BEING CAREFUL WITH A CAR-FULL OF BIOMETRIC DATA: BIOMETRICS AND DATA BREACH NOTIFICATION LAWS

Eric McCoy and Plamena Gerovska

The dilemma strikes five minutes after the moment one should have left. After retrieving your coat from the rack and proceeding down the driveway the realization gradually dawns that the garment weighs less than usual. A fumbling search of the jacket reveals that it holds no keys and inspires an eager search of the home. Automobile manufacturers aim to eliminate the annoyance of losing one's keys and a host of other problems facing drivers through the integration of biometric technology.[1] Inevitably, these functions necessitate the collection of "biometric data," such as one's fingerprint or iris pattern. Collecting biometric information will allow great advances in driverless cars; however, the collectors incur legal responsibility to properly maintain the information.

Privacy and data breach notification laws attempt to incentivize private companies to ensure that they store personal data in a manner that promotes security. While each law provides its own definition, personal data is broadly defined as any information that relates to an identified or identifiable person, such as their name, social security number, or email address. These laws regulate many specified types of data, such as credit card information, but surprisingly biometric data usually lacks similar protection. Biometric information is arguably the most sensitive form of personal data, as it is directly linked to a person's largely unchangeable biology. A lost credit card can be cancelled, a lost set of car keys can be remedied by replacing locks, but lost or stolen biometric information carries greater consequences.

The potential for abuse of driverless cars that use biometrics demonstrates the need for collectors of biometric data to protect the information they gather. Understanding and planning for this need requires reviewing current legislative protection for personally identifiable information and biometric information. However, states are now only beginning to grapple with the implication of devices, such as driverless cars, that routinely collect one's biometrics.[2] The current legislative approach has been decentralized and is fraught

[1] *See, e.g.*, Bojan Simic, *Navigating Fully Biometric Driver Experience*, FORBES (Apr. 11, 2017), https://www.forbes.com/sites/forbestechcouncil/2017/04/11/navigating-a-fully-biometric-driver-experience/#615cbeba455c; Michael Wayland, *AI, Biometrics could Accelerate Self-Driving Cars*, THE DETROIT NEWS (Jan. 6. 2017), http://www.detroitnews.com/story/business/autos/detroit-auto-show/2017/01/06/ces-ai-biometrics-driving-autonomous-cars/96269928/.

[2] *See, e.g.*, 740 ILL. COMP. STAT. 14/1 *et seq.* (2019).

with problems stemming from statutory variance and gaps in legislation. To protect biometric data as its use increases—both in driverless cars and other technologies—, a federal biometric data breach notification statute poses a potential solution for these statutory problems.

BIOMETRICS REALLOCATE RESPONSIBILITY FOR SECURITY TO DATA COLLECTORS

The car of the future will, luckily, immunize the user from the problem of losing their keys because the user will always possess the means of accessing the vehicle: their biology. The dilemma more likely to confront car owners of the future will be the peril of entrusting the "key" of their biometric information to a third party. Fully autonomous vehicles will likely collect biometric information to further enhance the driver's experience—like how cars currently on the market possess various convenience features, such as automatic parallel parking or lane departure assist. Car manufacturers plan to use authentication methods and sensors that collect biometric information to facilitate these features. Although drivers will never lose their "keys" in the same sense as experienced today, there is a risk that third parties entrusted with biometrics may—and thus will imperil a panoply of the driver's biometric-locked assets.

The technology driving biometric cars necessitates the collection and storage of a variety of biometric information. Car manufacturers propose to use biometric authentication methods that allow users to simply authenticate using their face, fingerprint, or unique voice signature.[3] Sensors that collect data will probably appear before any driverless vehicles roam the roadways and will be used to enhance driver comfort, monitor driver health, and prevent accidents. For example, Mitsubishi manufactured a car that recognizes the driver's face and then adjusts the car's seat settings, interior temperature, and other ancillary settings to fit the driver's stored preferences.[4]

Some propose that these cars could also help their driver's maintain health by monitoring important bodily metrics such as blood pressure and other vital signs.[5] People spend vast amounts of time in their vehicles; therefore, placing sensors in these cars provides an opportunity to increase the amount of health data available for each person. Beyond providing information for future medical treatments and needs, the data collected may also allow the

---

[3] *See* Simic, *supra* note 1.

[4] Kristen Hall-Geisler, *How Will the Car of The Future Use Biometrics?*, HOWSTUFFWORKS (Feb. 1, 2012), https://auto.howstuffworks.com/future-car-biometrics.htm.

[5] *Id.*

car react to the driver's health and physical condition in the moment.[6] For example, the Tesla X can sense if its driver is suffering a heart attack and pilot the vehicle to the nearest hospital.[7] This technology may also be used to detect if the driver is impaired by alcohol, stress, or fatigue, and to make the proper adjustments to the driver's ability to use the vehicle. For instance, if the car detects that its user is under the influence, it may refuse to start,[8] but if the driver merely suffers an increased stress level, the car may take measures to decrease stress, such as massaging the driver.[9]

On its face, biometric technology appears to solve problems facing today's driving, such as the classic example that begin this paper—losing one's keys. However, further analysis reveals that these vehicles merely reallocate responsibility for securing "keys" to third parties entrusted with sensitive biometric information. Physical key technology afforded a simple solution to this problem: keep the unique key in a secure place, such as a key bowl near the exit of one's home, and, if lost, change the lock. The world of digital keys based on biometric identifiers provides no analog to the "key bowl" because, as the next section will discuss in more detail, it only takes a single instance of skilled computer hacking to nullify the value of biometrics as a unique means of authentication.

BIOMETRICS ARE INCREASINGLY TIED TO ONE'S IDENTITY

The loss of biometric authentication information is more frightening than the loss of one's keys because the problem cannot be remedied simply by changing the locks and getting a new set. Biometric information is unchangeable; therefore, a single exposure would not merely endanger one's car, but also their whole inventory of biometric-secured assets: including their identity.

Biometric identifiers are beginning to be used as an essential component of one's identity in government programs and private industry. Many federal agencies, state programs, and private industries have started employing biometrics for identification and authentication. For example, the Department of Defense and the

---

[6] Analysis of this data could allow medical providers to more accurately identify the warning signs of maladies that require treatment. *See, e.g., Tesla Autopilot Helps Bring Sick Driver to the Hospital*, CBS NEWS (Aug. 8, 2016), https://www.cbsnews.com/news/tesla-autopilot-helps-save-driver-joshua-neally-pulmonary-embolism/.

[7] *Id.*

[8] Olivia Solon, *Cars of the Future Will Detect if You're Over the Limit and Refuse to Let You Drive*, MIRROR (June 8, 2015), https://www.mirror.co.uk/news/technology-science/technology/cars-future-detect-youre-over-5845340.

[9] Matthew Stock, *Intelligent Car Seat Detects Driver's Stress Level*, REUTERS (Sept. 23, 2015), https://www.reuters.com/article/us-car-technology/intelligent-car-seat-detects-drivers-stress-level-idUSKCN0RN11P20150923.

Federal Bureau of Investigation both maintain a database of biometric information to use in facilitating law enforcement efforts.[10] The Department of Homeland Security (DHS) also maintains a database of biometric information to prevent terrorism.[11] This database is populated by all immigrants and visitors to the United States who, under the US VISIT Act,[12] must provide biometric information if they wish to enter the United States.[13] DHS also uses biometric data to authenticate those seeking access to sensitive areas of the public transportation systems.[14] State law enforcement often piggy-backs on federal biometric databases to facilitate their law enforcement efforts.[15] Additionally, states employ biometrics to identify welfare participants and to reduce fraud in other social benefit systems.[16] Finally, private industries, such as banking, have experimented with using biometric identifiers as substitutes for traditional identifiers, like personal identification numbers.[17] For private consumers, almost all mobile applications can be accesses with a fingerprint.[18]

Biometrics' ability to identify accurately people and provide a secure method of authentication comes at a price, which includes extreme consequences for inadvertent disclosure of this data.[19] If a person's fingerprint, voice signature, or iris scan is compromised by a data breach, little can be done to restore the unique nature of that personal identifier. This means that others may potentially use the disclosed biometric data to undermine the federal and state agencies that rely on them for their databases. Leaked biometric data could potentially be used to access national security records held by DHS. Biometric data could also be used to commit fraud in any social benefits system that relies on them. For instance, hackers could 3-D print a person's fingerprint and use it to spoof a fingerprint scanner. The compromise of this data could also chill private industry's use

---

[10] CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING AND EAVESDROPPING: SURVEILLANCE IN THE INTERNET AGE §§ 31:37, 31:39 (3rd ed. 2008).
[11] *Id.* at § 31:38.
[12] 8 U.S.C. § 1365b *et. seq.*
[13] FISHMAN & MCKENNA, *supra* note 10 at § 31:38.
[14] *Id.*
[15] *Id.* at § 31:40.
[16] *Id.* at § 31:43.
[17] *Id.* at § 31:44.
[18] *See, e.g.*, Samicheen Khariwal, *How to Integrate Biometric Authentication in iOS and Android*, PROGRESS BLOG (Oct. 30, 2018), https://www.progress.com/blogs/how-to-integrate-biometric-authentication-in-ios-and-android.
[19] Biometrics technology also entails less serious consequences, such as a loss of convenience. For example, allowing someone to borrow something equipped with biometric technology becomes more difficult if a unique biometric identifier is required.

of biometrics by devaluing biometric data's capacity to serve as a unique identifier.

A PATCHWORK OF LEGAL REGIMES PROTECTS BIOMETRIC DATA

Although biometric data collectors and processors cannot easily protect against the risk of losing their subjects' biometric keys, the proper legal regime could incentivize them to minimize the risk of this occurrence and thus retain the benefit of the technology. A patchwork of federal and state laws attempts to advance this goal, but not all laws directly address biometric data, provide adequate enforcement mechanisms, or apply to private entities that collect biometric data.

1. Federal Protections

At the federal level, there are few express restrictions on how private entities may collect and handle biometric identifiers. The Privacy Act of 1974 gives citizens various rights in their personal data and mandates standards for the collection and storage of personal information.[20] However, this law only applies to government actors, providing no oversight to private industry use of biometric information.[21] Several industry-specific agencies have also addressed this issue in part. The Health Information Portability and Accountability Act (HIPAA) provides standards for information collection, use, and storage if the information is provided to a covered entity.[22] Therefore, if driverless cars transfer or share personal data to a health plan, health care clearinghouse, or other health care providers, HIPAA will provide a level of protection.[23] Even taking these regulatory gaps into account, the potential for regulatory conflict also exists if multiple agencies regulate these vehicles.

2. State Biometric Privacy Laws – Illinois & Texas

Likewise, a few states have endeavored to specifically protect biometric data, most notably through regulations that require entities to notify consumers when their biometric data has been unlawfully accessed, stolen, or otherwise compromised. In doing so, states generally follow one of two approaches: regulating biometric

---

[20] The act allows citizens to demand that a governmental agency produce any records kept on him or her, requires agencies to follow certain practices when gathering and handling personal information, places restrictions on how agencies can share a person's data with other people and agencies, and allows individuals to sue the government for violating the act's provisions. 5 U.S.C. § 552a *et seq.*

[21] *See id.*

[22] Health Insurance Portability & Accountability Act of 1996, Pub. L. No. 104-191, 100 Stat. 2548 [hereinafter HIPAA].

[23] *HIPAA Privacy Rule*, U.S. DEP'T HEALTH & HUMAN SERVICES NAT'L INST. HEALTH, https://privacyruleandresearch.nih.gov/pr_06.asp (last visited May 13, 2018).

data as a separate category of data, or integrating biometric data into their existing definition of personally identifiable information. For instance, Illinois and Texas both chose the former, and created separate biometric data regulation statutes.

Illinois' Biometric Information Privacy Act (BIPA) applies to entities that collect biometric identifiers or biometric information. Under BIPA biometric information includes retina or iris scans, fingerprints, voiceprints, hand scans, and face geometry. Biometric information could be any information—regardless of the method of capture, conversion, or sharing—that is based on a biometric identifier and used to identify an individual.[24] Illinois places strict regulations on those who obtain biometric identifiers or information. Before collecting the data, controllers must first: inform the subject of the identifier or information being collected or stored; disclose the purpose of the collection and the length of the term that the data will be used and stored; and receive a written release from the subject to use, collect, or store the biometric identifier or information.[25] This information will usually be included in the customer privacy policy that, for example, an autonomous or semi-autonomous car owner would be prompted to accept before using the car. After obtaining consent, the entity cannot profit from disclosing the biometric data unless: (1) it obtains the data subject's consent; (2) the subject requests a financial transaction necessitating the data's disclosure; or (3) the disclosure is otherwise authorized by law.[26] BIPA also requires that the data controller creates a written policy of their data use practices. If these practices fall below a reasonable standard of care within the industry, the act authorizes individuals to collect damages if injured—a characteristic unique to BIPA. The amount of damages is increased if the data controller acts recklessly or intentionally in violating the act.[27]

Texas's regulations are a little less strict than BIPA. Texas's Capture or Use of Biometric Identifiers Act (CUBI) prohibits collecting biometric identifiers unless the subject is notified and consents to the *collection*.[28] Texas allows consent to be taken in any form, allows the private entity to keep the purpose of the collection private, and does not require disclosures as to how long the data will be stored.[29] Like BIPA, Texas requires that the data controller destroy the identifier. The difference is that under BIPA the destruction must happen within three years of collection, whereas CUBI only requires the identifier's destruction within a reasonable

[24] 740 ILL. COMP. STAT. ANN. 14/10 (West 2019).
[25] *Id.* at 14/15.
[26] *Id.* Biometric data under BIPA may only be stored for three years. *Id.*
[27] *Id.* at 14/20.
[28] TEX. BUS. & COM. CODE ANN. § 503.001 *et. seq.* (2019).
[29] *See id.*

time no later than the first anniversary of the date the purpose for the identifier's collection expires.[30] Finally, the statute only allows the attorney general to recover damages for violations of the act, not private citizens.[31]

3. State Incorporation in Data Breach Notification Statutes

States that incorporate biometric information into their existing data breach statute grandfather in the controls that apply to other classes of information. However, as the following sections will illustrate, these breach notification laws often fail to adequately protect biometric information given the unique harms that occur when biometric data is unlawfully accessed. This is because the risks of a data breach for biometric information extend beyond merely conferring criminals with access to one's car. As discussed, biometric information serves as a unique identifier for a variety of other systems. As such, those who gain access to biometric data as the result of a breach gain a master key to any other applications or systems that rely on biometric identifiers. In turn, the owners of this biometric data may find it enormously challenging, if not impossible, to mitigate their losses after a breach. After all, changing one's fingerprints or iris is entirely unlike changing the locks on one's cars and acquiring a new set of keys, and also unlike other forms of data protected by state breach notification statutes.

4. International Approaches

By means of comparison, the European Union (EU) General Data Protection Regulation (GDPR)—which is applicable to all EU Member States and foreign entities who do business with EU residents—includes biometric data as part of its definition of special categories of personal data.[32] Amongst its other stringent data breach notification provisions, the GDPR requires that businesses notify the competent EU data protection authority within 72 hours of becoming aware of the breach.[33]

DATA BREACH NOTIFICATION LAWS ARE A KEY MECHANISM IN THE PATCHWORK

Users of biometric keys cannot merely pat their pockets to realize that their "keys" have been misplaced or stolen; data breach

[30] *Compare id. with* 740 ILL. COMP. STAT. ANN. 14/15.
[31] TEX. BUS. & COM. CODE ANN. § 503.001(d).
[32] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 2016 O.J. (L 119) 1, Art. 9(1) (copy available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN).
[33] *Id.* at Art. 33.

notification laws step in to address this difficulty by obligating data collectors to report breaches of various personal information, which puts the onus back on the subject of the personal information to remedy the effects of the breach. The information collected by driverless vehicles, regardless of its purpose, will eventually be stored and thus subject to the risk of breach. Data breach notification laws spur data owners to action to mitigate the effects of the data breach by requiring data controllers to notify data subjects and others affected when such a breach is discovered. Currently, all fifty states have their own data breach notification laws, with varying requirements and provisions; [34] no federal data breach notification law currently exists.

Most data breach notification statutes define what a breach is, what type of information must be reported after one occurs, who to notify, when the notification must be made, and what form the notice should take.[35] Many state data breach notification laws define personal information as the combination of two or more types of personally identifiable information (PII), which typically consists of a person's first initial and last name, combined with their social security number, driver's license number, state ID number, or bank account number. States usually define a data breach as the disclosure of PII to an unauthorized third party in a manner that compromises any of the following: *confidentiality*, or the unauthorized disclosure of information; *integrity*, or the unauthorized modification or destruction of information; and *availability*, or the disruption of access to or use of information or an information system.[36]

The stringency of the notification standards vary from state to state, but generally these statutes require notification:

> 1. If a third party *acquires* the data; or
>
> 2. If a third party *acquires* the data and proof exists of the data's *disclosure* to the third party; and

[34] *Security Breach Notification Laws*, NAT'L CONF. OF ST. LEGISLATURES (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[35] THOMAS J. SHAW, ET AL., INFORMATION SECURITY AND PRIVACY: A PRACTICAL GUIDE FOR GLOBAL EXECUTIVES, LAWYERS AND TECHNOLOGISTS 131-141 (1st ed. 2011).

[36] *Standards for Security Categorization of Federal Information and Information Systems*, NAT'L. INST. OF STANDARDS AND TECH. FIPS PUB 199 (2004).

> 3. Under condition 1 and/or 2, only if the breach poses a substantial threat to the data owner.[37]

The first condition requires notification after the theft of a physical device—like a laptop containing PII—or digitally stored data, but without requiring evidence of the thief's ability to misuse the PII. For example, if an employee dropped a flash drive containing unencrypted PII into a river whose current carried the drive away, no duty exists to notify consumers of a data breach due to the low likelihood of a third party acquiring the data.

The second category of data breach notification requires notification only if evidence exists that an unauthorized party acquired both the data and means of accessing it. For example, evidence that a recently discharged employee downloaded unencrypted PII from the company's database before his/her departure warrants notification, because the employee acquired the data and likely possesses a means of accessing it via his personal computer. However, if a thief acquired heavily-encrypted PII without any evidence that he/she possesses the encryption key, the incident may not warrant notification, as no evidence of the thief's ability to access the data exists.

The third notification criterion mandates an investigation to determine if the breach poses a substantial risk to victims if the breach meets the first and/or second criteria. The first criterion warrants notification only if an investigation determines that a substantial risk exists of the third party acquiring the data. For instance, if a few unlabeled data tapes containing unencrypted PII fell off from a transport truck on a deserted stretch of highway, the investigation may determine notification is unnecessary because little evidence exists that anyone acquired these tapes. Under the second data breach notification criterion, it would be necessary to prove that there is a sufficient risk of the PII being acquired and then disclosed to an unauthorized party. Tweaking the data tape example, notification would most likely be required if the unencrypted PII was contained in clearly labeled paper files that were stolen by a roadway bandit during transit. On the other hand, notification of the breach may not be required if the thief merely absconded with a truck that contained unlabeled and encrypted data tapes of PII, because, although the thief acquired the information, there would be little evidence that the PII had been disclosed to him in a manner that allowed it to put it to malicious use.

---

[37] It is important to note that employees who need to access PII in the course of their job duties do not trigger data breach notification laws unless they use the information they gain over the course of their job duties maliciously.

Whenever the notification criterion is triggered, holders of PII must disclose the breach to any affected party, as well as to the relevant state attorney general(s). This must be done as soon as possible—often within proscribed time limitations set forth by the statute—, except where the needs of law enforcement, or necessary measures to restore the entity's system integrity before revealing the breach to the public, require a delay.[38] Many data breach notification statutes contain also "safe harbors," which allow companies to forego notification if they comply with various security standards.

VARIATION IN DATA BREACH NOTIFICATION LAWS MAKES PROTECTING BIOMETRIC DATA PROBLEMATIC

Theoretically, data breach notification laws solve the problem of a third party losing the data subject's "keys" by apprising the subject of the breach and thus enabling them to take remedial measures akin to changing one's locks and getting a new set of keys.[39] Unfortunately, in practice, data breach notification statutes often fail to prevent the data collector from "losing the keys" in the first place, as entities often limit their data security compliance to certain "safe harbor" requirements—often some form of encryption. The "safe harbor" provisions contained in data breach notification laws provide suffers from a bias for encryption, which is but one of the many information security practices available to companies.[40]

Data breach notification laws are important because victims primarily gain awareness of their plight through the data breach notification notices companies produce to comply with these statutes.[41] However, ambiguities like those in Massachusetts and Nevada's data breach notification statutes illustrate how these laws require companies to report data breaches despite their compliance with the safe harbor—or, in contrast, allow companies to take advantage of safe harbor protections despite providing sub-standard security. The notable differences between these two states' definitions of encryption illuminate the issues arising from data

[38] SHAW, ET AL., *supra* note 35 at 94-96.

[39] The data subject is arguably in a better position to mitigate the loss of the breach because they are personally able to take remedial action, such as canceling credit cards and getting a new one.

[40] Justin C. Pierce, *Shifting Data Breach Liability: A Congressional Approach*, 57 WM. & MARY L. REV. 975, 987 (2016) (arguing that Congressional legislation poses the best method of allocating liability for data breaches, also referencing the stagnating effect that encryption safe harbors have on data security).

[41] Sasha Romanosky, et al., *Empirical Analysis of Data Breach Litigation*, 11 J. EMPIRICAL LEGAL STUD. 74 (2014) (discussing an empirical analysis of the common causes and outcomes of data breach litigation).

breach notification statutes' opaqueness.[42] Nevada's statute defines encryption as:

> "The use of any protective or disruptive measure, including without limitation, cryptography, enciphering, encoding or a computer contaminant, to:
>
> 1. Prevent, impede, delay or disrupt access to any data, information, image, program, signal or sound; 2. Cause or make any data, information, image program, signal, or sound unintelligible or unusable; or 3. Prevent, impede, delay or disrupt the normal operation or use of any component, device, equipment, system or network." [43]

On the other hand, Massachusetts defines encryption as a "processes which assign a low probability to the likelihood of an unauthorized party assigning meaning to the acquired information."[44] These definitions' vagueness allows companies in both states the ability to use sub-standard security practices. In Nevada, plaintext information, accessible only if one enters a five-digit employee ID number, theoretically fulfills the definition of encrypted information because the ID number constitutes a measure that makes the data "unintelligible or unusable" and "delays access to…data."[45] This provides sub-par security because any hacker with an automated script possesses the ability to easily foil this security measure.[46]

Massachusetts's definition of "encrypted" also leaves room for sub-par security because it potentially classifies plaintext PII accessible only after entering a lengthy password as having a low probability of an unauthorized party assigning meaning to the acquired information.[47] Although a lengthy password decreases the likelihood of someone cracking the password via automated

---

[42] Definitions of biometric information suffer from similar problems because their specificity varies from state to state. FISHMAN & MCKENNA, *supra* note 10 at § 31:30.30

[43] NEV. REV. STAT. § 205.4742 (2018).

[44] MASS. GEN. LAWS ANN. ch. 93H, § 1(a) (2019).

[45] NEV. REV. STAT. § 205.4742.

[46] Aaron L.-F. Han, et al., *Password Cracking and Countermeasures in Computer Security: A Survey,* CORNELL U. (Nov. 2014), http://arxiv.org/ftp/arxiv/papers/1411/1411.7803.pdf.

[47] MASS. GEN. LAWS ANN. ch. 93H, § 1(a).

software with enough computing power, little stands between them and the plaintext PII.[48]

FEDERAL BIOMETRIC DATA BREACH STATUTES PROVIDE A SOLUTION

If data breach notification laws are to be used as a method of preventing data collectors from losing data subjects' "keys," a federal statute would be the best option. A federal statute, which mandates standards for the collection and handling of biometric information by private companies, will help prevent inadvertent disclosure while retaining private industry's ability to benefit from biometrics. The chief benefit that the federal statute would offer is uniformity. Uniformity would provide private companies with a consistent method of evaluating their liability for potential breaches of biometric data, and ensure a baseline level of protection that consumers can expect.

Another important benefit is the existing federal subject-matter expertise for biometric data security. As previously discussed, several federal programs already utilize biometric databases, and many state law enforcement organizations coordinate their biometric databases to synchronize with the federal government's databases.[49] In relation to these programs, the federal government has existing standards for the safe storage and use of biometric information.[50] Drafting a biometric data breach notification statute that utilizes these standards would allow the law to take advantage of the expertise of the highly sophisticated agencies in charge of administering these databases in promulgating security standards.

Tying in biometric information to existing state data breach notification laws fails to adequately address the unique nature of biometric data, which is not replaceable or changeable like other PII. The result would be that either personally identifiable information will be subject to a much higher standard of security than necessary (if breach notification laws were changed to increase security across the board to account for the harms inherent to biometric data breaches), or biometric information will be collectible with fewer controls than desirable. Even where state laws have directly addressed biometric data, these laws are few and far between, and already diverge in the scope of information protected, the security measures required, and the means of enforcement. A federal statute—which draws on and expands upon the existing landscape

---

[48] Han, et al., *supra* note 46.

[49] *See* Hall-Geisler, *supra* note 4.

[50] *See e.g.* Patrick Grother, et al., *Biometric Specifications for Personal Identity Verification*, NAT. INST. STANDARDS & TECH. SP 800-76-2 (July 2013), https://csrc.nist.gov/publications/detail/sp/800-76/2/final.

of federal rules regarding biometric data—provides the best solution because it creates a uniform standard that can preserve the utility of biometric information while providing increased security and security.

CONCLUSION

Losing one's keys may seem like a pedestrian problem, but it is emblematic of a bigger dilemma: responsibility for security. In a world of physical keys, possessors have responsible for the keys' security because they were best able to take precautions to ensure their safety. In a digital world, where these keys are no longer in the driver's hands, the possessor of the key is not in the best position to secure them, but may better situated to mitigate damages resulting from the keys' loss.

In the wake of this new reality, a patchwork of data breach notification laws with varying security requirements is insufficient to obligate third parties to adequately secure the keys they hold against loss. A strong federal standard would ensure that holders of biometric information are placing their keys in the most secure digital "bowls." This additional effort for security is warranted because, unlike traditional means of authentication, a single exposure of biometric information destroys its value as a secure identifier. If these security measures prove inadequate against sophisticated hackers, notification provisions can allow data subjects—who are better situated to take remedial measures—to try to mitigate the damage caused by the loss of their keys.

In the moment, losing physical keys feels frightening; however, this fear is dulled by the underlying knowledge that access to one's car and the vehicle's security lie only a simple lock change away. Holders of biometric keys may never have that luxury, but under the proposed legal regime, they would at least know that the key holders are obligated to adequately secure their keys, and that they will have ample opportunity to mitigate their losses in the event of breach.