PROTECTING BIOMETRIC DATA

HYEISOO KIM

INTRODUCTION

The Fourth Amendment to the United States Constitution protects individuals from unwarranted searches and seizures, and individuals depend on their constitutional right to be free from government interference in their lives. However, the court-made "third-party doctrine" offers government officials a backdoor way of getting information from third parties' records. Instead of going through the proper procedure of getting a warrant, government officials can request information from a third party and the third party can share its consumers' information without the consumers ever knowing about the request. The third-party doctrine threatens consumers as more technologies both advance toward artificial intelligence and depend on consumers' biometric information to provide service. Consumers share their unique biological and behavioral information with companies in exchange for convenience and new technology applications. Through this doctrine, government officials can request biometric information (that is, facial scans and fingerprints from a third party).

This Note explores the Fourth Amendment, the third-party doctrine, and applications of different methods in the protection of biometric data. Part I discusses the Fourth Amendment and the third-party doctrine. It explains the history of the third-party doctrine under the most recent case: *Carpenter v. United States*. It also explores post-*Carpenter* decisions and the uncertainty behind the third-party doctrine's applicability. Part II discusses the value of biometric data and how federal and state governments recognize the significance of biometric information. Part III explains the ownership of biometric data and its relevance to arguing for Fourth Amendment protections and against the third-party doctrine. Part IV evaluates different standards that can be used to protect biometric data, including *Carpenter*'s three-part test, the reasonable expectation of privacy standard, and historical interpretations of the Fourth Amendment regarding "effects" and an individual's intent to limit exposure. This Part closes with a suggestion for judicial activism when individuals themselves are uncertain about the dangers.

I. FOURTH AMENDMENT PROTECTION

The Fourth Amendment prohibits government officials from conducting "unreasonable searches and seizures" of "persons, houses, papers, and effects."[1] Under *Boyd v. United* States, this limitation:

> "appl[ies] to all invasions on the part of the government . . . of the sanctity of a man's home and the privacies of life . . . it is the invasion

[1] U.S. CONST. amend. IV.

> of his indefeasible right of personal security, personal liberty, and private property [that constitutes the essence of the offense]."[2]

In a concurring opinion in *Katz v. United States,* Justice Harlan stated that an individual has a "reasonable expectation of privacy" in certain activities, and the Fourth Amendment protects those activities from unreasonable searches and seizures.[3] He articulated that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[4] Thus, the Fourth Amendment protection extends beyond physical boundaries.

A. AN EXCEPTION: THE THIRD-PARTY DOCTRINE

The third-party doctrine, principally born out of *United States v. Miller*[5] in 1976*,* carves out a broad exception to the Fourth Amendment. In *Miller*, the Court held that the Fourth Amendment does not protect any information that has "no legitimate 'expectation of privacy' in their contents."[6] Information without a legitimate expectation of privacy refers to "information voluntarily conveyed" by a customer and "exposed to [a third party's] employees in the ordinary course of business."[7] The case involved banks that were providing customer information to Bureau of Alcohol, Tobacco and Firearms agents: records of accounts, copies of deposit slips and checks, and financial statements with personal information. Justice Powell reasoned that the documents were not the customer's papers and, thus, did not fall within the textual interpretation of the Fourth Amendment. Additionally, a customer could "assert neither ownership nor possession" over the document and records because they were "business records . . . not confidential communications but negotiable instruments to be used in commercial transactions."[8]

Under the third-party doctrine, any individual who voluntarily shares any personal information for a limited purpose with a third party—even with an expectation of confidentiality—cannot protest nor invoke a constitutional right when a government official requests that information from the third party. A few years later, the Court further tested and strengthened the doctrine in the context of a telephone company sharing a list of phone numbers dialed by a customer, because the customer voluntarily shared that information with the company.[9]

Justices have repeatedly expressed concerns with the third-party doctrine, which emphasizes the consequences of permitting loose application. In *Miller*, Justice Brennan dissented against the third-party

---

[2] Boyd v. United States, 116 U.S. 616, 630 (1886).
[3] Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).
[4] *Id.* at 351.
[5] United States v. Miller, 425 U.S. 435 (1976).
[6] *Id.* at 442.
[7] *Id.*
[8] *Id.* at 440, 442.
[9] Smith v. Maryland, 442 U.S. 735, 742 (1979) ("All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed.").

doctrine.[10] Justice Brennan noted that a customer's consent to a third party's use of their information for internal business purposes did not represent valid consent for the third party to further share that information with the police.[11] Justice Brennan reasoned that access to information can lead to an intrusion of legitimate expectation of privacy because "[f]inancial transactions can reveal much about a person's activities, associations, and beliefs."[12]

In a dissent to *Smith v. Maryland*, Justice Stewart articulated that *Katz* protected numbers dialed from a private telephone because there is a reasonable expectation of privacy for information captured from conduct within a person's home.[13] More importantly, such information is "an integral part of . . . telephon[e] communication," because a call cannot be completed without dialing a phone number.[14] The captured phone numbers can "reveal the most intimate details of a person's life" because they can "reveal the identities of the persons and . . . places" related to the phone number.[15] Justice Marshall, joined by Justice Brennan, also dissented against the notion that customers have assumed the risk of surveillance from government officials. Justice Marshall stated that a customer has not chosen to assume any risk because the customer has "no realistic alternative" to using a service, which "for many has become a personal or professional necessity."[16] In a concurring opinion to the 2012 decision *United States v. Jones*, Justice Sotomayor stated that the third-party doctrine is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[17]

B. CARPENTER V. UNITED STATES

The most recent Supreme Court case concerning the third-party doctrine offers additional schemes for protecting information relating to a person's identity. The Court in *Carpenter v. United States* declined to apply the third-party doctrine in a case of government access to cell phone locations.[18] The Court decided that government access to 127 days of cell phone location data, which showed 12,898 location points, without a warrant, constituted a search and thus violated the Fourth Amendment. Chief Justice Roberts, writing for the majority, stated that given the "unique nature" of the information, a third party's access does not overcome "the user's claim to Fourth Amendment protection."[19] Justice Robert listed three key factors in determining whether third-party information deserves Fourth Amendment protection: (1) the deeply revealing nature of the information; (2) its depth, breadth, and comprehensive reach; and (3) the inescapable and automatic nature of its collection.[20]

[10] *Miller*, 425 U.S. at 447 (Brennan, J., dissenting).
[11] *Id*. at 448.
[12] *Id*. at 453.
[13] *Smith*, 442 U.S. at 747–48 (Stewart, J., dissenting).
[14] *Id.* at 747.
[15] *Id.* at 748.
[16] *Id.* at 750 (Marshall, J., dissenting).
[17] United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).
[18] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).
[19] *Id.* at 2217.
[20] *Id*. at 2223.

Echoing some of the concerns from the previous decisions, Justice Roberts rejected an extension of the third-party doctrine and stated that the government's access violated *Carpenter*'s reasonable expectation of privacy in his physical movements. Justice Roberts refused a broad allowance of the third-party doctrine because it contradicted an individual's "anticipation of privacy in his physical location."[21] Justice Roberts compared the modern tracking capabilities to traditional investigative tools.[22] He concluded that modern technology allows for the government to access a "deep repository of historical location information at practically no expense" and gain an ability to "travel back in time to retrace a person's whereabouts," which makes the depth of a search as comprehensive as the information a third party collects.[23] Ultimately, Justice Roberts used the three-factor test to determine the applicability of this doctrine.

In a dissenting opinion, Justice Kennedy stated that "individuals have no Fourth Amendment interests in business records which are possessed, owned, and controlled by a third party";[24] thus, individuals have no meaningful interest and no reasonable expectation of privacy in the records that they are not storing, modifying, or destroying.[25] Justice Kennedy also reasoned that the government has a compelling interest in taking necessary steps to stop crime.[26]

Similarly, in a separate dissent, Justice Thomas stated that the government did not search an individual's property because the user "did not create the records, he d[id] not maintain them, he cannot control them, and he cannot destroy them."[27] Justice Thomas emphasized the history and the text of the Fourth Amendment to highlight the problematic existence of the reasonable expectation of privacy. Also, Justice Thomas reasoned that neither the terms of the contract nor the provisions of the law gave the user any property rights. In his dissent, Justice Alito noted that allowing an individual "to object to the search of a third party's property . . . is revolutionary" because the Fourth Amendment does not guarantee the right for a person to bring a claim regarding another's persons, houses, papers, and effects.[28]

Justice Gorsuch dissented, suggesting three alternatives to responding to the evolving interpretation of the Fourth Amendment that allow for a reasonable expectation of privacy and the third-party doctrine: (1) allow the third party to reduce the Fourth Amendment rights "to nearly nothing"; (2) revive the reasonable expectation of privacy in the light of modern technology; or (3) "look for answers elsewhere."[29] Justice Gorsuch explained that the last approach solely relies on the original understanding of whether "a house, paper or effect was *yours* under [the] law," and the Fourth Amendment protection for the enumerated items prevails even if such

[21] *Id*. at 2217–18.
[22] *Id.* at 2216–17.
[23] *Id*. at 2218.
[24] *Id.* at 2223 (Kennedy, J., dissenting).
[25] *Id.* at 2227.
[26] *Id.* at 2229–30.
[27] *Id.* at 2235 (Thomas, J., dissenting).
[28] *Id.* at 2247 (Alito, J., dissenting).
[29] *Id.* at 2262 (Gorsuch, J., dissenting).

information is shared with third parties.[30] Justice Gorsuch leaned into the idea of bailment—a consumer is a bailor and the third party is a bailee. The bailor delivers personal information to the bailee, and the bailee must keep the entrusted material safe. He, alongside Justice Kennedy, interpreted data as "modern-day . . . papers or effects" in some cases.[31] Lastly, Justice Gorsuch suggested that neither complete ownership nor having a choice in entrusting data is required to exercise the Fourth Amendment right.[32]

C. POST-*CARPENTER* INCONSISTENCIES

Between the 2018 *Carpenter* decision and March 31, 2021, federal and state courts substantively applied *Carpenter* 399 times.[33] From those rulings, courts found a Fourth Amendment search in 34.1% of the rulings and did not find a search in 65.9% of the rulings.[34] Both federal and state courts applied the third-party doctrine and allowed for government officials to gain access in varying situations: user-generated location information from websites,[35] recordings of internet protocol ("IP") addresses,[36] doctors' prescription records,[37] patients' prescription drug records,[38] information located on the virtual currency's blockchain,[39] historical transactional data of cryptocurrency,[40] GPS data on rental cars,[41] and e-mail addresses.[42]

The lower courts inconsistently apply Justice Roberts's *Carpenter* factors. Courts have noted that certain elements favored or disfavored the moving party.[43] Courts have also discussed some of the factors that affected their reasoning while not mentioning other relevant factors; the courts' reasoning has revolved around certain factors more than others.[44] Overall, the outcome of a case is influenced by the revealing nature of the data, the amount of data collected, and the automatic nature of data disclosure, while the factors considering the number of persons affected minimally impact a case.[45]

Despite these variations, federal and state courts have consistently recognized the importance of protecting biometric data. The Seventh Circuit noted the existing "threat of irreparable privacy harms, identity theft, and other economic injuries [against consumers] arising from the increasing use of biometric identifiers and information by private entities."[46] The District

[30] *Id.* at 2268.
[31] *Id.* at 2269.
[32] *Id.* at 2268–71.
[33] Matthew Tokson, *The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law*, 2018-2021, 135 HARV. L. REV. 1790, 1808 (2022).
[34] *Id.* at 1809.
[35] United States v. Bledsoe, 630 F. Supp. 3d 1 (D.D.C. 2022).
[36] United States v. Soybel, 13 F.4th 584 (7th Cir. 2021).
[37] United States v. Gayden, 977 F.3d 1146 (11th Cir. 2020).
[38] U.S. Dep't of Just. v. Ricco Jonas, 24 F.4th 718 (1st Cir. 2022).
[39] United States v. Gratkowski, 964 F.3d 307 (5th Cir. 2020).
[40] *In re* the Search of Multiple Email Accts. Pursuant to 18 U.S.C. § 2703 for Investigation of Violation of 18 U.S.C. § 1956, 585 F. Supp. 3d 1 (D.D.C. 2022).
[41] United States v. Brown, 627 F. Supp. 3d 206 (E.D.N.Y. 2022).
[42] United States v. Trader, 981 F.3d 961 (11th Cir. 2020).
[43] Tokson, *supra* note 33, at 1821.
[44] Tokson, *supra* note 33, at 1822.
[45] Tokson, *supra* note 33, at 1822.
[46] Bryant v. Compass Grp. USA, Inc., 958 F.3d 617, 619 (7th Cir. 2020).

Court for the Northern District of California emphasized the role of biometric identifiers "in our digital world because technology now permits the wholesale collection and storage of an individual's unique biometric identifiers—identifiers that cannot be changed if compromised or misused."[47] In 2019, the Illinois Supreme Court decided that "[t]he injury is real and significant" when a private entity fails to adhere to statutory procedures to protect consumers' biometric data.[48] A recent Illinois Supreme Court decision echoed the Illinois General Assembly's concerns about the "risks to the public surrounding the disclosure of highly sensitive biometric information" by holding that individuals have five years to bring any claim under the Biometric Information Privacy Act.[49] The irregular application of *Carpenter* leaves room for implementing other ways of protecting biometric data from the third-party doctrine.[50]

II. VALUE OF BIOMETRIC DATA

The expanding world of intangible property, often based on assets available on the Internet or information shared through intangible connections, demands further analysis into protecting the consumer as part of a sales transaction, because intangible assets, particularly biometric data, are a commodity. Biometric data refers to information with "unique physical characteristics, such as fingerprints, that can be used for automated recognition."[51] Any information that defines or helps identify an individual can be considered biometric data. It can include biological and behavioral measurements such as fingerprints, face scans, DNA, blood, voice recordings,[52] gait, and gestures.[53] Many sectors brand the collection of biometric information as a unique feature of their service: a bank collects voice recordings to identify its customers over the phone;[54] an online retail giant focuses on a customer's palm print for payment;[55] and membership to an airport security clearance program allows expedited access through TSA checkpoints in exchange for travelers' iris scans.[56] In the name of convenience and innovation, businesses transform an individual's body parts, both tangible and intangible, into a commercial feature. Tech-driven companies highlight the extreme convenience of sharing biometric

[47] Patel v. Facebook Inc., 290 F. Supp. 3d 948, 954 (N.D. Cal. 2018).
[48] Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1206 (Ill. 2019).
[49] Tims v. Black Horse Carriers, Inc., 2023 IL 127801, ¶ 39.
[50] Tokson, *supra* note 33, at 1822.
[51] *Biometrics*, DEP'T HOMELAND SEC., https://www.dhs.gov/biometrics [https://perma.cc/W37U-AD5E] (last updated Dec. 14, 2021).
[52] Samantha Hawkins, *'Voiceprints' Roil Companies as Biometrics Litigation Skyrockets*, BLOOMBERG L. (May 18, 2022, 1:45 AM), https://news.bloomberglaw.com/privacy-and-data-security/voiceprints-roil-companies-as-biometrics-litigation-skyrockets [https://perma.cc/FEV2-QT9G].
[53] *Biometrics: Definition, Use Cases, Latest News*, THALES, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics [https://perma.cc/V6ZR-PGXM] (last updated May 20, 2023).
[54] *Schwab Voice ID Service*, CHARLES SCHWAB BANK, https://www.schwab.com/voice-id [https://perma.cc/3MVK-2LBA] (last visited Feb. 14, 2023).
[55] *Amazon One*, AMAZON, https://one.amazon.com [https://perma.cc/E77T-P4RW] (last visited Feb. 14, 2023).
[56] *How it Works: Stress-Free Airport Security Nationwide*, CLEAR, https://www.clearme.com/how-it-works [https://perma.cc/T5KY-LL5U] (last visited Feb. 14, 2023).

information with the company,[57] and the race to collect as much information as possible leaves much to wonder about the protection of the collected information from unwarranted access.

The increasing prevalence of biometric data in consumer products leads a user to reasonably expect adequate protection of their fingerprints for computer access,[58] their facial scans for mobile device access,[59] and their iris scans for access to their university's gym and dining hall[60] from unwarranted searches and government access. In 2022, the biometric system market was valued at 30.77 billion U.S. dollars ("USD") and is expected to grow to 76.70 billion USD by 2029.[61] Biometric information originates from a person and only has value because it relates to an individual. The innate worth of biometric data increases the risk of exploitation and confuses ownership rights because companies share and sell biometric information without a person ever knowing. A person is powerless against the exploitation of unique personal information, so they lack autonomy over themselves.

Similarly, any individual partaking in the current technology-driven society likely expects to have a claim over their biometric information against any unwarranted searches and seizures. *Carpenter* neither dismissed nor overruled the application of the third-party doctrine to these scenarios. Access to personal information through the third-party doctrine still exists, and the threat of abuse still looms over any consumer who uses an online service.

A. COMMERCIALIZATION OF BIOMETRIC DATA

Biometric data is valuable because there is a market that is fueled by a desire to know everything about a person. The market for an individual's biometric data is particularly well-documented in the world of sports gambling. Coaches and fans pour over collegiate and professional athletes' health and performance information that is gathered from wearable sports technology[62] and surveillance cameras.[63] The market for athletes' biometric data continues to grow as gamblers seek insights about specific athletes to predict their movement and bodily reaction in certain competitions.

---

[57] Janet Vertesi, *Data Free Disney*, PUB. BOOKS (Jan. 31, 2023), https://www.publicbooks.org/data-free-disney [https://perma.cc/LH3X-8FBV].

[58] Press Release, Fingerprints, Lenovo, the World's Largest PC Maker, Launches Its First Two Laptop Models with Fingerprints' Biometric PC Solution (Mar. 10, 2022), https://www.fingerprints.com/uploads/nasdaq-v2/press-releases/2022/03/fingerprints-press-release-202203100830-220310-lenovo-biometric-pc.pdf [https://perma.cc/C9JJ-KPST].

[59] *About Face ID Advanced Technology*, APPLE (Aug. 22, 2023), https://support.apple.com/en-us/HT208108 [perma.cc/QU89-6ZLB].

[60] *Iris Camera System*, UNIV. OF GA., https://dining.uga.edu/about/iris [perma.cc/HY6F-J9U7] (last visited Feb. 14, 2023).

[61] *Biometric System Market Size Worth USD 76.70 Billion By 2029: Report by Fortune Business Insights*, GLOBENEWSWIRE (Jan. 17, 2023, 7:16 AM), https://www.globenewswire.com/news-release/2023/01/17/2589810/0/en/Biometric-System-Market-Size-Worth-USD-76-70-Billion-by-2029-Report-by-Fortune-Business-Insights.html [https://perma.cc/22GX-ZCT3].

[62] *How Wearable Tech is Transforming a Coach's Decision-Making*, OHIO UNIV. (Jan. 23, 2020), https://onlinemasters.ohio.edu/blog/how-wearable-tech-is-transforming-a-coachs-decision-making [https://perma.cc/B7R5-DNKA].

[63] David Jarvis & Kevin Westcott, *The Hyperquantified Athlete: Technology, Measurement, and the Business of Sports*, DELOITTE (Dec. 7, 2020), https://www2.deloitte.com/xe/en/insights/industry/technology/technology-media-and-telecom-predictions/2021/athlete-data-analytics.html [https://perma.cc/AS8A-NYU3].

Biometric data is also shared and sold more discreetly than in the case of collegiate and professional athletes. In 2022, Clearview AI—a company that collects and sells faceprints—entered a settlement with the ACLU to stop selling faceprints to private U.S. companies.[64] Clearview AI has an image database with billions of individuals' faces from the Internet. Before the settlement, any party could pay Clearview AI for access to the database. Upon uploading a photo of an individual, the database connects the photo with all available information about the individual, including their name, residence, occupation, and known acquittances.[65]

Further, the American health data marketplace already exists, foreshadowing the abuse that will come from the lack of protection for other sensitive biometric data. Information shared with virtual health and health-related apps is often not protected by the Health Insurance Portability and Accountability Act ("HIPAA"),[66] and there is an active market in which data brokers could buy and sell sensitive mental health data. One study even shows the process of buying American health data, including how much a data brokerage firm charges for service and records: $275 for 5,000 aggregated counts of Americans' mental health records; $0.20 per record for a minimum spending of $2,000; $15,000 to $100,000 a year for data subscription; and $793.90 to rent 15,378 records.[67] From purchasing or renting the records, highly sensitive data can be accessed, such as information on "depression, attention disorder, insomnia, anxiety, ADHD, and bipolar disorder as well as data on ethnicity, age, gender, zip code, religion, children in the home, marital status, net worth, credit score, date of birth, and single parent status."[68] Such a marketplace is just one example of many different marketplaces that may already exist to collect individuals' biometric information without their consent or knowledge. Commercializing biometric data without an individual's consent threatens individual identity; it promotes lawlessness and exploitation of loopholes at the expense of unaware citizens.

B. STATE PROTECTION OF BIOMETRIC DATA

1. Lack of Federal Protection

There is no specific federal protection for biometric information. But, individuals enjoy certain related legislative protections: HIPAA protects information related to medical records;[69] the Fair Credit Reporting Act ("FCRA") protects against undisclosed use of an individual credit report and provides the right for the consumer to know what kind of information is held

[64] Press Release, ACLU, In Big Win, Settlement Ensures Clearview AI Complies With Groundbreaking Illinois Biometric Privacy Law (May 9, 2022, 11:45 AM), https://www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois [https://perma.cc/GXR9-8P3F]; ACLU v. Clearview AI, Inc., 2021 Ill. Cir. LEXIS 292 (2021).

[65] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It,* N.Y. TIMES (Nov. 2, 2021), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/QPQ2-G6YN].

[66] Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 2033 (1996).

[67] JOANNE KIM, DATA BROKERS AND THE SALE OF AMERICANS' MENTAL HEALTH DATA: THE EXCHANGE OF OUR MOST SENSITIVE DATA AND WHAT IT MEANS FOR PERSONAL PRIVACY 8–9 (2023).

[68] *Id.* at 4.

[69] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936.

by a consumer reporting agency;[70] and the Family Educational Rights and Privacy Act ("FERPA") protects student and parental control over the student's education records.[71] Federal legislation protecting biometric data has been introduced from both sides of the political aisle, yet no piece of legislation has garnered enough support for Congressional enactment.[72] Proposals from past years still sit in limbo after their introduction.[73]

However, the interest in protecting biometric information is gathering momentum as biometric technology becomes more embedded in individuals' lifestyles. In 2021, the White House Office of Science and Technology Policy published a Request for Information ("RFI"), asking both public and private sector firms about their policies and uses of biometric technologies.[74] The RFI was intended to help collect information about "past deployments, proposals, pilots, or trials, and current use of biometric technologies for the purposes of *identity verification, identification of individuals, and inference of attributes including individual mental and emotional states*."[75] The RFI was published in response to entities using biometric information for "*identification* or *inference* of emotion, disposition, character, or intent"; it also recognized the existing concerns about manipulation and "the role of biometric systems in increasing the use of surveillance technologies and broadening the scope of surveillance practices."[76]

Lacking federal regulation, individuals turned to their elected representatives to protect their online information. With states like California and Illinois leading the charge towards biometric regulation, many other states are proposing and enacting legislation to partially protect online biometric information.[77] However, the state protection only extends to the residents of that state; thus, certain oppressed or underrepresented populations will once again be disproportionately affected by the lack of protection.

2. California

The California Constitution protects people's "inalienable rights" in "pursuing and obtaining . . . privacy."[78] The California Consumer Privacy Act of 2018 ("CCPA") protects consumer information from certain third-

[70] 15 U.S.C. § 1681 et seq; *see* SUMMARY OF YOUR RIGHTS UNDER THE FAIR CREDIT REPORTING ACT, CONSUMER FIN. PROT. BUREAU, AGENCY (last visited Sept. 8, 2023), https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf [https://perma.cc/CJN2-RSK5].

[71] 20 U.S.C. § 1232g; *see Family Educational Rights and Privacy Act (FERPA)*, U.S. DEP'T OF EDUC., https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html [https://perma.cc/F9TU-VRDZ] (last updated Aug. 25, 2021).

[72] MÜGE FAZLIOGLU, US FEDERAL PRIVACY LEGISLATION TRACKER: INTRODUCED IN THE 117TH CONGRESS (2021-2022), https://iapp.org/media/pdf/resource_center/us_federal_privacy_legislation_tracker.pdf [https://perma.cc/53W7-JWU3].

[73] *See, e.g.*, National Biometric Information Privacy Act of 2020, S. 4400, 116th Cong. (2020).

[74] Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies, 86 Fed. Reg. 56300 (Oct. 8, 2021).

[75] *Id.*

[76] *Id.*

[77] BRYAN CAVE LEIGHTON PAISNER LLP, U.S. BIOMETRIC LAWS & PENDING LEGISLATION TRACKER (June 2, 2023), https://www.bclplaw.com/en-US/events-insights-news/us-biometric-laws-and-pending-legislation-tracker.html [https://perma.cc/V436-ATG2].

[78] CAL. CONST. art. I § 1.

party behaviors.[79] Amongst other rights, a consumer has the right to direct a business not to sell their personal information (referred to as the "right to opt-out") and "the right to request that a business delete any personal information about the consumer which the business has collected from the consumer."[80] A consumer's personal information relates to an individual's physiological, biological, or behavioral characteristics including DNA, "imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information."[81]

Additionally, the California Privacy Rights Act ("CPRA") amended the CCPA and added new provisions, including establishing the California Privacy Protection Agency.[82] CPRA applies to any for-profit legal entity doing business in California that collects consumers' personal information.[83] It requires a third party to allow users to opt-out of certain data usage if it wishes to use their personal information for any purpose other than those enumerated in the CPRA. If businesses use sensitive personal information beyond the purpose expressly permitted by the CPRA, the business must include a link on their website providing consumers with a way to limit the use of their information.[84] Also, businesses must make attempts to correct their data by using "commercially reasonable efforts to correct the inaccurate personal information as directed by the consumer."[85]

The CCPA and CPRA explicitly deal with the issue of control that the *Carpenter* dissenters discussed.[86] The legislation offers consumers a right to opt-out of the unpermitted sale of their personal information. More importantly, the state legislation grants the consumers rights to delete and correct all personal information that a third party may have. Thus, the consumer directly controls all biometric identifiers maintained by a third party, at least to a point. Though the consumer will neither maintain nor collect, they can exercise their right to delete, correct, and limit the usage and disclosure. Therefore, the third party relinquishes at least some rights. California courts and courts that deal with a California business must consider the state legislation that specifically protects consumers from unwanted disclosure of their information. Thus, the public's desire to control their data works against the dissenters in *Carpenter* who theorized that individuals have no meaningful interest or control over their biometric data that's held by a third party.

[79] CAL. CIV. CODE § 1798.100 et seq.
[80] CAL. CIV. CODE § 1798.105(a).
[81] CAL. CIV. CODE § 1798.140.
[82] CAL. CIV. CODE § 1798.145.
[83] *Id.*
[84] *CPRA On the Way*, ORRICK, https://www.orrick.com/en/Solutions/CPRA [https://perma.cc/RXZ9-LCCH] (last visited Sept. 4, 2023).
[85] CAL. CIV. CODE § 1798.106(c).
[86] *CCPA vs CPRA: What's the Difference?*, BLOOMBERG L. https://pro.bloomberglaw.com /brief/california-consumer-privacy-laws-ccpa-cpra [https://perma.cc/RXF4-AJS8] (last visited Sept. 4, 2023).

3. Illinois

The Illinois Constitution protects against "invasions of privacy or interceptions of communications by eavesdropping devices or other means."[87] The Illinois Biometric Information Privacy Act ("BIPA") protects against an unauthorized collection or use by a third party of any customer's "biometric identifier" such as "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[88] Any third party must first provide a written explanation that it will collect or store a biometric identifier for a certain length of time for a certain purpose. If the consumer provides written consent, then the third party may possess the consumer's biometric identifier. Furthermore, no third party may disclose a person's biometric identifier without consent unless it complies with established law.[89] BIPA uniquely allows for a private right of action, permitting "any person aggrieved by a violation" to bring a suit in either state or federal court.[90]

The Illinois Supreme Court held that a private entity violates an individual's right when the private entity fails to satisfy any of the factors listed in BIPA regarding collecting, retaining, disclosing, and destroying an individual's biometric identifiers;[91] thus, any violation is an "invasion, impairment, or denial of the statutory rights of any person or customer whose biometric identifier or biometric information is subject to the breach."[92] Additionally, state and federal courts have held that compliance costs are insignificant compared to the "substantial and irresistible harm that could result if biometric identifiers and information are not properly safeguarded."[93]

Illinois provides specific rights through clear steps. BIPA applies to a private entity and outlines obligations to consumers regarding safeguarding and managing their information. Since a consumer must explicitly consent to the collection of their biometric information, any uncertainty around whether a consumer genuinely consented is removed. BIPA focuses on collecting biometric information without consent or disclosure, yet the provisions in BIPA reflect the consumer's interest in their biometric data and that they exercise rights over it. By referencing to BIPA, state and federal courts may be more convinced that consumers are entitled some property rights in their biometric data and that without their consent, thirty parties' disclosures of such information violate consumers' Fourth Amendment rights.

---

[87] ILL. CONST. art. I, § 6.
[88] 740 Ill. Comp. Stat. Ann. § 14/10 (LexisNexis 2013).
[89] *Id.* § 14/15(b)–(d).
[90] *Id.* § 14/20.
[91] Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1206 (Ill. 2019).
[92] *Id. See also* Patel v. Facebook Inc., 290 F. Supp. 3d 948, 1274 (N.D. Cal. 2018) (finding that BIPA was established to protect an individual's "concrete interests" in privacy, not solely their procedural rights).
[93] Sosa v. Onfido, Inc., 600 F. Supp. 3d 859, 884 (N.D. Ill. 2022) (citing Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1207 (2019)); *see also* Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019).

III. WHO OWNS BIOMETRIC DATA?

Ownership of biometric data is constantly disputed amongst scholars. Some argue that an intentional definition of property can provide clarity under the Fourth Amendment.[94] Others say that due to the nature of the biometric data collection and the parties involved in its creation, "parties can allocate the ownership and use of different categories of data through contract law."[95] This Note will next discuss the plausible ways to think about biometric data ownership.

A. THE INDIVIDUAL: INTERPRETATION OF "EFFECTS" UNDER THE FOURTH AMENDMENT

The inconsistencies among the constitutional theories make it difficult to predict the scope of a person's biometric data within the Fourth Amendment. The Roberts Court shows a preference for text and history over other methods of constitutional interpretations; thus, it is helpful to understand the scope of the word "effects" in the Amendment through textual and historical lenses.

Early cases focused on physical trespass to determine whether there was a search, without much regard to "effects."[96] Even in the face of technological development, if a government official did not physically enter a private space, the Supreme Court often refused to determine that there was a search.[97] As time passed and technology advanced, the lower courts leaned into the idea of subjective and objective expectations of privacy.[98] The word "effects" in the Fourth Amendment has so far meant: a vehicle,[99] wrapped or sealed parcel delivered to a private freight carrier,[100] suitcases,[101] beehives,[102] a person's pet dog,[103] locked containers and packages,[104] and personal email[105] in various courts.

In *Carpenter*, Justices Gorsuch and Kennedy gave thought to treating virtual information as "modern-day papers and effects."[106] In some cases, the treatment of the text "effects" expanded to encompass tangibly related items to intangible information that have meaning to an individual's property. The

[94] Joao Marinotti, *Escaping Circularity: The Fourth Amendment and Property Law*, 81 MD. L. REV. 641 (2022).

[95] John T. Holden & Kimberly A. Houser, *Taboo Transactions: Selling Athlete Biometric Data*, 49 FLA. ST. U. L. REV. 103, 141 (2021).

[96] *See* United States v. Jones, 565 U.S. 400, 406 (2012) ("[F]or most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates.").

[97] *See* Olmstead v. United States, 277 U.S. 438, 466 (1928) (holding that wiretapping telephones without trespassing defendants' property does not constitution a Fourth Amendment search because of lack of entry of defendants' property).

[98] *See* Katz v. United States, 389 U.S. 347 (1967) (Harlan, J., concurring).

[99] United States v. Chadwick, 433 U.S. 1, 12 (1977).

[100] United States v. Jacobsen, 466 U.S. 109, 114 (1984); United States v. La France, 879 F.2d 1, 4 (1st Cir. 1989).

[101] United States v. Soriano, 482 F.2d 469, 472 (5th Cir. 1973).

[102] Allinder v. Ohio, 808 F.2d 1180, 1186 (6th Cir. 1987).

[103] Maldonado v. Fontanes, 568 F.3d 263, 270-71 (1st Cir. 2009).

[104] Chrispen v. Sec'y, Fla. Dep't of Corr., 246 Fed. Appx. 599 (1st Cir. 2007).

[105] Grand Jury Subpoena v. Kitzhaber, 828 F.3d 1083 (9th Cir. 2016).

[106] Carpenter v. United States, 138 S. Ct. 2206, 2269 (Gorsuch, J., dissenting).

trend points to "effects" encompassing online information to ultimately allow the individual to claim ownership of biometric data.

B. A TEMPORARY JOINT-OWNERSHIP: APPLICATION OF *CARPENTER*'S DISSENTS

Carpenter's dissenting opinions also point to the individual's ownership of biometric data, depending on state property law. In *Carpenter*, Justices Kennedy, Thomas, and Alito exclusively relied on historical and textual evidence to emphasize third-party ownership of consumer records. Justice Kennedy relied on the facts of a consumer not partaking in regulating their personal information.[107] Justice Thomas stated that an individual may not claim property rights in intangible objects if they do not create, maintain, control, or destroy them.[108] Their emphasis on an individual's participation in the life cycle of a record may direct lower courts to look for an individual's property rights based on how much interaction the individual has with a third-party database. However, the unique nature of biometric information begs for additional scrutiny regarding the application of property law theories on biometric records.

From the beginning, consumers partake in creating biometric information because they provide essential information. The record could not be created without a consumer providing part of their physical identity to the third party. The physical identity is unique to the consumer; thus, it cannot be taken from triangulating unrelated data. Additionally, as long as the consumer uses a third-party product, they interact with their biometric information. If a consumer wants to sign into their electronic device or service, they must provide their fingerprint or face scan to confirm and securely gain access. Such common daily interaction exemplifies how a consumer's usage automatically triggers maintenance of the biometric information record in a third-party database; if the consumer's physical, biological, or behavioral measurements change, the third-party database likely captures it. Through simple examples of consumer interaction with a third party, a consumer exerts constant presence in the life cycle of biometric data.

Even within property law, it is too broad to claim that property rights belong to the person who controls it; a single focus on physical ownership is inappropriate for a complex society where an individual may connect to other forms of ownership. Instead, valuing a person's "self-determination that allows us to make meaningful choices" offers a more accurate lens into understanding ownership over biometric data.[109] In *Carpenter*, Justice Gorsuch's analysis suggests consideration of societal expectations and social norms.[110] His approach to modern electronic data is inspired by property rights—which differs from Justice Powell's opinion in *Miller*—that states that since certain documents were not a customer's "private papers," they did

[107] *Id*. at 2229–30 (Kennedy, J., dissenting).
[108] *Id*. at 2235 (Thomas, J., dissenting).
[109] Christopher K. Odinet, *Data and the Social Obligation Norm of Property*, 29 CORNELL J. L. & PUB. POL'Y 643, 668 (2019).
[110] *Id.* at 663.

not fall within the Fourth Amendment protection.[111] If a consumer temporarily entrusts possession of their biometric information to a third party, then the third party owes a duty to the consumer and cannot use the biometric information outside the purpose of the bailment. This way of considering property respects a person's innate need to guard their most personal and unique possession.

C. THE COMMUNITY: SOCIAL NORMS OF PROPERTY

In considering societal expectations and social norms, an individual's actions as a consumer cannot properly reflect consent or waiver. According to Professor Cass R. Sunstein, a citizen acts differently from a consumer because different priorities drive these two roles; people acting as citizens try to change social practices while people acting as consumers focus on their interactions with service providers.[112] In private, citizens wish to safeguard their personal information. Thus, people who are aware of the danger behind the exploitation of biometric data speak through their representatives to enact laws that protect their information or bring awareness to others to collectively change existing norms. Yet, when people act as consumers, they continue to share even the most sensitive and personal information at whim for various online and technology services. Market-driven technology feeds on consumers' willingness and obliviousness to share their biometric identifiers. However, willingness cannot be considered a social norm because social norms differ from market norms. Societal expectations consider a person's actions as a citizen, enacting a collective change for the public good while market norms consider a person's actions as a consumer and their engagement in the exchange of goods and services.[113] Therefore, Justice Gorsuch's inclusion of societal expectations and social norms would focus on the conduct of citizens, not consumers, and their choices made without the full knowledge of the existence of the backdoor method of government gaining access to private information.

In the context of biometric data, in which the question of ownership is unclear, it may also be necessary to consider a social obligation norm in property law. A social norm of property rights requires "some social vision . . . of the common good that serves as the fundamental context for the exercise of the rights and duties of private ownership."[114] An extreme community-based obligation depends on justice; however, the theory of justice eventually leads to a conclusion of promoting wealth and property distribution, an idea that is contrary to the Constitution and individual rights. However, rather than fully implementing a social-obligation norm, understanding community-based property rights helps diffuse the tension over ownership claims in online information, including a person's biometric data.[115]

---

[111] *See* United States v. Miller, 425 U.S. 435, 440 (1976).
[112] Cass R. Sunstein, *Social Norms and Social Roles*, 96 COLUM. L. REV. 903, 923–25 (1996).
[113] *Id.*
[114] Gregory S. Alexander, *The Social-Obligation Norm in American Property Law*, 94 CORNELL L. REV. 745, 757 (2009).
[115] Odinet, *supra* note 109, at 667–68.

IV. PROTECTING BIOMETRIC DATA

A. *CARPENTER*'S THREE-PART TEST PROTECTS BIOMETRIC DATA

This section applies the three-part test introduced in *Carpenter* to biometric information. The overall analysis calls for the protection of biometric information from the third-party doctrine.

1. Deeply Revealing Nature

The Court analyzed the deeply revealing nature of the information that works as "an intimate window into a person's life" by revealing movement and a person's associations; this first factor does not grant protection for biometric data against the third-party doctrine.[116] In *Carpenter*, the compilation of the cell phone locations provided an intimate window into "an all-encompassing record of the holder's whereabouts."[117] Biometric information does not report any active data to a third party. It does not work as an intimate window because it does not show a person's associations.

On the other hand, even though it is harder to decipher embedded information within a piece of biometric information than it is to utilize a more direct piece of information, such information has a deeply revealing nature to those who have access to technology that can unravel the complexity and match that information with other existing information. The intrinsic nature of biometrics provides a comprehensive record of a person; once a technology parses out the bundle of information, deeply revealing information about an individual openly avails itself.[118] A face scan on its surface shows simply an image. However, within seconds of uploading it onto certain technology, the search returns detailed information about an individual, including their social media accounts and a catalog of related images from street views.[119] An ability to easily decipher embedded information would reveal a person's associations and movements. Ultimately, however, biometric data on its face does not deeply reveal a person's daily life, beliefs, or whereabouts.

2. Depth of Reach

The second factor relates to the depth, breadth, and comprehensive reach of the information accessed. First, the depth of information grants protection for biometric data against the third-party doctrine. The depth refers to the detail and precision of the information.[120] The biometric information effectively is the individual; it may be the most precise information available to describe a person.

Second, the breadth of information does not grant protection for biometric data against the third-party doctrine. The breadth refers to the frequency of data collected and the length of the recording.[121] Third parties

[116] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).
[117] *Id*.
[118] Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J.L. & TECH. 357, 371–72 (2019).
[119] Matthew Doktor, Note, *Facial Recognition and the Fourth Amendment in the Wake of* Carpenter v. United States, 89 U. CIN. L. REV. 552, 570–71 (2021).
[120] Ohm, *supra* note 118, at 372.
[121] *Id.*

generally do not constantly ask their consumers to add more biometric data; the nature of biometrics is so unique that a single capture satisfies continuous and adaptable usage. Additionally, while the cell phone locations in *Carpenter* collected detailed movement for 127 days, biometric information does not show a person's movement. On the other hand, the Court analogized unauthorized access to traveling back in time to gain access to information from the past because the cell phone information was stored for five years after collection.[122] Similarly, biometric information is likely stored with a third party for as long as the customer is using the service.

Lastly, the comprehensive reach of the number of people that could be affected grants protection for biometric data against the third-party doctrine. The share of biometric-enabled active phones in North America, Western Europe, and Asia-Pacific reached 80% in 2020.[123] The market for biometric systems continues to grow, projected to reach a worldwide market revenue of $82.9 billion USD in 2027.[124]

The three elements within the second factor require a balancing act; while the depth favors the use of third-party doctrine, the breadth and comprehensive reach do not favor the third-party doctrine for biometric data.

3. Inescapable and Automatic Nature of the Collection

The last factor is the inescapability of the collection, which grants protection for biometric data against the third-party doctrine. The inescapable and automatic nature of collection refers to the inability of an individual to opt-out of the collection of personal information. The collection of personal information for services is a "pervasive and insistent part of daily life."[125] Some biometric information collection is inescapable because biometric data is effectively essential to modern life. Many modern mobile devices use a face scan or fingerprint scan for secured personalized access. With scant options to choose another type of mobile device, it is difficult to conclude that a consumer genuinely and voluntarily chooses to use that certain technology.[126]

Automatic nature also refers to the automatic generation of a person's information as part of a service.[127] After a piece of biometric information is recorded on an online server, there may be more biometric information that is automatically generated. This may include an electronic device recording partial matches of face scans or fingerprints. It may also include DNA information that is automatically analyzed when looking for a match. Additionally, the omnipresent use of mobile devices and social media applications allows technology companies to collect biometric information without a user ever recognizing it. For example, TikTok, a popular social

[122] *Carpenter*, 138 S. Ct. at 2218.

[123] *Share of Active Phones with Enabled Biometrics in North America, Western Europe & Asia Pacific from 2016 to 2020*, STATISTA (Mar. 2021), https://www.statista.com/statistics/1226088/north-america-western-europe-biometric-enabled-phones [https://perma.cc/G3TM-MJLX].

[124] *Global Biometric System Market Revenue from 2020 to 2027*, STATISTA (Mar. 2022), https://www.statista.com/statistics/1048705/worldwide-biometrics-market-revenue [https://perma.cc/4T4M-GLDN].

[125] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (quoting Riley v. California, 573 U.S. 373, 385 (2014)).

[126] Tokson, *supra* note 33.

[127] Ohm, *supra* note 118, at 377.

media application, automatically collects certain information from all of its 1.534 billion users such as keystroke patterns or rhythms, "face and body features and attributes," and "faceprints and voiceprints."[128] The application attracts users by encouraging audio and visual creations and sharing them worldwide; yet, it takes advantage of its one billion monthly users' naivety by automatically capturing and storing biometric information without notice unless "required by law."[129]

Ultimately, the *Carpenter* decision did not follow the previous precedent of loose interpretations of the third-party doctrine to allow broad exceptions for government officials. The overall test, as well as the reasoning, speaks to the cautionary approach by the Court in *Carpenter*. It may be the case that *Carpenter* was a limited exception to the third-party doctrine due to the "unique nature" and the "novel circumstances" of the case.[130] The *Carpenter* decision could also be considered a new standard in the current technology-driven period.[131] Future decisions will likely consider the similar nature and intimacy of biometric data and may continue to decline to apply the third-party doctrine. Additionally, the *Carpenter* test will analyze the deeply revealing nature, comprehensive reach, and inescapable and automatic nature of biometric data collection while reinforcing Fourth Amendment protection of an individual's biometric data.

B. TEXTUAL SUPPORT OF THE REASONABLE EXPECTATION OF PRIVACY FROM *KATZ*

Another path to protecting biometric data is through the reasonable expectation of privacy doctrine and focusing on the person, not the property. The reasonable expectation of privacy doctrine was first introduced in a concurrence to the 1967 Supreme Court case *Katz v. United States*.[132] In *Katz*, FBI agents attached an electronic listening and recording device to the outside of a public telephone booth to gather evidence of an individual using the telephone booth to place illegal bets. Justice Stewart, writing for the Court, focused on the protection of the people, not areas, against unreasonable searches and seizures.[133] The Court held that the person inside the telephone booth could rely on Fourth Amendment protection for the conversation inside the public telephone booth.[134] The majority explained that the location of the search does not create an exception to the protection.[135] In a concurring opinion, Justice Harlan introduced the two-part

---

[128] *Privacy Policy*, TIKTOK, https://www.tiktok.com/legal/page/us/privacy-policy/en [https://perma.cc/874P-4FCF] (last updated May 22, 2023).

[129] *Id.*; Allison Fiedler, *New Trends May Help TikTok Collect Your Personal, Unchangeable Biometric Identifiers*, ACLU (Apr. 14, 2022) https://www.aclu.org/news/privacy-technology/new-trends-may-help-tiktok-collect-your-personal-unchangeable-biometric-identifiers [https://perma.cc/53AS-JFJ4]; Mansoor Iqbal, *TikTok Revenue and Usage Statistics (2023)*, BUS. OF APPS (Aug. 3, 2023), https://www.businessofapps.com/data/tik-tok-statistics [https://perma.cc/3YB5-A4UR].

[130] *Carpenter*, 138 S. Ct. 2206, 2217.

[131] Chadwick Lamar, Note *The Third-Party Doctrine Crossroads: Rules and Direction for a Tech-Savvy Fourth Amendment*, 39 REV. LITIG. 215, 240–45 (2019).

[132] Katz v. United States, 389 U.S. 347 (1967) (Harlan, J., concurring).

[133] *Id.* at 351.

[134] *Id.* at 359 ("These considerations do not vanish when the search in question is transferred from the setting of a home, an office, or a hotel room to that of a telephone booth. Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures.").

[135] *Id.*

test under the reasonable expectation of privacy standard: (1) a person exhibits an actual expectation of privacy and (2) "the expectation be one that society is prepared to recognize as 'reasonable.' "[136] Justice Black dissented that the language of the Fourth Amendment does not support the holding and that the judicial branch working to reach an outcome that is desired by many is not an appropriate role.[137]

Applying the reasonable expectation to privacy doctrine is a frequently discussed topic, as some argue that it lacks textual support in the Constitution and therefore should not be applied in Fourth Amendment considerations.[138] Others argue that the reasonable expectation of privacy standard is rooted in the text of the Fourth Amendment.[139] An individual right "against unreasonable searches and seizures" only applies to "their persons, houses, papers, and effects."[140] In *Katz*, the public telephone booth could have been considered a person's "houses" or even "effects." The individual closed the door to the public telephone booth and placed a call in the comfort of the enclosure. Also, the booth held the conversation and was part of the conversation. Therefore, the telephone booth could have been part of a person's "effects."

Along the same lines of thought that considers tangible items—like the telephone booth—an individual's "effects," the two-part standard presented by Justice Harlan in *Katz* parallels how individuals treat other people's "effects" while respecting each other's privacy. For example, if someone saw that a telephone booth was occupied by an individual making a phone call and the door was closed, then they would neither try to open the door nor eavesdrop on the conversation.

Therefore, the reasonable expectation of privacy standards remains a valid method of protecting biometric data. The reasonable expectation of privacy is high in biometric data and thus must be protected from searches and seizures without a warrant. Biometric information derives from an individual's existence. Biometric information strictly relates to a person's uniqueness. It is highly likely that a person intends to keep their biometric information private, as it contains information that is intimate to their existence and biological composition. Biometric information reveals much about a person beyond what Justice Brennan analyzed in *Miller*; even though it does not share "a person's activities, associations, and beliefs," it reveals a person's appearance, stride, and biological makeup.[141] It is the surest way to identify a person. As Justice Stewart reasoned in *Smith*, when information "reveal[s] the identities of the persons" it can naturally reveal the "most intimate details of a person's life"; he reminded the Court that a reasonable expectation of privacy protects conduct in a person's home.[142] By expecting privacy in one's most private space, one may also expect privacy when they interact with a technology that asks for their most private information.

[136] *Id.* at 361 (Harlan, J., concurring).
[137] *Id*. at 364 (Black, J., dissenting).
[138] *See* Anna Lvovsky, *Fourth Amendment Moralism*, 166 U. PA. L. REV. 1189 (2018).
[139] Orin S. Kerr, *Katz as Originalism*, 71 DUKE L.J. 1047, 1050 (2022).
[140] U.S. CONST. amend. IV.
[141] United States v. Miller, 425 U.S. 435, 453 (1976) (Brennan, J., dissenting).
[142] *See* Smith v. Maryland, 442 U.S. 735, 748 (1979) (Stewart, J., dissenting).

Unlike previously seen cases that deal with documents and locations, biometric information cannot be changed; it is finite and eternally fixed to an individual's identity. It holds sensitive and intimate information, and it is incompatible with the third-party doctrine. It encompasses much more information than a record shared with a third party: a fingerprint is a key that unlocks personal devices; facial scan searches lead to bias against communities of color;[143] and a wearable device records how a consumer feels, so anyone with access can go back to a specific time and witness the emotions.[144] Biometric information is much more than a historical repository of information or real-time coordinates like in *Carpenter*. The depth of information it contains is incomprehensible to an average user who permits a third party to use their biometric information. Additionally, biometric information is not "exposed to [a third party's] employees in the ordinary course of business" because it is no longer shared amongst employees like bank account records or phone call histories.[145] Societal concerns for protecting limited, unique identifiers weigh heavily against the permission of third-party doctrine.

C. HISTORY SUPPORTS THE INTENT TO LIMIT EXPOSURE

The original intent of the Fourth Amendment with emphasis on history protects biometric data and denies third-party doctrine application because the purpose of the Fourth Amendment and the intent of the parties all endorse constitutional protection for the individual. Looking at the broad reasoning behind the enactment of the Fourth Amendment, the Framers focused on protection from government officials. In *Boyd v. United States*, Justice Bradley explains in detail the intent behind the Fourth Amendment:

> The practice had obtained in the colonies of issuing writs of assistance to the revenue officers, empowering them, in their discretion, to search suspected places for smuggled goods, which James Otis pronounced "the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law, that ever was found in an English law book;" since they placed "the liberty of every man in the hands of every petty officer." This was in February, 1761, in Boston, and the famous debate in which it occurred was perhaps the most prominent event which inaugurated the resistance of the colonies to the oppressions of the mother country. "Then and there," said John Adams, "then and there was the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born." These things, and the events which took place in England immediately following the argument about writs of assistance in Boston, were fresh in the memories of those who

[143] Nicol Turner Lee & Caitlin Chin, *Police Surveillance and Facial Recognition: Why Data Privacy is Imperative for Communities of Color*, BROOKINGS INST. (Apr. 12, 2022), https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color [https://perma.cc/2V85-TY4D].

[144] Austin Carr, *Amazon's New Wearable Will Know If I'm Angry. Is That Weird?*, BLOOMBERG (Aug. 31, 2020, 3:45 AM PDT), https://www.bloomberg.com/news/newsletters/2020-08-31/amazon-s-halo-wearable-can-read-emotions-is-that-too-weird [https://perma.cc/2SRE-F5QZ].

[145] *Miller*, 425 U.S. 435, 442 (1976).

> achieved our independence and established our form of government.[146]

After extensively quoting Lord Camden, Justice Bradley concludes that "[constitutional liberty and security] apply to all invasions on the part of the government and its employees of the sanctity of a man's home and the privacies of life."[147] The opinion shows that the Framers' focus during the enactment of the Fourth Amendment was to fight against the power that compelled an individual to produce something they wished to keep private. Even though many legal scholars have argued that the Fourth Amendment protection only applies to an individual's residence,[148] the Court's expansive explanation in *Boyd* includes places and things beyond a residence; thus, the historical interpretation of the clause should be broad enough to encompass any part of an individual's private life. Consequently, in *Katz*, Justice Stewart stated what an individual "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[149] In *Carpenter*, Chief Justice Roberts also emphasized that the original intent of the Fourth Amendment was "to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials."[150]

Therefore, an individual's intent to keep the public out of their private life is a key part of interpreting the Fourth Amendment protection for biometric data. Biometric data is a deeply embedded part of a person's life; it is what makes that person unique and defines that person's physical and biological characteristics. Evidence of an individual's intent can be seen from what consumers select in their "privacy settings"; the explicit decision to not share information with other users or even with a third party is a clear expression of intent.[151]

D. UNCERTAINTY IN CONSUMER BEHAVIOUR CALLS FOR JUDICIAL ACTIVISM

Moreover, judicial restraint may not be appropriate when dealing with protecting biometric information because there is evidence that external factors such as uncertainty and external influence affect people's ability to properly articulate their need for privacy.[152] With biometric technologies keeping their records in the digital Cloud or some other intangible digital format, people have no choice but to depend on state privacy laws or third-party specific terms of use to maintain privacy of their online data.

---

[146] Boyd v. United States, 116 U.S. 616, 624–25 (1886).

[147] *Id*. at 630.

[148] *See* Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547 (1999); *see also* David E. Steinberg, *Restoring the Fourth Amendment: The Original Understanding Revisited*, 33 HASTINGS CONST. L.Q. 47 (2005).

[149] Katz v. United States, 389 U.S. 347, 351 (1967).

[150] Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) ("The Founding generation crafted the Fourth Amendment as a 'response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity.' ").

[151] Wayne A. Logan & Jake Linford, *Contracting for Fourth Amendment Privacy Online*, 104 MINN. L. REV. 101, 104 (2019).

[152] Alessandro Acquisti, Laura Brandimarte, & George Loewenstein, *Privacy and Human Behavior in the Age of Information*, 347 SCIENCE 509 (2015).

However, a study shows that an individual's behavior regarding protection of their privacy is affected by lack of knowledge about what private information is shared with other individuals, firms, and the government, and the consequences that may arise from it.[153] Even if they are aware of the consequences, individuals are uncertain about their privacy preferences because they may care about privacy, but balancing the costs and benefits of privacy may drive them to not seek privacy protection.[154] Individuals struggle with identifying the value of their privacy because not only does the preference for privacy change depending on the context, but also because "[h]umans are social animals, and information sharing is a central feature of human connection. . . . progressively increasing levels of self-disclosure are an essential feature of the natural and desirable evolution of interpersonal relationships from superficial to intimate."[155] Therefore, the ability to share intimate details with others without a threat of unwarranted search from government officials and commercialization of such information is crucial to the foundation of social connections and individual livelihood.

Therefore, judicial restraint may not be appropriate when protecting biometric information. A single constitutional theory does not have the capability of answering all legal questions with the proper consideration that they deserve.[156] The absence of certain words or strict references to the colonial era and prior restraint will not serve the current American people nor match the eager advancement of technology that seeks to partake in the gold rush of capitalizing on the unprotected commodity. The Courts should be ready to protect the people with consideration of the potential consequences that result from delayed action.

CONCLUSION

Increased risk of identification from pieces of information supports explicit protection for biometric data. As shown in Clearview AI's technology, a piece of information can be connected to another, and the string of information can reveal intimate details about a person's lifestyle and preferences.[157] This threat of being able to uncover information that an individual desires to keep private also exists beyond facial recognition technology. For example, in a person's medical records, HIPAA protects patient information by limiting access and de-identifying health data—removing names, usernames, email addresses, street addresses, and telephone numbers.[158] However, a person's medical information can be re-identified by matching it to public or private data to reveal "hospital medical record data, hospital discharge data, adverse drug event data, physical activity data, and infectious disease data."[159]

---

[153] *Id.*
[154] *Id*. at 510.
[155] *Id.*
[156] Richard A. Posner, *The Rise and Fall of Judicial Self-Restraint*, 100 CAL. L. REV. 519, 540 (2012) ("No master theories are available to guide judges in performing their lawmaking role in a constitutional case, for there are no logical or empirical methods of choosing one constitutional theory (originalism, textualism, 'living Constitution,' etc. ad nauseam) over another.").
[157] Kashmir, *supra* note 65.
[158] Stacey A. Tovino, *Not So Private*, 71 DUKE L.J. 985, 990 (2022).
[159] *Id.* at 992.

Additionally, there are increasing numbers of cyberattacks on databases across different fields, including recent attacks on the U.S. Marshals Service,[160] a federal U.S. law enforcement database,[161] a health insurance marketplace,[162] a rideshare company,[163] a medical center,[164] and the National Basketball Association.[165] Database breaches affect the security of millions of Americans. For example, a healthcare database breach is detrimental not only to hospital operations, but also to the safekeeping of medical and personal records. Moreover, when databases are breached, it is difficult to identify what exactly was stolen. Without understanding what information was taken and the consequence of sharing that information, Americans are even more stranded, without clear guidance or control over their data.

The comments responding to the RFI by the White House Office of Science and Technology indicated that there was no clear agreement on what is considered "biometrics."[166] Ultimately, there is also a threat looming beyond an under-inclusive definition because certain biometric information will lack protection; consequently, those in marginalized communities are most heavily impacted by the lack of proper protection.[167]

Even with the *Carpenter* Court suggesting the inapplicability of the third-party doctrine in the current technology era, biometric information should be excluded from the third-party doctrine. The same concerns about the loose application of the third-party doctrine from decades past still ring true today. There is a reasonable expectation of privacy over the biometric information that a person provides to a third party, because a consumer only shares limited information with a select party, showing their intent to keep such information private.

Consent given to a third party to use information does not express valid consent for the third party to provide that information to the police or other officials, because the user is not informed of the extent of the use. A piece of biometric information provided is an integral part of many services, and consumers cannot help but accept the risk since there are no realistic alternatives to the services; the world continues to modernize its processes with more common integration of biometric information. Some online

[160] Glenn Thrush & Chris Cameron, *Hackers Breach U.S. Marshals System with Sensitive Personal Data*, N.Y. TIMES (Feb. 27, 2023), https://www.nytimes.com/2023/02/27/us/politics/us-marshals-ransomware-hack.html [https://perma.cc/SAV3-Z4QE].

[161] Joseph Cox, '*Nobody is Safe': In Wild Hacking Spree, Hackers Accessed Federal Law Enforcement Database*, VICE (Mar. 15, 2023), https://www.vice.com/en/article/pkae7g/nobody-is-safe-in-wild-hacking-spree-hackers-accessed-federal-law-enforcement-database [https://perma.cc/J377-ELE2].

[162] Barbara Sprunt, *Personal Information of Members of Congress Exposed in Health Data Breach*, NPR (Mar. 11, 2023, 10:29 AM), https://www.npr.org/2023/03/09/1162191035/personal-information-of-u-s-house-members-exposed-in-health-data-breach [https://perma.cc/S5KE-4T6P].

[163] Kate Conger & Kevin Roose, *Uber Investigating Breach of Its Computer Systems*, N.Y. TIMES (Sept. 15, 2022), https://www.nytimes.com/2022/09/15/technology/uber-hacking-breach.html [https://perma.cc/UZ9K-W54Z].

[164] Ken Alltucker & Bianca Pallaro, *Health Care Data Breaches are Surging*, USA TODAY, Mar. 20, 2023, at 1, 6.

[165] Sergiu Gatlan, *NBA Alerts Fans of a Data Breach Exposing Personal Information*, BLEEPING COMPUT. (Mar. 17, 2023), https://www.bleepingcomputer.com/news/security/nba-alerts-fans-of-a-data-breach-exposing-personal-information [https://perma.cc/VL9M-W4T2].

[166] Tatiana Rice, *When is a Biometric No Longer a Biometric?*, FUTURE OF PRIV. F. (May 19, 2022), https://fpf.org/blog/when-is-a-biometric-no-longer-a-biometric [https://perma.cc/9F9Z-YV35]; the disagreement about the scope of a "biometric" is another discussion that requires an in-depth analysis about the impact of excluding and including certain characteristics.

[167] *Id.*

services specifically track a person's heartbeat, walking distance, or menstrual cycles; these services accomplish their objective only by asking for and using a person's biological and behavioral measurements. Thus, there is no choice but to "reveal the most intimate details of a person's life."[168] As Justice Sotomayor said a decade ago, the third-party doctrine is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[169]

Even when someone knowingly shares their bodily information with a service or product, the third-party doctrine cannot allow government officials to access the biometric information without a warrant. With more states enacting legislation to specifically protect a consumer's right to delete, edit, and opt-out, consumers are more aware of the need for privacy.[170] States' actions show that their constituents, who are the consumers of products and services that ask for biometric information, have a legitimate "expectation of privacy" in sharing their physical, biological, and behavioral information. People's expectation of privacy, states' actions, and applications of *Carpenter* all point to the fact that the Fourth Amendment protects biometric information and does not allow for the third-party doctrine to remain applicable in our evolving society.

[168] Smith v. Maryland, 442 U.S. 735, 747–48 (1979) (Stewart, J. dissenting).
[169] United States v. Jones, 565 U.S. 400, 417 (2012).
[170] INT'L ASS'N OF PRIV. PRO., US STATE PRIVACY LEGISLATION TRACKER: COMPREHENSIVE CONSUMER PRIVACY BILLS (2023), https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf [https://perma.cc/5RTV-9V3Z].