justice] Roberts carved out a special ‘cell phone exception.’”); Daniel Solove, *Carpenter v. United States, Cell Phone Location Records, and the Third Party Doctrine*, TEACHPRIVACY: PRIVACY + SECURITY BLOG (July 1, 2018), <https://bit.ly/37AzFR2> [<https://perma.cc/J7QA-BUMN>] (“The Supreme Court should have overruled the Third Party Doctrine or at least carved out a greater chunk of it.”).

in *Miller*²³⁴ or the phone records in *Smith*,²³⁵ presented unique concerns that triggered the Fourth Amendment's protections.²³⁶ First, the Court noted that the sheer scope of information collected through CSLI implicates concerns not previously addressed by the Court's third-party-doctrine cases.²³⁷ The aggregated CSLI data acquired by police in *Carpenter* provided an "exhaustive chronicle" of Carpenter's location information.²³⁸ Moreover, the Court noted, the information collected in previous third-party-doctrine cases had inherent limitations.²³⁹ For instance, the telephone call logs in *Smith* "reveal[ed] little in the way of 'identifying information,'" and the bank deposits in *Miller* were "not confidential communications but negotiable instruments to be used in commercial transactions."²⁴⁰ In both cases, the *Carpenter* Court explained, the information obtained from third parties did not implicate highly sensitive information about who a person is.²⁴¹ CSLI data, on the other hand, provides a "detailed chronicle of a person's physical presence compiled every day, every moment, over several years."²⁴²

The Court also found that cell phone users do not "voluntarily" expose their CSLI to wireless carriers, as would be required for the third-party doctrine to apply.²⁴³ In reaching this conclusion, the Court noted two important aspects of the technology at issue. First, the Court noted again that cell phones have become such a pervasive force in modern life that carrying one is now a near-necessity.²⁴⁴ Second, the Court noted that cell phones share their users' location information without any affirmative act on the part of the user.²⁴⁵ Users begin sharing their location information with wireless companies from the moment they turn on their phones.²⁴⁶ For the

²³⁴ See *United States v. Miller*, 425 U.S. 435 (1976).

²³⁵ See *Smith v. Maryland*, 442 U.S. 735 (1979). For further discussion of the third-party doctrine, including its application in *Miller* and *Smith*, see *supra* Section II.B.2.b.

²³⁶ See *Carpenter*, 138 S. Ct. at 2219–20.

²³⁷ *Id.* at 2219.

²³⁸ *Id.*

²³⁹ See *id.* at 2219–20.

²⁴⁰ *Id.* at 2219.

²⁴¹ See *id.* at 2219–20.

²⁴² *Id.* at 2220.

²⁴³ See *id.*

²⁴⁴ *Id.* ("[C]ell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society." (quoting *Riley v. California*, 573 U.S. 373, 383 (2014))).

²⁴⁵ *Id.* ("[A] cell phone logs a cell-sit record by dint of its operation, without any affirmative act on the part of the user beyond powering up.").

²⁴⁶ *Id.*

Court, this dynamic rendered the sharing of CSLI an involuntary act.²⁴⁷ Based on these key distinctions, the Court declared its unwillingness to extend the third-party doctrine to this “distinct category of information.”²⁴⁸

d. Fourth Amendment Privacy and Advancements in Technology Redux

As the forgoing Fourth Amendment cases demonstrate, privacy interests extend beyond the common law and technology has created serious implications for historic notions of privacy. But the value of those cases is limited to the context in which they arose—namely, Fourth Amendment challenges. Accordingly, the question facing the Court was not necessarily whether an invasion of privacy occurred but rather whether the government intruded on a person’s reasonable expectation of privacy and, if so, whether the intrusion was unreasonable.

While the Court in *King* held that Maryland’s cheek swab practices did not violate the Fourth Amendment, it did not find that individuals possess no privacy interests in their DNA.²⁴⁹ In fact, by deeming the cheek swab a “search” under the Fourth Amendment, the Court necessarily concluded that the Government’s use of a cheek swab intrudes upon a person’s reasonable expectation of privacy.²⁵⁰ Similarly, while the court in *Birchfield* found that “breath tests do not ‘implicat[e] significant privacy concerns,’”²⁵¹ it did not find that breath-test procedures do not implicate privacy interests at all.²⁵²

²⁴⁷ *Id.* (“Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily ‘assume the risk’ of turning over a comprehensive dossier of his physical movements.” (brackets omitted) (quoting *Smith v. Maryland*, 442 U.S. 735, 745 (1979))).

²⁴⁸ *Id.*

²⁴⁹ *See Maryland v. King*, 569 U.S. 435, 461–66 (2013) (finding while a person maintains a privacy interest in his or her DNA, an incident-to-arrest DNA swab does not unreasonably intrude on that interest).

²⁵⁰ *See id.* at 446 (“It can be agreed that using a buccal swab on the inner tissues of a person’s cheek in order to obtain DNA samples is a search.”).

²⁵¹ *Birchfield v. North Dakota*, 136 S. Ct. 2160, 2176 (2016) (quoting *Skinner v. Ry. Labor Execs.’ Ass’n*, 489 U.S. 602, 626 (1989)) (emphasis added).

²⁵² *See id.* at 2184. Notably, the Court’s analysis of the breath test assumed that a search had in fact occurred since the question presented was whether a breath test administered incident to arrest was reasonable. *See id.* at 2174 (“In the three cases now before us, the drivers were searched or told that they were required to submit to a search after being placed under arrest

A deeper look into the holdings in *King* and *Birchfield* suggests that the Court's treatment of privacy interests under the Fourth Amendment turns not only on the extent to which the Government physically intrudes on an individual's person but also on (1) the type of information obtained and limitations thereon as well as (2) the scope of information available. The apparent narrowness of the Court's holding in *King*²⁵³ resulted from the limitations that Maryland imposed on police officers' use of the information—specifically, the officers were limited to using the DNA for identification purposes only.²⁵⁴ Presumably, then, the Court in *Birchfield* could have found blood draws for the limited purpose of measuring a person's BAC proper. Admittedly, the Court's refusal to establish such a rule could have resulted from the physically intrusive nature of blood draw procedures.²⁵⁵ But the Court's analysis in *Birchfield* did not stop at the physical intrusion. Instead, the Court went on to state:

[A] blood test, unlike a breath test, places in the hands of law enforcement authorities a sample that can be preserved and from which it is possible to extract information beyond a simple BAC reading. *Even if the law enforcement agency is precluded from testing the blood for any purpose other than to measure BAC, the potential remains and may result in anxiety for the person tested.*²⁵⁶

The Court's statement suggests two concerns. First, by invoking the potential for misuse, the Court seemingly factors into its analysis the information attainable through a blood sample. A blood sample can reveal significantly more information about a person than a cheek swab.²⁵⁷ By removing from police the ability to obtain such information, the Court's decision suggests a distrust of government maintenance of such broadly applicable information absent in *King*.

for drunk driving. We therefore consider how the search-incident-to-arrest doctrine applies to breath and blood tests incident to such arrests.”).

²⁵³ See *supra* Section II.B.3.a (discussing the holding in *King*).

²⁵⁴ See *King*, 569 U.S. at 465–66.

²⁵⁵ See *Birchfield*, 136 S. Ct. at 2178 (“Blood tests are a different matter. They ‘require piercing the skin’ and extract a part of the subject’s body. And while humans exhale air from their lungs many times per minute, humans do not continually shed blood.” (quoting *Skinner*, 489 U.S. at 625) (citations omitted)).

²⁵⁶ *Id.* (emphasis added).

²⁵⁷ *Compare Saliva Samples Can Reveal Serious Illnesses*, SCI. DAILY (July 29, 2013), <https://bit.ly/2SEru2t> [<https://perma.cc/RGW8-GYSR>] (noting limitations on disease detection using saliva samples), with Tim Jewell, *All About Blood Tests*, HEALTHLINE (Feb. 19, 2019), <https://bit.ly/37hq4gH> [<https://perma.cc/MGB8-9UGD>] (describing the vast information about a person that can be obtained through blood samples).

Second, the Court seemingly placed some weight on the mental harm that blood draws can cause.²⁵⁸ That harm, however, was not the physical harm caused by administering the blood draw itself. Rather, the Court focused on the potential mental harm caused by the lingering prospect of the Government misusing such a broad array of personal information.²⁵⁹

Similar concerns manifested in *Carpenter*. The Court in *Carpenter* bookended its analysis with some “basic guideposts” for assessing Fourth Amendment challenges to the Government’s use of technology.²⁶⁰ First, the Court noted, “the Fourth Amendment seeks to secure ‘the privacies of life’ against ‘arbitrary power.’”²⁶¹ At the heart of this concept is the fundamental concern that the Government, equipped with the full power of the State, will use its authority to pry into the private lives of citizens.²⁶² This concern emerges from the power imbalance that exists between the Government and the people. Without constitutional safeguards in place, the Government could use its power to intrude into peoples’ private affairs without facing any meaningful barriers.

But the Court’s concerns do not end there. The second guidepost, the Court noted, is “a central aim of the Framers [] ‘to place obstacles in the way of a too permeating police surveillance.’”²⁶³ Assessed against the backdrop of the Court’s more recent Fourth Amendment technology cases,²⁶⁴ the Court’s concerns suggest a deeper distrust of the Government’s use of power to collect and use information that appears harmless—namely, a person’s locations over an extended period of time—but that *reveals* highly private, intimate details about peoples’ lives. The majority in *Carpenter* understood that CSLI reveals much more than a person’s location: it reveals information about who the person is through his or her “‘familial, political, professional, religious, and sexual associations.’”²⁶⁵

A person’s movements and locations over an extended period of time can paint a detailed portrait of that person by revealing the person’s work

²⁵⁸ See *Birchfield*, 136 S. Ct. at 2178 (“Even if the law enforcement agency is precluded from testing the blood for any purpose other than to measure BAC, the potential remains and may result in anxiety for the person tested.”).

²⁵⁹ See *id.*

²⁶⁰ See *Carpenter v. United States*, 138 S. Ct. 2206, 2213–16 (2018).

²⁶¹ See *id.* at 2214 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).

²⁶² See *id.* (“As technology has enhanced the Government’s capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to ‘assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.’” (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001))).

²⁶³ *Id.* at 2214.

²⁶⁴ See *supra* Sections II.B.3.a–c.

²⁶⁵ See *Carpenter*, 138 S. Ct. at 2217 (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012)).

and home addresses; the places that he or she does and does not visit; the businesses at which he or she shops; his or her place of worship; and whether the person visits the locations of political protests. And through CSLI, all of this information is conveniently timestamped to reveal the precise time at which the person arrived at a location, as well as the duration of time that elapsed before the person traveled to his or her next destination. Together, this information can reveal much about who the person is, including the people with whom he or she frequently, or infrequently, associates; the organizations in which he or she participates; and his or her spending preferences, religious affiliations, and level of political involvement. *Carpenter* thus represents more than the Court's unwillingness to permit the Government to obtain information about a person's location, but instead stands for the proposition that the information about a person that one can learn through extended surveillance of his or her movements paints a far-too-detailed portrait of that person's life. Accordingly, people can reasonably expect to retain privacy in those details—regardless of the methods used to circumvent their expectations.

It is against this backdrop that Part III assesses the privacy rights implicated when private actors obtain an individual's biometric information.

IV. CURRENT PRIVACY CLAIMS AND BIOMETRIC PRIVACY

A. *Privacy in Tort*

Over the course of several decades, the American right to privacy took shape in the civil context through four now-commonly recognized privacy torts.²⁶⁶ Privacy torts generally aim to protect individuals from “mental pain and distress” arising from privacy invasions²⁶⁷ and seek to remedy emotional, reputational, and proprietary injuries.²⁶⁸ This section first overviews the privacy tort most relevant to facial recognition technology—appropriation of name or likeness—and assesses the viability of appropriation claims that are based on privacy injuries caused by facial recognition technology in the social-media context. It concludes that such claims would likely fail. Next, this section uses O'Neill's 10-Year Challenge theory to demonstrate how even appropriation-by-manipulation claims would also likely fail.

²⁶⁶ See *supra* notes 106–20 and accompanying text.

²⁶⁷ See Warren & Brandeis, *supra* note 98, at 196 (“[M]odern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.”).

²⁶⁸ See *supra* notes 106–20 and accompanying text.

1. Appropriation and Facebook's Facial Recognition Techniques

The appropriation tort protects an individual's "exclusive use of his own identity, in so far as it is represented by his name or likeness, and in so far as the use may be of benefit to him or to others."²⁶⁹ Under the definition of appropriation provided by the *Restatement (Second) of Torts*, which many states have adopted, an appropriation occurs when a person appropriates "the name or likeness of another" for his or her "own use or benefit."²⁷⁰

a. Name or Likeness

Most courts have found that the phrase "name or likeness" extends beyond a person's actual name or likeness to broader aspects of the person's identity.²⁷¹ Accordingly, courts have held that "name or likeness" includes, among other things, nicknames,²⁷² professions,²⁷³ identifying characteristics,²⁷⁴ and catch phrases,²⁷⁵ provided that those aspects are reasonably tied to the injured party's identity. On the other hand, "name or likeness" does not encompass matters generally removed from the person's identity, such as a passing reference to a person.²⁷⁶

²⁶⁹ RESTATEMENT (SECOND) OF TORTS § 652C cmt. c (AM. LAW. INST. 1977).

²⁷⁰ *Id.* § 652C.

²⁷¹ See SOLOVE & SCHWARTZ, *supra* note 106, at 218–19; see also RESTATEMENT (SECOND) OF TORTS § 652C cmt. c ("The interest protected by the rule stated in this Section is the interest of the individual in the exclusive use of his own identity, in so far as it is represented by his name or likeness, and in so far as the use may be of benefit to him or to others.").

²⁷² See *Hirsch v. S. C. Johnson & Son, Inc.*, 280 N.W.2d 129, 137 (Wis. 1979) (finding the use of a famous football player's nickname fell within the ambit of the appropriation tort) ("The fact that the name, 'Crazylegs,' used by [defendant], was a nickname rather than [plaintiff's] actual name does not preclude a cause of action. *All that is required is that the name clearly identify the wronged person.*" (emphasis added)).

²⁷³ See *Ali v. Playgirl, Inc.*, 447 F. Supp. 723, 726–29 (S.D.N.Y. 1978) (finding a magazine's depiction of a person with facial features similar to a famous boxer sitting near a boxing ring implicated the appropriation tort).

²⁷⁴ See *Motschenbacher v. R. J. Reynolds Tobacco Co.*, 498 F.2d 821, 827 (9th Cir. 1974) (finding a photograph that depicted a race car bearing similar, distinct characteristics of a famous race car driver constituted appropriation of the driver's name or likeness).

²⁷⁵ See *Carson v. Here's Johnny Portable Toilets, Inc.*, 698 F.2d 831, 836 (6th Cir. 1983) (finding the use of a well-known television host's catch phrase constituted appropriation of the host's name or likeness).

²⁷⁶ See *Stien v. Marriott Ownership Resorts*, 944 P.2d 374, 380 (Utah Ct. App. 1997) (finding plaintiff failed to establish that the producers of a video in which her husband was featured making passing references to her did not constitute an appropriation of her name or likeness).

Facebook appropriates its users' name or likeness by capturing and storing their facial biometrics. By definition, facial biometrics are inherent to a person's identity.²⁷⁷ As the ACLU explained in a recent amicus brief, facial scans target the very essence of peoples' identities because "each [face] is unique, and cannot be altered."²⁷⁸ Similarly, the Illinois legislature found that biometric information is "biologically unique to the individual."²⁷⁹

b. Commercial or Other Value

To prevail on an appropriation claim, plaintiffs in some states are required to show that the appropriated identity possesses some inherent value that the defendant exploited.²⁸⁰ In establishing these requirements, courts have relied on the language of the *Restatement's* commentary, which limits the actionable conduct to a defendant's appropriation of the "reputation, prestige, social or commercial standing, public interest or other values of the plaintiff's name or likeness."²⁸¹ Some courts that impose these requirements have found it necessary for plaintiffs to prove that they possess some "notoriety or skill,"²⁸² and others have required plaintiffs to show that their name or likeness carries some "market value" or "economic worth."²⁸³

Other courts, however, have found a showing of commercial value unnecessary. For example, in *Fraley v. Facebook*,²⁸⁴ the U.S. District Court for the Northern District of California found California's appropriation statute requires no showing of a "preexisting value, and in fact can be read to presume that a person whose name, photograph, or likeness is used by another for commercial purposes without their consent is 'injured as a result thereof.'"²⁸⁵

²⁷⁷ See *Putting More than Just a Name to a Face*, NEC, <https://bit.ly/2BRkpkF> [<https://perma.cc/L5M3-V5RC>] ("The human face plays an important role in our social interaction, conveying people's identity."); *Facial Recognition*, *supra* note 17 ("Like all biometrics solutions, face recognition technology measures and matches the unique characteristics for the purposes of identification or authentication.").

²⁷⁸ Brief of Amicus Curiae American Civil Liberties Union in Support of Plaintiffs-Appellees Seeking Affirmance at 13, *Patel v. Facebook*, 932 F.3d 1264, 1270-75 (9th Cir. 2019), <https://bit.ly/2V3stG8> [<https://perma.cc/JJV4-LTHK>].

²⁷⁹ 740 ILL. COMP. STAT. ANN. 14/5(g) (LexisNexis 2019).

²⁸⁰ See, e.g., *Meadows v. Hartford Life Ins. Co.*, 492 F.3d 634, 638 (5th Cir. 2007); *Lawrence v. A.S. Abell Co.*, 475 A.2d 448, 453 (Md. 1984).

²⁸¹ RESTATEMENT (SECOND) OF TORTS § 652C cmt. c (AM. LAW INST. 1977).

²⁸² See *Meadows*, 492 F.3d at 638.

²⁸³ See *Lawrence*, 475 A.2d at 453.

²⁸⁴ *Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785 (N.D. Cal. 2011).

²⁸⁵ *Id.* at 806 (assessing the injury element under California's misappropriation statute).

Perhaps the schism stems from a misunderstanding of the distinction between the *appropriation* tort and the *right of publicity* tort. As the Supreme Court of Nevada noted in *People for the Ethical Treatment of Animals v. Bobby Berosini, Ltd.*²⁸⁶:

The common law appropriation tort ordinarily involves the unwanted and unpermitted use of the name or likeness of an *ordinary, uncelebrated* person for advertising or other such commercial purposes, although it is possible that the appropriation tort might arise from the misuse of another's name for purposes not involving strictly monetary gain. The right of publicity tort, on the other hand, involves the appropriation of a *celebrity's* name or identity for commercial purposes. The distinction between these two torts is the interest each seeks to protect. The appropriation tort seeks to protect an individual's personal interest in privacy; the personal injury is measured in terms of the mental anguish that results from the appropriation of an ordinary individual's identity. The right to publicity seeks to protect the property interest that a celebrity has in his or her name; the injury is not to personal privacy, it is the economic loss a celebrity suffers when someone else interferes with the property interest that he or she has in his or her name.²⁸⁷

Absent a change in the ways in which state courts approach the appropriation tort, however, Facebook would likely avoid liability in the majority of appropriation cases. Under the commercial-value approach, a person must maintain celebrity status to mount a successful appropriation claim,²⁸⁸ leaving appropriation claims open to only a small portion of users.²⁸⁹

²⁸⁶ PETA v. Bobby Berosini, Ltd., 895 P.2d 1269 (Nev. 1995).

²⁸⁷ *Id.* at 1283 (emphasis added) (footnote omitted); see also Hirsch v. S. C. Johnson & Son, Inc., 280 N.W.2d 129, 132 (Wis. 1979) (“We conclude that the right of a person to be compensated for the use of his name for advertising purposes or purposes of trade is distinct from other privacy torts which protect primarily the mental interest in being let alone.”).

²⁸⁸ See Note, *In the Face of Danger: Facial Recognition and the Limits of Privacy Law*, 120 HARV. L. REV. 1870, 1880 (2007) (“[T]he only ones who can invoke [the misappropriation tort] are those whose names and faces are well recognized, and who therefore have commercial value that could be exploited—in short, celebrities.” (footnote omitted)).

²⁸⁹ As of December 2018, there were over 2.32 billion Facebook users worldwide who used Facebook regularly each month. See Press Release, Facebook, Facebook Reports Fourth Quarter and Full Year 2018 Results (Jan. 30, 2019), <https://bit.ly/2GBIMaW> [<https://perma.cc/V2V3-98HL>]. Some estimates indicate that between approximately 1 in 10,000 and 5 in 10,000 people worldwide are famous. See Samuel Arbesman, *The Fraction of Famous People in the World*, WIRED (Jan. 22, 2013), <https://bit.ly/2nXPI5s> [<https://perma.cc/P7BD-TXRB>]. The role of social-media “influencers” (i.e., users who have acquired a relatively large social-media following) might complicate these numbers, as influencers often receive payment through paid advertising and have therefore likely attained

c. Use or Benefit

Problems again arise when assessing whether Facebook gathers and stores its users' biometric data for its own "use or benefit." While the *Restatement's* approach encompasses instances where a person appropriates another's name or likeness for *any* purpose or benefit—"even though the use is not a commercial one, and even though the benefit sought to be obtained is not a pecuniary one"²⁹⁰—some states limit liability to the appropriator's commercial use.²⁹¹

For its part, Facebook claims to collect and use biometric data strictly to benefit users.²⁹² And while some have observed that Facebook also uses the data to support its research into artificial intelligence technology,²⁹³ the link between that use and any potential pecuniary gain Facebook derives from the research may be too attenuated to satisfy the "use or benefit" element. Absent implementing a practice of selling its users' biometric data to third parties, Facebook's current biometric-data practices fall short of "commercial use."

d. Consent

Perhaps the largest barrier to establishing liability is consent. While the concept of consent does not explicitly appear in the *Restatement's* definition of appropriation,²⁹⁴ the absence of consent is a widely accepted requirement for appropriation claims. Some scholars have posited that lack of consent is an element implied in the definition of "appropriate";²⁹⁵ others view consent

celebrity status for purposes of the appropriation tort. *Accord* Mona Hellenkemper, *State of the Industry—Influencer Marketing in 2019*, INFLUENCERDB (Jan. 14, 2019), <https://bit.ly/35uvJ2l> [<https://perma.cc/2592-8LWS>] ("Instagram today has more than 1.4 million accounts with more than 15k followers.").

²⁹⁰ RESTATEMENT (SECOND) OF TORTS § 652C cmt. b (AM. LAW INST. 1977).

²⁹¹ *See id.* ("Statutes in some states have, however, limited the liability to commercial uses of the name or likeness."); *see also* Lee v. Picture People, Inc., No. K10C-07-002 (RBY), 2012 Del. Super. LEXIS 159, at *6 (Mar. 19, 2012) ("Appropriation claims seek redress for the 'appropriation of some element of a person's personality for commercial use . . .'" (quoting Guthridge v. Pen-Mod, Inc., 239 A.2d 709 (Del. Super. Ct. 1967))).

²⁹² *See Facebook Face Recognition*, *supra* note 35 (explaining how Facebook's use of facial recognition technology is limited to creating a user-friendly experience); Sherman, *supra* note 19 (same).

²⁹³ *See* Bennett, *supra* note 20.

²⁹⁴ *See* RESTATEMENT (SECOND) OF TORTS § 652C (AM. LAW INST. 1977).

²⁹⁵ *See* Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 128 (2003). Merriam-Webster Dictionary defines "appropriate," in part, as: "to take or make use of without authority or

as an affirmative defense.²⁹⁶ Indeed, some states have expressly incorporated “lack of consent” into the elements of an appropriation claim.²⁹⁷

According to Prosser,²⁹⁸ consent serves as an affirmative defense to appropriation claims and “may be given expressly, or by conduct, such as posing for a picture with knowledge of the purposes for which it is to be used.”²⁹⁹ Thus, courts have held, consent can occur when a person voluntarily acts after the purported tortfeasor discloses to the person how it will use the surrendered information.³⁰⁰

In the online context, a company’s privacy policy or terms of service may establish the basis for consent. For example, courts have found that consent exists when a person uses a company’s website and the company maintains a privacy policy that clearly (1) states the company’s intent to receive users’ information; (2) explains how the company will use that information; and (3) makes acceptance of the terms a precondition to using the website.³⁰¹ These types of agreements are known as “browsewrap” agreements.³⁰² When a company uses a browsewrap agreement, consent is valid even if the user did not read the privacy policy, “provided that the user

right.” *Appropriate*, MERRIAM-WEBSTER, <https://bit.ly/2T4SGXp> [<https://perma.cc/8D85-9PL8>].

²⁹⁶ See Prosser, *supra* note 113, at 419 (“Chief among the available defenses is that of the plaintiff’s consent to the invasion, which will bar his recovery as in the case of any other tort.”).

²⁹⁷ See, e.g., *Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1214 (N.D. Cal. 2014).

²⁹⁸ See *supra* notes 106–20 and accompanying text.

²⁹⁹ Prosser, *supra* note 113, at 419.

³⁰⁰ See *In re Google, Inc. Privacy Policy Litig.*, No. C-12-01382-PSG, 2013 U.S. Dist. LEXIS 171124, at *39–42 (N.D. Cal. Dec. 3, 2013) (finding plaintiffs failed to state a misappropriation claim because plaintiffs consented to using Google’s “+1” feature by voluntarily clicking on the “+1” feature after Google clearly disclosed how the feature worked).

³⁰¹ See *Garcia v. Enter. Holdings, Inc.*, 78 F. Supp. 3d 1125, 1137 (N.D. Cal. 2015). These types of contracts are known as “browsewrap agreements.” See *id.*

Contracts formed on the Internet come primarily in two flavors: ‘clickwrap’ (or ‘click-through’) agreements, in which website users are required to click on an ‘I agree’ box after being presented with a list of terms and conditions of use; and ‘browsewrap’ agreements, where a website’s terms and conditions of use are generally posted on the website via a hyperlink at the bottom of the screen.

Id. (quoting *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1175–76 (9th Cir. 2014)).

In the context of “clickwrap” agreements, however, a user may successfully demonstrate lack of consent by producing evidence showing he or she did not click the “I agree” box because assent to the agreement arises when the user clicks on the box. See *Garcia*, 78 F. Supp. 3d at 1137. On the other hand, assent to “browsewrap” agreements arises when the user simply uses the website. *Id.*

³⁰² See *supra* note 301.

had actual knowledge of the agreement or the website put ‘a reasonably prudent user on notice of the terms of the contract.’”³⁰³

Facebook uses a browsewrap agreement,³⁰⁴ which makes acceptance of Facebook’s data policy a precondition to using the platform.³⁰⁵ Thus, by using Facebook, users consent to the data policy, which clearly states that Facebook uses facial recognition technology if users “have it turned on.”³⁰⁶ Accordingly, users are precluded from claiming misappropriation of their biometric data to the extent Facebook discloses how it uses their data.³⁰⁷ Facebook provides several examples of how it currently uses facial-recognition technology, which include assisting with “tagging” photos, detecting impersonation, and assisting users with visual impairments.³⁰⁸ Thus, absent evidence showing Facebook uses its facial recognition technology for an undisclosed purpose,³⁰⁹ Facebook’s use of biometric data will not give rise to civil liability because consent will always stand in the way.

³⁰³ *Garcia*, 78 F. Supp. 3d at 1137 (quoting *Nguyen*, 763 F.3d at 1177).

³⁰⁴ *See Terms of Service*, *supra* note 24.

³⁰⁵ *See id.* (“To provide these services, we must collect and use your personal data. We detail our practices in the Data Policy, which you must agree to in order to use our Products.”).

³⁰⁶ *See Data Policy*, *supra* note 24 (“If you have it turned on, we use face recognition technology to recognize you in photos, videos and camera experiences.”). In the past, Facebook’s facial recognition technology was “turned on” by default. Sidney Fussell, *Facebook’s New Face Recognition Features: What We Do (and Don’t) Know*, GIZMODO (Feb. 27, 2018), <https://bit.ly/2CXtpIY> [<https://perma.cc/87MP-2PPQ>]. However, Facebook recently announced a new face recognition feature that is turned off by default. *Id.*

³⁰⁷ If, however, Facebook used a consumer’s data in a manner in which it failed to disclose, a plaintiff may plausibly argue that he or she did not consent. *See Cohen v. Facebook, Inc.*, 798 F. Supp. 2d 1090, 1095–96 (N.D. Cal. 2011). The plaintiffs in *Cohen v. Facebook* claimed Facebook misappropriated their names or likenesses when Facebook used their profile pictures to promote its “Friend Finder” service. *See id.* at 1094. Pointing to broad, sweeping statements in its Terms of Service, Facebook argued that the plaintiffs consented to such use. *See id.* at 1094–96. The court rejected Facebook’s argument, finding instead that “[n]othing in the provisions of the Terms documents to which Facebook has pointed constitutes a clear consent by users to have their name or profile picture shared in a manner that discloses what services on Facebook they have utilized, or to endorse those services.” *Id.* at 1095.

³⁰⁸ *See Facebook Face Recognition*, *supra* note 35.

³⁰⁹ Such a situation, however, does not fall outside the realm of possibility, given Facebook’s historical handling of users’ private information. In 2012, Facebook entered into a consent decree with the Federal Trade Commission (FTC) after the FTC found Facebook was deceiving its users. *See Agreement Containing Consent Order, In re Facebook, Inc.*, No. 092-3184 (F.T.C. Aug. 10, 2012). The FTC’s complaint alleged, among other things, that Facebook told users that third-party apps could access users’ personal information only to the extent necessary to operate. *See Complaint at 10, In re Facebook, Inc.*, No. 092-3184 (F.T.C.). In reality, the FTC alleged, Facebook permitted third-party apps to access users’ information that was unrelated to the apps’ operations. *Id.*

2. *Appropriation by Manipulation*

Even appropriation of biometric data by manipulation falls outside the purview of privacy-tort claims. Consider the 10-Year Challenge. Theoretically, if Facebook had generated and used the 10-Year Challenge as pretext to lure users into exposing their biometric data to Facebook's facial recognition software, then participating users would be disclosing information that would have otherwise remained private but for Facebook's inducement. In other words, Facebook would have caused its users to disclose their biometric information under false pretenses—regardless of whether users actually realized what information they were disclosing.³¹⁰ While objectionable to some, this strategy does not implicate private tort liability. The reason—consent.

Assuming a plaintiff can establish all the express elements of the appropriation tort,³¹¹ Facebook's data policy³¹² remains a viable means by which Facebook can avoid liability. In fact, it is unlikely that the pretext under which Facebook theoretically obtained the information negates users' consent at all. First, some courts have explicitly found that consent obtained under false pretenses does not invalidate otherwise valid consent.³¹³ More important, however, is the context in which Facebook theoretically manipulated its users into disclosing their personal information: Facebook did not use pretext to obtain users' *consent*; rather, it used pretext to obtain the *information*. By using Facebook's services, users consent to Facebook's data policy and thereby consent to any subsequent data collection.³¹⁴ The consent subsists regardless of the circumstances under which the person posts to the platform and covers every subsequent act of data collection.

Absent a major change in the law, Facebook and other data collectors can skirt tort liability even when they manipulate users into disclosing biometric information that would have otherwise remained private. In

³¹⁰ See Anthony Cuthbertson, *Most People Don't Know About Facebook's Invasive Data Practices, Study Finds*, INDEPENDENT (Jan. 17, 2019), <https://ind.pn/2sBLAwC> [<https://perma.cc/M2VU-BKQP>] (reporting that a recent study found roughly seventy-five percent of Facebook users do not know how Facebook collects and uses their data).

³¹¹ The express elements of an appropriation claim include: (1) the defendant appropriates the name or likeness of the plaintiff; and (2) the defendant did so for his or her own use or benefit. See RESTATEMENT (SECOND) OF TORTS § 652C (AM. LAW INST. 1977); see also *supra* Section III.A.1.

³¹² See *Data Policy*, *supra* note 24; see also *supra* notes 304–08 and accompanying text.

³¹³ See, e.g., *Baugh v. CBS, Inc.*, 828 F. Supp. 745, 757 (N.D. Cal. 1993) (finding a plaintiff's "improperly induced" consent barred her claim for intrusion upon seclusion).

³¹⁴ Consent to the data policy is a precondition to using Facebook's platform; by using Facebook's services, users consent to the policy. See *supra* notes 304–08 and accompanying text.

efforts to curb biometric privacy intrusions, three states have enacted laws that attempt to prevent biometric data-collection injuries but nevertheless fall short of protecting against practices designed to manipulate consumers into disclosing their information. The next section discusses those statutes.

B. Biometric Privacy in State Statutory Law

Illinois became the first state to enact a comprehensive biometric privacy law in 2008.³¹⁵ Since then, only two other states—Texas and Washington—have enacted biometric privacy laws of similar, albeit lesser, magnitude.³¹⁶ Meanwhile, federal efforts have stagnated.³¹⁷ This section first overviews the three state laws that directly address biometric privacy. It then demonstrates how those laws fall short of protecting against pretextual biometric data-collection techniques.

1. Statutory Protections at the State Level

a. Illinois

In 2008, Illinois enacted the Illinois Biometric Information Privacy Act (BIPA)³¹⁸ to protect its citizens' biometric information from data collectors. In recent years, however, companies like Facebook have taken steps to erode BIPA's protections.

i. Overview of BIPA

BIPA has become known as the “archetype” of biometric privacy laws for both its scope and enforcement provisions.³¹⁹ The statute's legislative

³¹⁵ See Jane Bambauer, *Biometric Privacy Laws: How a Little-Known Illinois Law Made Facebook Illegal 2* (2017), <https://bit.ly/2GXl7Ag> [<https://perma.cc/6CUD-U4YU>] (unpublished manuscript) (crediting Illinois as the first state to pass a comprehensive biometric privacy law). Other states have passed less-comprehensive biometric-privacy laws. See *id.* at 2 n.1.

³¹⁶ See *infra* Section III.B.1.

³¹⁷ For example, Senator Patrick Leahy introduced the Consumer Privacy Protection Act of 2017, see S.2124, 115th Cong. (2017), which would have provided some federal protection of consumers' biometric data, on November 14, 2017. The bill did not make it out of the Judiciary Committee. See *S.2124—Consumer Privacy Protection Act of 2017*, CONGRESS.GOV, <https://bit.ly/2SVdweL> [<https://perma.cc/5MVR-S6S2>].

³¹⁸ 740 ILL. COMP. STAT. ANN. 14/1-14/99 (LexisNexis 2019).

³¹⁹ See, e.g., Bambauer, *supra* note 315, at 2 (“The archetype example of a biometric privacy law is the Illinois Biometric Information Privacy Act (‘BIPA’).”); *Biometrics Laws and Privacy Policies*, PRIVACYPOLICIES.COM, <https://bit.ly/2E5k4el> [<https://perma.cc/D38P-JZ39>] (“[BIPA is] the archetype of biometric privacy laws that other states—Texas and Washington—would draw up on [sic] later.”).

findings and intent demonstrate the Illinois legislature's concerns over (1) the growth in businesses that use biometric technology;³²⁰ (2) the risk of harm to which the technology exposes consumers and the anxiety resulting from that risk;³²¹ and (3) the unknown ramifications of biometric technology.³²²

Importantly, the Illinois General Assembly recognized that:

Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. *Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse,* is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.³²³

BIPA prohibits individuals, businesses, and other groups from collecting, capturing, purchasing, or otherwise obtaining a person's "biometric identifier"³²⁴ or "biometric information,"³²⁵ without first:

- (1) inform[ing] the subject . . . in writing that a biometric identifier or biometric information is being collected or stored;
- (2) inform[ing] the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
- (3) receiv[ing] a written release executed by the subject of the biometric identifier or biometric information.³²⁶

Additionally, BIPA strictly prohibits profiting off of another person's biometric data³²⁷ and requires private actors to obtain express consent prior to disseminating the biometric information they collect.³²⁸ BIPA also imposes rigorous data-protection obligations³²⁹ and requires companies in possession of such data to implement and disclose to the public their retention policies.³³⁰ Most notably, however, BIPA provides a private right

³²⁰ 740 ILL. COMP. STAT. ANN. 14/5(a)-(b).

³²¹ *Id.* 14/5(c)-(e).

³²² *Id.* 14/5(f).

³²³ *Id.* 14/5(c) (emphasis added).

³²⁴ BIPA defines "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." *Id.* 14/10.

³²⁵ Under BIPA, the definition of "biometric information" includes "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." *Id.*

³²⁶ *Id.* 14/15(b).

³²⁷ *See id.* 14/15(c).

³²⁸ *See id.* 14/15(d).

³²⁹ *See id.* 14/15(e).

³³⁰ *See id.* 14/15(a).

of action for individuals harmed by violations of the statute,³³¹ awarding \$1000 in statutory damages for negligent violations³³² and \$5000 in statutory damages for intentional or reckless violations.³³³

ii. Attacks on BIPA and Recent Litigation

Private companies have made several attempts to undermine and seriously weaken BIPA's protections. For instance, the New York Times reported in 2016 that Facebook had launched the lobbying effort³³⁴ behind an amendment to BIPA that would have removed protections against facial-recognition scans and undercut then-ongoing litigation against Facebook and other companies that violated BIPA in its original form.³³⁵ Ultimately, the bill's author announced that he would not call for a vote after privacy advocates and the Illinois Attorney General announced opposition to the bill.³³⁶ Nevertheless, Illinois state legislators continue to introduce bills that would undermine BIPA's protections.³³⁷

In addition to mounting legislative challenges, BIPA's opponents have challenged the law in the courts.³³⁸ Of all the rulings issued in BIPA litigation, arguably the most consequential ruling was issued by the U.S. Court of

³³¹ See *id.* 14/20.

³³² See *id.* 14/20(1).

³³³ See *id.* 14/20(2).

³³⁴ See Conor Dougherty, *Tech Companies Take Their Legislative Concerns to the States*, N.Y. TIMES (May 27, 2016), <https://nyti.ms/34fEMEm> [<https://perma.cc/NW2H-9WG6>] (“The amendment was lobbied for by Facebook . . .”).

³³⁵ Adam Schwartz, *The Danger of Corporate Facial Recognition Tech*, ELECTRONIC FRONTIER FOUND. (June 7, 2016), <https://bit.ly/2DbeDL6> [<https://perma.cc/N3XR-WR2G>] [hereinafter *Corporate Facial Recognition*]. BIPA's definition of “biometric identifier” excludes “photographs” from the definition. See ILL. COMP. STAT. ANN. 14/10. Among other substantive changes, the bill would have modified the word “photographs” with the words “physical or digital” and would have therefore excluded protections for both physical and digital photographs. See Letter from Privacy Groups to Sen. Terry Link, Ill. Gen. Assemb. 2 (May 27, 2016), <https://bit.ly/35sk2ta> [<https://perma.cc/6CN6-BK8W>]. In addition, the bill would have applied retroactively and therefore undercut claims in pending BIPA litigation. See H.R. 6074, S. Amend. 1, 99th Gen. Assemb., Reg. Sess. § 5(h) (Ill. 2016).

³³⁶ *Corporate Facial Recognition*, *supra* note 335.

³³⁷ See, e.g., Adam Schwartz, *New Attack on Illinois Biometric Privacy Act*, ELECTRONIC FRONTIER FOUND. (Apr. 10, 2018), <https://bit.ly/2XQ83TP> [<https://perma.cc/Z56Z-LE3U>].

³³⁸ See, e.g., *Patel v. Facebook*, 932 F.3d 1264, 1270–75 (9th Cir. 2019) (finding plaintiffs suffered an injury-in-fact, and therefore had standing to sue, when Facebook allegedly violated BIPA by not receiving the plaintiffs' opt-in consent to Facebook's use of facial recognition technology); *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, ¶¶ 19–33 (finding BIPA's private right of action provisions apply even when the sole injury is a violation of a person's statutory rights).

Appeals for the Ninth Circuit in *Patel v. Facebook*.³³⁹ The plaintiffs in *Patel*—who were all Illinois residents—filed suit against Facebook alleging that Facebook’s “Tag Suggestions” feature violated BIPA.³⁴⁰ The feature, which was enabled by default, used facial-recognition technology to detect whether users’ faces appeared in images posted to Facebook’s platform.³⁴¹ The plaintiffs argued that Facebook violated their rights under BIPA when Facebook used facial-recognition technology on images displaying the plaintiffs’ faces without first obtaining the plaintiffs’ opt-in consent.³⁴² Facebook moved to dismiss the plaintiffs’ complaint for lack of Article III standing, arguing that the plaintiffs had not alleged any concrete injury.³⁴³ The district court denied Facebook’s motion, and Facebook appealed to the Ninth Circuit.³⁴⁴

On appeal, the Ninth Circuit held that the plaintiffs had pleaded a concrete injury sufficient to confer standing to sue.³⁴⁵ Specifically, the Ninth Circuit found that the statutory violations alleged by the plaintiffs did not constitute mere “procedural” violations but instead amounted to concrete injuries-in-fact.³⁴⁶ Drawing on the origins and development of the right to privacy, in both the common-law and constitutional contexts, the Ninth

³³⁹ *Patel v. Facebook, Inc.*, 932 F.3d 1264 (9th Cir. 2019).

³⁴⁰ *Id.* at 1268.

³⁴¹ *Id.* at 1267–68.

³⁴² *See id.* at 1268.

³⁴³ *Id.* at 1269. The standing doctrine is rooted in the “cases and controversies” clause of Article III of the U.S. Constitution. *See Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016). Article III limits the power of federal courts to deciding “cases and controversies.” U.S. CONST. art. III, § 2. Over time, the Supreme Court has interpreted the clause to require plaintiffs to establish “standing” to sue a defendant. *See Spokeo*, 136 S. Ct. at 1547. The standing doctrine requires, in part, that the plaintiff “suffered an injury in fact” which occurs when the plaintiff “suffered ‘an invasion of a legally protected interest’ that is ‘concrete and particularized’ and ‘actual or imminent, not conjectural or hypothetical.’” *Id.* at 1547–48 (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992)). In *Spokeo v. Robinson*, the Supreme Court held that a plaintiff does not necessarily meet the “concrete injury” requirement “whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right.” *Id.* at 1549. “Bare procedural violation[s],” the Court explained, cannot form the basis for standing if the procedural violation did not give rise to an actual, concrete injury. *Id.* “In other words, for Article III purposes, it is not enough for a plaintiff to allege that a defendant has violated a right created by a statute; we must still ascertain whether the plaintiff suffered a concrete injury-in-fact due to the violation.” *Patel*, 932 F.3d at 1270. Accordingly, the Ninth Circuit in *Patel* had to determine whether the plaintiffs had alleged a “bare procedural violation” of BIPA or an actual, concrete injury. *Id.* at 1270–71.

³⁴⁴ *See Patel*, 932 F.3d at 1269–70.

³⁴⁵ *See id.* at 1275.

³⁴⁶ *See id.* at 1271–74.

Circuit found that the privacy interests protected by BIPA align with the historic privacy interests protected in the common-law and Fourth-Amendment contexts.³⁴⁷ The court drew heavily on the Supreme Court’s opinion in *Carpenter*, finding many of the privacy concerns arising from CSLI also arose in the biometric-privacy context and therefore implicate “concrete interests in privacy”³⁴⁸:

As in the Fourth Amendment context, the facial-recognition technology at issue here can obtain information that is “detailed, encyclopedic, and effortlessly compiled,” which would be almost impossible without such technology. Once a face template of an individual is created, Facebook can use it to identify that individual in any of the other hundreds of millions of photos uploaded to Facebook each day, as well as determine when the individual was present at a specific location. Facebook can also identify the individual’s Facebook friends or acquaintances who are present in the photo. Taking into account the future development of such technology as suggested in *Carpenter*, it seems likely that a face-mapped individual could be identified from a surveillance photo taken on the streets or in an office building. Or a biometric face template could be used to unlock the face recognition lock on that individual’s cell phone. We conclude that the development of a face template using facial-recognition technology without consent (as alleged here) invades an individual’s private affairs and concrete interests. Similar conduct is actionable at common law.³⁴⁹

The court in *Patel* concluded that Facebook’s alleged violations of BIPA “necessarily violate the plaintiffs’ substantive privacy interests.”³⁵⁰ The plaintiffs had alleged that Facebook violated BIPA’s provisions by failing to obtain written releases from each user prior to collecting, using, and storing their biometric identifiers and was therefore able to create and use face templates for each of the plaintiffs and to retain those templates for all time.³⁵¹ The Ninth Circuit found that “[b]ecause the privacy right protected

³⁴⁷ See *id.* at 1273. Specifically, the court stated:

In light of this historical background and the Supreme Court’s views regarding enhanced technological intrusions on the right to privacy, we conclude that an invasion of an individual’s biometric privacy rights ‘has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts.’

Id. (quoting *Spokeo*, 136 S. Ct. at 1549).

³⁴⁸ *Id.* at 1274 (quotation marks omitted).

³⁴⁹ *Id.* at 1273 (quoting *Carpenter v. United States*, 138 S. Ct. 2206, 2216 (2018)).

³⁵⁰ *Id.* at 1274.

³⁵¹ *Id.*

by BIPA is the right not to be subject to the collection and use of such biometric data, Facebook’s alleged violation of these statutory requirements would necessarily violate the plaintiffs’ substantive privacy interests.”³⁵² Accordingly, the court concluded, the *Patel* plaintiffs alleged a concrete injury sufficient to establish Article III standing.³⁵³

b. Texas

Texas became the second state to pass a biometric information privacy law in 2009.³⁵⁴ While the Texas statute bears many of the same characteristics of BIPA, some have referred to the Texas law as “BIPA-lite” for its lack of teeth.³⁵⁵ Unlike BIPA, the Texas law does not create a private right of action for violations of the statute³⁵⁶ but instead permits the Texas Attorney General to enforce the statute through civil actions.³⁵⁷ And while the Texas law requires notice and consent before a person may capture another’s biometric identifiers,³⁵⁸ it does not require a written release.³⁵⁹ In addition, unlike BIPA, the Texas statute does not prohibit people from profiting off of the sale of someone else’s biometric information.³⁶⁰

c. Washington

Enacted in 2017, the Washington State biometric privacy law³⁶¹ aims to protect consumers from businesses that collect biometric information without first receiving consumers’ consent.³⁶² Much like the Texas law,

³⁵² *Id.*

³⁵³ *Id.*

³⁵⁴ See TEX. BUS. & COM. CODE ANN. § 503.001 (2017).

³⁵⁵ See John G. Browning, *The Battle Over Biometrics*, 81 TEX. B.J. 674, 676 (2018).

³⁵⁶ See *id.*

³⁵⁷ See TEX. BUS. & COM. CODE ANN. § 503.001(d) (2017). The statute provides that the Texas Attorney General may obtain up to \$25,000 per violation in damages. See *id.*

³⁵⁸ *Id.* § 503.001(b)-(c). These notice and consent requirements, however, only apply to instances where the person capturing or possessing the information does so for a “commercial purpose.” See *id.*

³⁵⁹ See Browning, *supra* note 355, at 676.

³⁶⁰ See TEX. BUS. & COM. CODE ANN. § 503.001 (2017).

³⁶¹ See WASH. REV. CODE ANN. §§ 19.375.010-.040 (LexisNexis 2019).

³⁶² See *id.* § 19.375.900. In the law’s finding and intent section, the legislature noted:
[The] citizens of Washington are increasingly asked to disclose sensitive biological information that uniquely identifies them for commerce, security, and convenience. The collection and marketing of biometric information about individuals, without consent or knowledge of the individual whose data is collected, is of increasing concern. The legislature intends to require a business that collects and can attribute biometric data to a specific uniquely identified individual to disclose how it uses that biometric data, and provide notice to and

however, the Washington law does not create a private right of action but instead delegates enforcement to the Washington State Attorney General through the state's consumer protection act³⁶³ and does not require written consent.³⁶⁴ The law, which only covers commercial uses of biometric identifiers,³⁶⁵ prohibits the collection of a person's biometric identifiers "in a database for a commercial purpose" without first providing notice to and obtaining consent from that person.³⁶⁶ The Washington law also requires companies to obtain consent before selling, leasing, or otherwise disclosing a person's biometric identifiers absent specific, unique circumstances.³⁶⁷

Despite its similarities to the Texas law, the Washington law arguably provides less protection than its counterparts. When the Washington bill was originally introduced, it provided fairly robust biometric-privacy protections, including protections against surreptitious collection of biometric information through facial recognition technology.³⁶⁸ The bill's

obtain consent from an individual before enrolling or changing the use of that individual's biometric identifiers in a database.

Id.

³⁶³ See *id.* § 19.375.030(2).

³⁶⁴ See Browning, *supra* note 355, at 676.

³⁶⁵ See generally WASH. REV. CODE ANN. § 19.375.020 (LexisNexis 2019). The law defines "biometric identifier" as "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." *Id.* § 19.375.010(1).

³⁶⁶ *Id.* § 19.375.020(1).

³⁶⁷ See *id.* § 19.375.020(3). Those circumstances include instances where disclosure:

- (b) Is necessary to provide a product or service subscribed to, requested, or expressly authorized by the individual;
- (c) Is necessary to effect, administer, enforce, or complete a financial transaction that the individual requested, initiated, or authorized, and the third party to whom the biometric identifier is disclosed maintains confidentiality of the biometric identifier and does not further disclose the biometric identifier except as otherwise permitted . . . ;
- (d) Is required or expressly authorized by a federal or state statute, or court order;
- (e) Is made to a third party who contractually promises that the biometric identifier will not be further disclosed and will not be enrolled in a database for a commercial purpose inconsistent with the notice and consent described in [the statute]; or
- (f) Is made to prepare for litigation or to respond to or participate in judicial process.

Id.

³⁶⁸ See H.R. 1094, 64th Leg., Reg. Sess. § 1(4) (Wash. 2015). Specifically, the original bill's definition of "biometric identifier" included "less sensitive identifiers, including, but not

final form, however, included no reference to facial-recognition technology³⁶⁹ and excluded some of the most troubling aspects of biometric identification.³⁷⁰

2. *Applicability of State Statutes to the 10-Year Challenge*

While the state biometric-privacy laws discussed above provide additional protections to consumers, the laws nevertheless fall short of protecting consumers against pretextual-collection tactics, such as those

limited to facial imaging, voice, and gait when used specifically for identification purposes.”
Id.

³⁶⁹ See WASH. REV. CODE ANN. § 19.375.010(1) (LexisNexis 2019). The final legislation defined “biometric identifier,” in its entirety, as follows:

“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.

Id. (emphasis added).

³⁷⁰ For example, in a letter of opposition to a later form of the Washington bill, the Electronic Frontier Foundation raised the following concerns:

It appears that the bill would not address ordinary people’s concern about surreptitious collection of biometric information in commercial venues. A shopping mall could, with impunity, face-scan or iris-scan mall visitors for marketing purposes because the mall visitors would not be “access[ing] a system or account.” We think most people would be surprised that the bill excludes such biometric collection. Moreover, the mall apparently would have no duty of reasonable care under Sec. 4(a). We are also concerned that this limited definition, combined with Sec. 4 of the bill (enforcement by attorney general under state consumer protection law), will be taken to mean that the legislature is comfortable with all other biometric collection.

Letter from Lee Tien, Senior Staff Attorney, Elec. Frontier Found., to Rep. Mark Hemsworth, Wash. House of Representatives, and Rep. Jeff Morris, Wash. House of Representatives (Feb. 22, 2016), <https://bit.ly/2KN769b> [<https://perma.cc/7J8D-GGEL>]. The Washington law’s definition of “biometric identifier” no longer limits its coverage of collection of biometric data to instances where an individual “accesses a system or account.” Compare H.R. 1094, 64th Leg., Reg. Sess. § 3(2) (Wash. 2016) (““Biometric identifier” means data generated by automatic measurements of an individual’s biological characteristics . . . [used to] authenticate an individual’s identity when the individual accesses a system or account.”), with WASH. REV. CODE ANN. § 19.375.010(1) (LexisNexis 2019). Nevertheless, the current form of the law excludes from the definition “a physical or digital photograph, video or audio recording or data generated therefrom” and makes no express reference to facial recognition technology. See WASH. REV. CODE ANN. § 19.375.010(1) (LexisNexis 2019).

hypothetically behind the 10-Year Challenge.³⁷¹ The notice and consent provisions are the major force behind these laws, yet protections that hinge on consent often fall short.³⁷² When consumers consent to surrendering their data before starting to use a third party's service, they agree to continually surrender their personal information to that third party each time they use the service. Thus, each disclosure is based, at least in theory, on the consumer's own volition and uninhibited choice. That dynamic changes, however, when the party seeking the information pretextually inserts itself into the consumer's decision-making process. Because the statutory consent provisions permit businesses to use one-time consent as a license to all subsequent data gathering, nothing prevents companies from luring (or even compelling) otherwise private information into the public sphere.

Moreover, even if the statutes prohibited pretextual-collection tactics, the statutes hardly deter companies from engaging in this type of behavior. While citizens of Illinois may seek relief through private suits, citizens of Texas and Washington are forced to rely on government enforcement, which is often limited by constrained resources and enforcement priorities.³⁷³ The inherent problems of this patchwork approach to biometric privacy necessitate a federal solution.

V. PROPOSED SOLUTION

The privacy implications of biometrics extend beyond expectations of privacy in one's facial geometry or fingerprint pattern.³⁷⁴ In 2007, the U.S. government acknowledged that a person's biometric information "can be used to distinguish or trace an individual's identity."³⁷⁵ Today, both private and state actors increasingly use biometrics both to identify and to verify individuals' identities:³⁷⁶ banks have begun using facial recognition instead of PIN numbers and passwords to provide access to customers' bank

³⁷¹ See *supra* notes 3–12 and accompanying text.

³⁷² See *supra* Section III.A.1.d.

³⁷³ See *Deposit Guar. Nat'l Bank v. Roper*, 445 U.S. 326, 339 (1980) ("The aggregation of individual claims in the context of a classwide suit is an evolutionary response to the existence of injuries unremedied by the regulatory action of government.").

³⁷⁴ See *supra* notes 76–96 and accompanying text.

³⁷⁵ OMB MEMO, *supra* note 21, at 1 n.1.

³⁷⁶ See Danny Thakkar, *Global Biometric Market Analysis: Trends and Future Prospects*, BAYOMETRIC, <https://bit.ly/2VhxeVQ> [<https://perma.cc/QN8L-CLKA>].

accounts³⁷⁷ and digital wallets, such as Apple Pay,³⁷⁸ use fingerprint and facial scans to authorize payments.³⁷⁹ But some companies have gone beyond using biometrics to ensure the security of information and have instead begun trading biometric information as a commodity.³⁸⁰ Researchers even predict that marketers could one day use facial recognition technology to identify a person on the street and instantaneously retrieve that person's credit score.³⁸¹ Much like blood and DNA samples, as well as CSLI,³⁸² facial biometrics can reveal a wide swath of intimate information about a person, and the potential for misuse or mishandling of that information “may result in anxiety for the person” to whom the information is connected.³⁸³ That anxiety may only be exacerbated by recent upticks in large-scale data breaches³⁸⁴ and the proliferation of “lower cost biometric handheld devices [that] now make it possible to obtain rapid identification virtually anywhere.”³⁸⁵

Today's online society has made biometric data collection inevitable, reinforced by the unequal bargaining relationship between consumers and

³⁷⁷ See Jeanne Lee, *More Banks Turn to Biometrics to Keep an Eye on Security*, NERDWallet (May 20, 2016), <https://bit.ly/22mfaP9> [<https://perma.cc/6ZVR-89XP>].

³⁷⁸ Apply Pay is a mobile payment app that allows users to make contact-less payments. See *Pay*, APPLE PAY, <https://apple.co/1rmmha4> [<https://perma.cc/8W6G-2X55>].

³⁷⁹ See *Biometrics: Are Fingerprint ID and Facial Recognition Secure?*, FIREFLY CREDIT UNION: LIFE ILLUMINATED (Jan. 30, 2019), <https://bit.ly/2NqCZER> [<https://perma.cc/8NNY-9HYQ>].

³⁸⁰ See *supra* notes 76-96 and accompanying text.

³⁸¹ See Natasha Singer, *Face Recognition Makes the Leap from Sci-Fi*, N.Y. TIMES (Nov. 12, 2011), <https://nyti.ms/2SVfGcn> [<https://perma.cc/4HYZ-URTL>]. In a 2011 study, for example, researchers at Carnegie Mellon University used “off-the-shelf facial recognition software” to identify anonymous college students by comparing photographs of those students to photographs publicly available on Facebook. *Id.* The researchers then used the information available on some students' Facebook profiles to identify their interests and predict parts of their social security numbers. *Id.*

³⁸² See *supra* Section II.B.3.

³⁸³ *Birchfield v. North Dakota*, 136 S. Ct. 2160, 2178 (2016).

³⁸⁴ See Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N.Y. TIMES (Mar. 19, 2018), <https://nyti.ms/2HP4Dr3> [<https://perma.cc/28S5-D5ZA>] (reporting that a political data firm gained access to more than 50 million Facebook users' private information and had tools to influence voter behavior); Brian Fung, *Equifax's Massive 2017 Data Breach Keeps Getting Worse*, WASH. POST (Mar. 1, 2018), <https://wapo.st/2U5aQWr> [<https://perma.cc/K3BU-H9J2>] (reporting that as many as 147.9 million people may have been affected by the 2017 Equifax data breach, which revealed partial driver's license data of consumers).

³⁸⁵ NAT'L SCI. & TECH. COUNCIL, SUBCOMM. ON BIOMETRICS & IDENTITY MGMT., THE NATIONAL BIOMETRICS CHALLENGE 19 (Sept. 2011).

the companies that traffic in biometrics.³⁸⁶ While many companies collect biometric information for the limited purpose of providing verification technology, many others collect that information to monetize their consumers' personal identities.³⁸⁷ In fact, personal information has now, in many instances, replaced cash payments, causing many consumers to believe that the services they use each day are "free."³⁸⁸ To use the services that these companies provide, participating consumers have no option but to agree—through carefully crafted terms-of-service agreements—to hand over their personal information. But whereas consumers in the past knew what they were giving up in return for a good or service (i.e., money), consumers of these so-called "free" services often do not realize that they are in fact making payment with their personal information, an arguably much more valuable and risky form of contractual consideration.³⁸⁹ And as technology continues to pervade every aspect of modern life, consumers will only become more dependent on these services, making life in the modern world without constantly surrendering personal information nearly impossible.³⁹⁰

³⁸⁶ See A REVIEW OF THE DATA BROKER INDUSTRY, *supra* note 84, at 1–2 (discussing the recent societal shift toward conducting everyday activities on the Internet).

³⁸⁷ See McKenna, *supra* note 78, at 1067–68. According to Facebook's CEO, Mark Zuckerberg, Facebook does not sell its users' data, despite reports to the contrary. See Mark Zuckerberg, *The Facts About Facebook*, WALL ST. J. (Jan. 24, 2019), <https://on.wsj.com/33z0nGz> [<https://perma.cc/EN5R-PB8N>].

³⁸⁸ See Will Oremus, *Are You Really the Product?*, SLATE (Apr. 27, 2018), <https://bit.ly/34B7OP1> [<https://perma.cc/9MYV-RDU5>]. Mark Zuckerberg explained the payment dynamic in a *Wall Street Journal* op-ed:

[B]ased on what pages people like, what they click on, and other signals, we create categories—for example, people who like pages about gardening and live in Spain—and then charge advertisers to show ads to that category. Although advertising to specific groups existed well before the internet, online advertising allows much more precise targeting and therefore more-relevant ads. . . . In an ordinary transaction, you pay a company for a product or service they provide. Here you get our services for free—and we work separately with advertisers to show you relevant ads.

Zuckerberg, *supra* note 387.

³⁸⁹ See FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS 25–28 (Dec. 2010), <https://bit.ly/34C8pzQ> [<https://perma.cc/RSR7-SFXU>] [hereinafter FTC PROPOSED FRAMEWORK] (“[M]any data collection and use practices are invisible to consumers. . . . [C]onsumers often do not understand the extent to which their data is shared with third parties.”); McKenna, *supra* note 78, at 1067–68, 1076.

³⁹⁰ *Accord* *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018) (“[C]ell phones and the services they provide are ‘such a pervasive and insistent part of daily life’ that carrying one is indispensable to participation in modern society.” (quoting *Riley v. California*, 573 U.S. 373, 385 (2014))).

This type of arbitrary power, used to exploit an already unequal bargaining relationship, is ripe for federal constraints. Common-law remedies have not kept up with technology in protecting privacy interests.³⁹¹ And while a few state laws provide some additional protections, those protections do not cross state borders and are based on archaic understandings of consent that fail to prevent businesses from manipulating consumers into disclosing information that they would have otherwise kept private. Even broader federal consumer-protection laws fail to prevent this type of dubious conduct.³⁹²

While the Fourth Amendment's approach to privacy and modern technology can provide guidance in this area,³⁹³ Fourth-Amendment precepts—namely, the reasonable-expectation-of-privacy test—fall short of providing a biometric-privacy solution. The Government's ability to collect private information is limited by a person's reasonable expectations of privacy.³⁹⁴ On the other hand, absent industry-specific legislation, the only restraints on private industry's ability to collect biometric information are contractual arrangements between companies and consumers.³⁹⁵ Those contractual arrangements, however, arise from unequal bargaining relationships in which the consumer must choose either to accept the terms or to forgo the service. At the same time, many consumers are unaware both that private companies are handling their biometric information and, more importantly, of the breadth of information that biometrics can reveal about them.³⁹⁶ Moreover, most of those agreements do not contemplate limitations on the company's access to the information or the methods by which the company can gather the information. Accordingly, companies can use any methods they deem fit to compel consumers to disclose their information—

³⁹¹ See *supra* Section III.A.

³⁹² See FTC PROPOSED FRAMEWORK, *supra* note 389, at 19–20. Although the FTC Act prohibits “unfair or deceptive acts or practices in or affecting commerce” and provides the FTC with enforcement authority for FTC Act violations, *see* 15 U.S.C. § 45 (2018), the FTC has acknowledged “limitations” in its approach to privacy-based harms. See FTC PROPOSED FRAMEWORK, *supra* note 389, at 19–20.

³⁹³ See *supra* Section II.B.3.

³⁹⁴ See *supra* Section II.B.2–3.

³⁹⁵ See SOLOVE & SCHWARTZ, *supra* note 106, at 786–90 (discussing the United States' “sectoral approach” to consumer privacy).

Consumer privacy in the United States is regulated by ‘sectoral’ laws that focus on various sectors of the economy. Different laws regulate different industries. In contrast to the United States, Europe and many other countries have an ‘omnibus’ approach toward regulating privacy. Under an omnibus approach, one overarching statute regulates personal information use irrespective of the entities or industry that wishes to process the information. *Id.* at 786.

³⁹⁶ See Cuthbertson, *supra* note 310; *see also supra* Section I.B.

even manipulation. Each of these layers coalesce into a dynamic that undercuts application of the reasonable-expectation-of-privacy test in favor of less privacy.

The federal government has begun taking steps toward protecting biometric-information privacy through federal legislation.³⁹⁷ While those efforts are laudable, it is important for the federal response to fill the gaps in the current state statutory schemes.³⁹⁸ A federal response to appropriation by manipulation would not be the first time that the federal government has addressed such dubious behavior. For instance, in 2006, the federal government enacted the Telephone Records and Privacy Protection Act of 2006 (TRPPA),³⁹⁹ which prohibits people from “knowingly and intentionally obtain[ing], or attempt[ing] to obtain, confidential phone records information” from telecommunication providers “by (1) making false or fraudulent statements or representations to an employee of a [telecommunications provider]; [or] (2) making such false or fraudulent statements or representations to a customer of a [telecommunications provider].”⁴⁰⁰ The concern that Congress sought to address at the time was a practice known as “pretexting.”⁴⁰¹

Black’s Law Dictionary defines “pretext” as “[a] false or weak reason or motive advanced to hide actual or strong reason or motive.”⁴⁰² The concept of “pretexting” reached the public’s consciousness in 2006 after news of a spying scandal involving Hewlett-Packard broke.⁴⁰³ The reports described actions taken by Hewlett-Packard’s board of directors to identify the source of an information leak.⁴⁰⁴ According to the reports, Hewlett-

³⁹⁷ See, e.g., Personal Data Notification and Protection Act of 2017, H.R. 3806, 115th Cong. (2017); Consumer Privacy Protection Act of 2017, S. 2125, 115th Cong. (2017); H.R. 3816, 115th Cong. (2017).

³⁹⁸ At the same time, however, the federal response should not preempt state laws designed to protect biometric privacy, as some of the introduced federal legislation attempts to do. See American Data Dissemination Act of 2019, S. 142, 116th Cong. (2019).

³⁹⁹ Telephone Records and Privacy Protection Act of 2006, Pub. L. No. 109-476, 120 Stat. 3568 (codified as amended in scattered sections of 18 U.S.C.).

⁴⁰⁰ 18 U.S.C. § 1039(a)(1)–(2) (2018).

⁴⁰¹ See Telephone Records and Privacy Protection Act of 2006, Pub. L. No. 109-476 § 2(4)(B), 120 Stat. 3568.

⁴⁰² See *Pretext*, BLACK’S LAW DICTIONARY (8th ed. 1999); see also *Pretext*, BALLENTINE’S LAW DICTIONARY (3d ed. 1969) (defining “pretext” as “[a]n ostensible reason or motive assigned or assumed as a color or cover for the real reason or motive; false appearance; pretense”).

⁴⁰³ See David A. Kaplan, *Suspicious and Spies in Silicon Valley*, NEWSWEEK (Sept. 17, 2006), <https://bit.ly/37nWQhh> [<https://perma.cc/V5VW-YZR3>] (breaking the news of the Hewlett-Packard spying scandal).

⁴⁰⁴ See *id.*

Packard admitted that the board launched an investigation into the leaks, which included obtaining the phone records of board members and journalists by impersonation.⁴⁰⁵

The United States House Committee on Energy and Commerce (“Committee”) launched an investigation into Hewlett-Packard’s actions shortly after the news broke.⁴⁰⁶ During Committee hearings, members of the Committee made clear the implications of this type of activity in terms of both the general privacy concerns and the ramifications of these types of privacy intrusions:

To be clear what we are talking about, pretexting, or “social engineering,” means using fraud, deceit, and impersonation to acquire someone’s personal records without his consent. In this high-tech age, personal information is not only valuable, but vulnerable, and the relative ease with which unscrupulous pretexters can literally can their way into our personal lives is cause for great concern.⁴⁰⁷

The Committee also acknowledged and expressed surprise that the broader federal consumer protection laws—namely, Section 5 of the FTC Act—shielded against these types of acts but nevertheless failed to deter wrongdoers due to a lack of explicit statutory prohibitions:

The FTC had successfully brought pretexting cases under its Section 5 authority which prohibits unfair or deceptive acts and practices. You would have thought that that would have set the stage for understanding that this is not a legal act. A number of States, including my home State of Illinois, under our Attorney General Lisa Madigan, used their general consumer protection and consumer fraud statutes to file suits against the practice, and now, along with 11 other States, Illinois has passed a law. But obviously there are still those who missed the point and choose to dabble in what they claim is a grey area of the law.⁴⁰⁸

The Committee’s Hewlett-Packard hearings ultimately served as the catalyst for the TRPPA’s passage.⁴⁰⁹ In the TRPPA’s congressional findings, Congress noted that:

⁴⁰⁵ See Scott Horsley, *Dunn, Others Charged in HP Spying Case*, NAT’L PUB. RADIO (Oct. 4, 2006), <https://n.pr/2OxregC> [<https://perma.cc/C6V7-RR68>].

⁴⁰⁶ See James S. Granelli, *HP’s CEO Offers to Testify to Congress About Spying Scandal*, L.A. TIMES (Sept. 22, 2006), <https://lat.ms/2rVnJsM> [<https://perma.cc/XW44-AAUB>].

⁴⁰⁷ *Hewlett-Packard’s Pretexting Scandal: Hearing Before the Subcomm. on Oversight & Investigations of the H. Comm. on Energy & Commerce*, 109th Cong. 3 (2006) (statement of Rep. Ed Whitfield, Chairman, Subcomm. on Oversight and Investigations).

⁴⁰⁸ *Id.* at 17 (statement of Rep. Schakowsky).

⁴⁰⁹ See Kim Zetter, *First ‘Pretexting’ Charges Filed Under Law Passed After HP Spy Scandal*, WIRED (Jan. 9, 2009), <https://bit.ly/33EAzJv> [<https://perma.cc/TNJ3-AMQZ>]. The House

[T]elephone records have been obtained without the knowledge or consent of consumers through the use of a number of fraudulent methods and devices that include . . . “pretexting”, whereby a data broker or other person represents that they are an authorized consumer and convinces an agent of the telephone company to release the data.⁴¹⁰

Congress’s response to the pretexting problem can guide federal legislation addressing future manipulative collection tactics employed by biometric-data collectors.⁴¹¹ Like an individual who seeks to obtain telephone records by impersonating an authorized consumer, companies seeking to obtain consumers’ biometric data under false pretenses cause otherwise private information to be revealed through manipulation.

The current problem, however, raises a dilemma not present in 2006—consent. Consider the 10-Year Challenge. While pretexting occurs without the information owner’s consent, Facebook’s theoretical acquisition of users’ information occurred *after* the users consented to Facebook’s data policy. This distinction clearly complicates the comparison. The federal response must therefore reconceptualize how consumers consent to biometric data-collection practices. The validity of consent to biometric data collection should account not only for the company’s ability to collect consumers’ data but also for the *context* in which that data is made available to the company. For example, a BIPA-compliant consent agreement may suffice when consumers disclose biometric information strictly by their own volition.⁴¹² However, if a company initiates pretextual campaigns or other strategies to lure users into disclosing biometric information, then the company should be required to again (1) notify its consumers of its data-collection practices and (2) seek its consumers’ consent to collect that information on a per-capture basis.

of Representatives passed the bill in April 2006, but the Senate initially made no progress on the bill. See *H.R.4709 - Telephone Records and Privacy Protection Act of 2006*, CONGRESS.GOV, <https://bit.ly/37SRISN> [<https://perma.cc/U33Z-BPTB>] (follow “Actions” hyperlink). Three months after reports of Hewlett-Packard’s pretexting scandal broke, however, the Senate unanimously passed the bill. See *id.*

⁴¹⁰ *Id.*

⁴¹¹ The pretexting example is admittedly imperfect. Pretexting involves a third party contacting another third party to obtain an individual’s records by impersonating that individual. Appropriation by manipulation, on the other hand, involves a third party using false pretenses to coax a consumer into disclosing his or her private information. Nevertheless, both actions involve some level of deceit by the wrongdoer to obtain otherwise private information. The remedies set forth below are meant to account for the defects in the comparison. See *infra* notes 413–15 and accompanying text.

⁴¹² See *supra* note 326 and accompanying text.

The consequences for failure to comply with these requirements should not carry the same weight as the consequences attached to the TRPPA.⁴¹³ While using manipulative tactics to lure disclosure of biometric information is suspect and certainly amounts to an invasion of privacy, this type of act does not measure up to the level of fraud inherent in the pretexting scandal and should therefore not be treated as a criminal act.⁴¹⁴ Instead, the consequences should aim to promote responsible data-gathering, -storage, and -use practices without stifling innovation. Accordingly, the legislation should provide a private cause of action to injured consumers. And because damages may be uncertain,⁴¹⁵ the legislation should provide for statutory damages. By empowering the plaintiffs' bar to pursue these types of actions, companies should theoretically be more willing to comply with the requirements and, in turn, consumers may become more aware that they are disclosing sensitive information.

VI. CONCLUSION

While O'Neill's semi-sarcastic⁴¹⁶ concerns over the 10-Year Challenge's implications may have not accurately reflected the reality of Facebook's role in the challenge's inception,⁴¹⁷ the op-ed nevertheless shines light on some of the gaps in U.S. privacy law. Current U.S. laws do not adequately protect consumers' biometric information, despite the information's highly sensitive and private nature. Even laws containing relatively robust notice and consent provisions permit biometric data collectors to exploit the U.S. legal system's current understanding of "consent" by luring consumers into disclosing information that they would have retained but-for the data collector's actions. Any attempts at comprehensive federal legislation should account for these concerns.

⁴¹³ Violations of the TRPPA carry criminal penalties, including fines, imprisonment up to ten years, or both. *See* 18 U.S.C. § 1039(a).

⁴¹⁴ On the other hand, there are instances where taking such actions could warrant criminal charges. Those types of situations, however, are not contemplated in the hypothetical scenarios set forth in this Article.

⁴¹⁵ *See, e.g.,* *Kehoe v. Fid. Fed. Bank & Trust*, 421 F.3d 1209, 1213 (11th Cir. 2005) ("Damages for a violation of an individual's privacy are a quintessential example of damages that are uncertain and possibly unmeasurable.").

⁴¹⁶ *See* O'Neill, *supra* note 5 (explaining that O'Neill's argument originated from a "semi-sarcastic tweet").

⁴¹⁷ *See* Facebook Response, *supra* note 9 ("The 10 year challenge is a user-generated meme that started on its own, without our involvement. It's evidence of the fun people have on Facebook, and that's it.").