Journal of Technology Law & Policy

Volume XX – 2019-2020

ISSN 2164-800X (online)

DOI 10.5195/tlp.2020.232

http://tlp.law.pitt.edu

Can the CCPA Access Right Be Saved? Realigning Incentives in Access Request Verification

Rebecca Iafrati

Abstract

The California Consumer Privacy Act access right has the potential to give Californians a level of control over their personal information that is unprecedented in the United States. However, consumer privacy interests will be in peril unless the access right is accompanied by an effective access request verification requirement. Requiring companies to respond to access requests when they cannot verify that the requestor is the subject of the requested data puts sensitive personal information at risk. Inversely, allowing companies to shirk their access request responsibilities by claiming that data is unverifiable diminishes consumers' data control rights. Thus, in the context of access request verification policy, there is an inherent tension between privacy as confidentiality and privacy as control. The success of the access right, and thus all CCPA data control rights, hinges on an access request verification policy that successfully balances these competing privacy interests. The endemic identity theft caused by credit application verification systems demonstrates why such balancing cannot be wholly left to private companies. In the credit context, balancing has been driven by the profit maximization interests of businesses, which currently do not align with consumer privacy interests. Fortunately, several scholars have proposed methods for aligning these divergent interests. The strengths and weaknesses from these proposed solutions to identity theft provide a useful framework for building a system that incentivizes companies to prioritize consumer privacy when developing access request verification systems.

This site is published by the University Library System of the University of Pittsburgh as part of its D-Scribe Digital Publishing Program and is cosponsored by the University of Pittsburgh Press.

Can the CCPA Access Right Be Saved? Realigning Incentives in Access Request Verification

Rebecca Iafrati*

I. INTRODUCTION

While the federal government has repeatedly failed to enact comprehensive consumer privacy legislation, several states have become leaders in the privacy space. Of particular importance is the legislation from the nation's premier technology hub—California. When it goes into effect in 2020, the California Consumer Privacy Act (CCPA) will grant Californians broad data control rights including deletion, access to information, and the right to opt-out of data sale.[1] The access right enables consumers to compel businesses to disclose the information that the businesses hold about them.[2] The right of access is the foundational data control right. For example, a consumer would be unable to exercise her deletion right without first knowing what information the company holds. However, if the access right is not carefully implemented, sensitive consumer data, including geolocation and biometrics, will be vulnerable to unauthorized access. Thus, legislation must ensure that companies respond to access requests and that, when they respond, they only share data with the data subject.

The California legislature attempted to ensure that companies would only disclose data to the data subject by specifying that access right obligations are only triggered by *verifiable* access requests.[3] However, the California Attorney General (AG) has not yet defined "verifiable."[4] The meaning of verifiable will have a significant impact on the effectiveness of the access right because it will dictate the circumstances in which companies are required to comply with access requests. Generally, verification is the process of confirming that the requestor is who she

* Georgetown University Law Center, J.D. Candidate 2020; Tufts University B.A. 2016. Thank you to Professor Julie Cohen for helping me through every step of the writing process. Thank you also to Professor Alexandra Givens for introducing me to the world of technology law and policy.

[1] CAL. CIV. CODE §§ 1798.100–1798.199 (Deering 2018).

[2] *Id.* § 1798.100(a).

[3] *Id.* § 1798.100(c).

[4] *Id.* § 1798.140(y).

Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.232 ● http://tlp.law.pitt.edu

claims to be.[5] For instance, to go to France, I have to present my passport to the TSA agent—this is a verification procedure—the agent is now sufficiently assured of my identity to let me leave the country. In the context of access rights, an access request verification process ensures that the company can confirm the requestor's identity with some measure of certainty. The definition of verification is important because if "verification" requires a very high degree of certainty, fewer people will be able to exercise their access rights, but also fewer people will have their data shared with unauthorized parties.

Verification is never foolproof; people still steal passports and forge government licenses. However, access requests made to third-party online advertising technology ("ad tech") companies invoke new and particularly vexing verification challenges.[6] These companies typically pseudonymize personal data and distinguish it via only a persistent identifier.[7] Persistent identifiers are considered "personal information" (PI) under the broad definition of PI in the CCPA, which largely aligns with the European Union's General Data Protection Regulation (GDPR) and evolving norms in the United States.[8] Nonetheless, for third-party ad tech companies persistent identifiers are not linked to any other identifying

---

[5] JASON ANDRESS, THE BASICS OF INFORMATION SECURITY: UNDERSTANDING THE FUNDAMENTALS OF INFOSEC IN THEORY AND PRACTICE 25 (Syngress 2d ed. 2014).

[6] *See generally* Jack Marshall, *WTF is Third-Party Data*, DIGIDAY (Feb. 5, 2014), https://digiday.com/media/what-is-third-party-data/ (explaining that "third-party" ad tech companies are companies that receive personal data from someone other than the data subject).

[7] *See generally* Jules Polonetsky & Stacey Gray, *Cross Device: Understanding the State of State Management* (Nov. 2015), https://fpf.org/wp-content/uploads/2015/11/FPF_FTC_CrossDevice_F_20pg-3.pdf. A persistent identifier is a unique set of characters assigned to the consumer. The persistent identifier is used to track the consumer's online activity over time. Some persistent identifiers can track users across devices and browsers, while others can only be used to track the consumer's activity on one device or platform. One such identifier is "hashed" email addresses—a kind of one-way encryption that makes it difficult to re-identify the originating email address while still being able to match the email address to the same hashed email in another data set. Other persistent identifiers include cookie ids, unique identifiers stored on a web browser's local directory that can track users across the websites that deploy them; IP addresses, unique strings of numbers that computers use to communicate over networks; and mobile device identifiers, resettable codes provided by the mobile devices' operating systems.

[8] Jessica Rich, *Keeping Up with the Online Advertising Industry*, FED. TRADE COMMISSION (Apr. 21, 2016, 10:30 AM), https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry; "Personal information" is defined in the CCPA as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, . . . unique personal identifier[s], online identifier[s], [and] Internet Protocol address[es] . . . ." California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.140(o)(1) (Deering 2018). In the GDPR, "personal data" means any "information relating to an identified or identifiable natural person . . . in particular by reference to an identifier such as a[n] . . . online identifier." Commission Regulation 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, (General Data Protection Regulation), 2016 O.J. (L 119) 1, art. (4).

Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.232 ● http://tlp.law.pitt.edu

information, such as a name or an email address.[9] The anonymity provided by pseudonymization has clear privacy benefits. However, it also makes complying with access requests more difficult because traditional means of verification, such as a driver's license, cannot link a requestor to the requested data when the data is not associated with the requestor's legal identity.

Thus, the verification requirement in the CCPA also implicates the "linkability" of the requestor to her pseudonymized persistent identifier.[10] The issues surrounding linkability underscore the inherent tension between privacy as confidentiality, and privacy as control. Privacy enhancing techniques that attenuate the link between the data subject and her data, such as pseudonymized persistent identifiers, increase confidentiality. However, the user cannot access her data under the CCPA if pseudonymization makes it impossible for the business to adequately verify her request, thus reducing data control. Inversely, a robust link between the user and her identifier increases control because access requests can be more easily verified but decreases confidentiality. Thus, tradeoffs between confidentiality and control inherently underlie all access request verification processes.

The already in-effect GDPR access right highlights the difficulty of operationalizing a verification process that properly balances confidentiality and control. Like the CCPA, the GDPR requires access request verification but does not elaborate on the meaning of verified.[11] Numerous data protection authorities have addressed verification to some degree but have not directly addressed the challenges posed by pseudonymous data.[12] Given the lack of guidance, it is no surprise that access rights have not been fully realized in the EU. In a study that surveyed 103

---

[9] *See* Polonetsky & Gray, *supra* note 7.

[10] "Linkability" in this paper means the connection between a data subject and her persistent identifier.

[11] Commission Regulation 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, (General Data Protection Regulation), 2016 O.J. (L 119) 1, art. (4).

[12] The Article 29 Data Protection Working Party guidance says that there are no prescriptive requirements for verification in GDPR, but that additional user information can sometimes be requested for verification if such a request does not lead to excessive demands and to the collection of personal data which are not relevant or necessary to strengthen the link between the individual and the personal data requested. *See Article 29 Data Protection Working Party "Guidelines on the Right to Data Portability*," WP 242 (Dec. 13, 2016), http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf. ICO similarly recognizes the necessity of verification processes and allows companies to collect additional data if they are "reasonable about what [they] ask for." The guidance also notes that whether and how the requestor's identity must be confirmed will be affected by "the means by which the SAR is delivered" and "the possible harm and distress that inappropriate disclosure of the information could cause to the individual concerned." INTERNATIONAL COMMISSIONER'S OFFICE, SUBJECT ACCESS CODE OF PRACTICE, 2017, SAR Version 1.2, at 23–24 (UK).

Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.232 ● http://tlp.law.pitt.edu

European data-holding companies, about 70% of companies failed to adequately respond to access requests as required by the GDPR.[13] In another study of access requests under the GDPR's predecessor, the Data Privacy Directive, researchers found that the primary reason companies failed to respond to access requests was a lack of awareness as to the existence and scope of data rights.[14] Furthermore, the ambiguity in the statute gives companies enormous latitude in the design of their verification processes. Consequently, verification processes differ substantially between companies.[15]

The EU's experience demonstrates how crafting a verification process that facilitates access rights without increasing the vulnerability of personal information is a formidable task. This paper first explores why confirming that the data requestor is the subject of the requested data is especially challenging for third-party ad tech companies. Next, I compare access request verification to the identity theft caused by the credit application process and analyze several proposed solutions to identity theft. Based on this analysis, I conclude that access rights can only effectively enhance consumer privacy if legislation incentivizes companies to prioritize consumers when balancing the control and confidentiality interests that motivate their verification procedures. Finally, I apply the underlying logic of the credit verification approaches to access request verification and assess the strengths and weaknesses of each approach in this context. This analysis provides a rough framework for how legislation should approach realigning incentives moving forward.

II. CHALLENGES IN THIRD-PARTY AD TECH VERIFICATION

It is particularly challenging for third-party ad tech companies to confirm that the person making the access request is the subject of the requested data because such companies do not gather data directly from the data subject.[16] Instead, they buy

[13] Press Release, Talend, The Majority of Businesses Surveyed are Failing to Comply with GDRP, According to New Talend Research (Sept. 13, 2018).

[14] Jef Ausloos & Pierre Dewitte, *Shattering One-Way Mirrors: Data Subject Access Rights in Practice*, 8 INT'L DATA PRIVACY L. 4, 4–28 (2018).

[15] Based on my review of digital advertising companies, companies use a wide range of verification processes. For example, Taboola uses automated programs that match the requestor's cookie ID, IP address or mobile advertising ID to the corresponding data. TABOOLA, *Taboola's Data Subject Access Request Portal*, https://accessrequest.taboola.com/access/ (follow directions then hit "show me the data"). Oracle differs from Taboola. It requires email correspondence with a company representative who will either give the information upon a signed form swearing that you are the data subject or will require further information. *Oracle Privacy Policy*, ORACLE, https://www.oracle.com/legal/privacy/privacy-policy.html#12.

[16] Marshall, *supra* note 6.

Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.232 ● http://tlp.law.pitt.edu

personal data from the first-party data collector or from other third-party ad tech companies.[17] Indeed, it is likely that the access request is the first contact between the company and the data subject, which makes *authenticating* the request challenging. Authentication is the process of confirming that a specific individual is the same person as the one who engaged in a particular activity at an earlier time.[18] Using a password to log in to an email account is authentication. Inputting a password that was known to the creator of the account is sufficient to assure the email provider that the person attempting to access the account is the same person as the one who created it. This is different from verification because inputting the password does not necessarily reveal the person's identity.

First-party data collectors have the opportunity to establish a relationship with the data subject at the point of data collection, which can later be used to authenticate data access requests. For example, Facebook, a first party data collector, requires requestors to input their user names and passwords to exercise their GDPR data control rights.[19] However, third-party ad tech companies have no opportunity at the point of data collection to gather information about the data subject that can later be used for authentication. The pseudonymization of data by third-party ad tech companies further complicates this situation because, in the access request context, verification is a method of authentication. Verifying the requestor's identity both at the time of the data collection and at the time of the access request is a way to authenticate the request—i.e. to confirm that the subject of the data is the same person as the one who is requesting it. Therefore, the aforementioned unlinkability between a requestor and her persistent identifier makes it difficult for the third-party ad tech company to use verification as a means of authentication.

Many companies responding to GDPR access requests use only the requestor's knowledge of the persistent identifier to authenticate the request.[20] Unfortunately, knowledge of the persistent identifier is not a secure means of authentication because it can be obtained by anyone with direct or remote access to the data subject's device. Thus, disclosing data upon the receipt of a persistent identifier diminishes confidentiality even though the very purpose of the pseudonymization was to

[17] *Id.*

[18] ANDRESS, *supra* note 5, at 26.

[19] *Accessing & Downloading Your Information*, FACEBOOK, https://www.facebook.com/help/1701730696756992.

[20] Some companies, including Taboola, will provide a requestor with all the personal data linked to a persistent identifier if the requestor provides the company with just the persistent identifier. There are no additional procedures to link the requestor to the persistent identifier they are providing. *See* TABOOLA, *supra* note 15.

Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.232 ● http://tlp.law.pitt.edu

increase confidentiality. Alternatively, some companies use these security concerns as a justification not to disclose data at all, thus diminishing data control rights.[21]

The aforementioned verification issues in the EU largely stem from the free reign given to companies in crafting their authentication policies. Profit-seeking companies are incentivized to reduce their data protection obligations by prioritizing confidentiality over control rights.[22] For example, making a database unsearchable by name or identifier (a confidentiality enhancing technique) makes verification more difficult, therefore enabling the company to escape its obligation to respond to access requests, thus reducing control.[23] If the California AG implements a GDPR-like approach, profit-seeking companies will make crucial trade-offs with minimal transparency. Since the purpose of the CCPA is to vindicate Californian's fundamental privacy rights, consumer privacy, rather than corporate interests, should drive control-confidentiality balancing.[24]

III. Comparison to Credit Application Process

Although access rights give rise to new authentication issues, the fundamental struggle to balance accurate authentication against competing interests is also salient in the credit industry. The lack of verification and authentication procedures in the credit application process has enabled identity theft to reach endemic proportions.[25] Just like in the access request context, credit verification and authentication processes are motivated by the balancing of competing interests. Lax procedures enable identity theft, while stringent procedures are burdensome for the creditor and the applicant. Therefore, safeguards are necessary to ensure that the balance benefits consumers.

A. The Current Credit Application Process

The first step in the credit application process is the applicant provides the creditor with her personal information such as her name, date of birth, social security number (SSN), phone number, and address. Next, the creditor provides the credit-reporting agency (CRA) with the applicant's personal information and the CRA

[21] Michael Veale, Reuben Binns & Jeff Ausloos, *When Data Protection by Design and Data Subject Rights Clash*, 8 Int'l Data Privacy L. 105, 108 (2018).

[22] *Id.*

[23] For example, Apple Inc.'s response to Siri users' access requests. *Id.* at 111.

[24] Cal. Civ. Code § 1798.2.

[25] *See generally* Erika Harrell, Bureau of Justice Statistics, U.S. Dep't of Justice, NCJ251147, Victims of Identity Theft, 2016 (Jan. 2019), https://www.bjs.gov/content/pub/pdf/vit16.pdf.

Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.232 ● http://tlp.law.pitt.edu

locates the credit report with the corresponding data points.[26] The credit report compiles all of the instances in which the individual was granted credit, whether she paid her debt, and if she did so in a timely fashion. If the credit score in the credit report is sufficient, the creditor will likely extend the applicant credit. If the score is too low or no score can be located, the creditor will most likely reject the applicant's credit application.

The major flaw in this process is that verification is practically non-existent. Credit can be extended online without any face-to-face interaction or examination of government issued documents. Thus, the creditor's only assurance that the requestor is who she claims to be is her knowledge of a name, social security number, and other identifying information. The authentication process—i.e. that the applicant is the subject of the credit report—is also non-existent. The creditor's only assurance that the applicant is the subject of the credit report is that the personal information that she provided matches the set of personal information held by the CRA. The creditor typically deems this matching process sufficient to extend credit, even though the identity of the person whose information is in the credit report and the identity of the current applicant are not verified.[27] According to Lynn LoPucki, this system is "doomed to failure because [it] depend[s] on keeping secret information that must be available to literally thousands of people in the routine operation of the credit-reporting system."[28] To make matters worse, the key pieces of information involved (name and social security number) typically remain the same throughout a person's lifetime. Thus, "information cannot be recalled" once it is released.[29] Moreover, creditors sometimes extend applicants credit even if the information on their applications does not perfectly match the information held by the CRA.[30]

These vulnerabilities enable imposters to commit "new account fraud," a form of identity theft in which an imposter opens a line of credit using another person's information.[31] The creditor typically bears the cost of the credit that it extended to the imposter; however, the victim still spends time and money proving that she did not take out the credit and repairing her credit report. A Department of Justice study

---

[26] Julia Kagan, *Credit Application*, INVESTOPEDIA (last updated Feb. 6, 2018), https://www.investopedia.com/terms/c/credit-application.asp.

[27] Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 TEX. L. REV. 89, 103–04 (2001); Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1256–58 (2003).

[28] LoPucki, *supra* note 27, at 94.

[29] *Id.*

[30] Chris J. Hoofnagle, *Internalizing Identity Theft*, 13 UCLA J.L. & TECH. 1, 6 (2009).

[31] *Id.* at 4.

Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.232 ● http://tlp.law.pitt.edu

found that victims of identity theft experienced a combined average loss of $1,343.[32] These costs are very difficult to recover from the creditor because the burden on the victim to prove that the creditor is liable for the identity theft is impossibly high.[33]

B. Prior Attempts to Address Identity Theft

Congress has attempted to address identity theft several times, but ultimately all efforts fell short. The first effort was the 1970 Fair Credit Reporting Act (FCRA). FCRA required CRAs to adopt reasonable procedures to ensure the accuracy and confidentiality of credit reports.[34] The purpose of the act was to ensure that creditors' financial decisions about whether to extend credit were based on accurate and complete information.[35] Relatedly, it addressed identity theft by creating consumer rights to correct credit reports and to guard against future identity theft, and by imposing confidentiality responsibilities on CRAs.[36] The confidentiality requirements were intended to make it more difficult for identity theft perpetrators to access personal information that they could use to open new accounts.[37]

However, identity theft continued to be a serious problem. In 2003, Congress amended the FCRA with the Fair and Accurate Credit Transaction Act (FACTA), which added provisions specifically designed to prevent identity theft.[38] Section 114 of the FACTA required designated federal agencies to jointly issue identity theft guidelines for creditors and to promulgate regulations requiring creditors to establish reasonable policies for implementing the guidelines.[39] Under their FACTA authority, the agencies promulgated the Red Flag rules in 2007 to prevent identity theft.[40] A

---

[32] *See generally* ERIKA HARRELL, BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, NCJ248991, VICTIMS OF IDENTITY THEFT, 2014 (Sept. 2015), https://www.bjs.gov/content/pub/pdf/vit16.pdf.

[33] Knowledge required to support conviction for aggravated identity theft can be proven by knowledge in fact, or by proof of "willful blindness," for which the government has to show that defendant: (1) "was aware of a high probability of wrongdoing," and (2) "consciously and deliberately avoided learning of the wrongdoing." United States v. Lopez-Diaz, 794 F.3d 106, 111 (1st Cir. 2015).

[34] Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681 (1970).

[35] *Id.*

[36] 15 U.S.C. § 1681(c)(1) (2011).

[37] 15 U.S.C. § 1681(b) (2011).

[38] Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (amending the Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681 (2000)).

[39] 15 U.S.C. § 1681m(e)(1)(B) (2009).

[40] Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1960 (amending the Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681m (2003)).

Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.232 ● http://tlp.law.pitt.edu

"red flag" is a "pattern, practice, or specific activity that indicates the possible existence of identity theft."[41]

The Red Flag rules require creditors to adopt an identity theft prevention program. The rules list four basic elements that must be included in the program. The program must contain "reasonable policies and procedures" to "identify relevant Red Flags . . . and incorporate those Red Flags into the Program; detect Red Flags that have been incorporated into the Program; respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and ensure the Program is updated periodically to reflect changes in risk to customers or to the safety and soundness of the financial institution or creditor from identity theft."[42] The agencies identified 31 specific Red Flags, which each creditor is required to incorporate into its program if the Red Flag is relevant to its business.[43] To promote flexibility and responsiveness to the changing nature of identity theft, the rules also state that covered entities need to include in their programs relevant Red Flags from their own experiences.[44] Once a Red Flag is detected, the rules require an "appropriate response" that is "commensurate with the degree of risk."[45] The FTC has the authority to enforce the Red Flag rules and can impose a penalty of up to $2,500 for each independent violation of the rules, but there is no private right of action.[46]

C. The Reasons that Red Flag Rules Failed to Alleviate Identity Theft

Since the Red Flag rules went into effect in 2010, the annual incidence of credit card new account fraud has continued to grow, with increased incidence of 24% since 2017.[47] This is attributable in part to the fact that the Red Flag rules give creditors a lot of discretion in the design and execution of their programs.[48] For example, the meaning of "appropriate response" and "commensurate" are quite flexible. This weakens the effectiveness of the Red Flag system because if a creditor spots a Red Flag it can apply weak "appropriate responses" that still result in new credit being granted. Also, there are insufficient incentives for creditors to identify new Red Flags. While the agencies can designate new Red Flags on their own, agencies will

---

[41] 16 C.F.R. § 681.1(b)(9) (2009).

[42] 15 U.S.C. § 1681m(e)(1)(B) (2009).

[43] 16 C.F.R. § 681, app. A (2009).

[44] *Id.*

[45] 16 C.F.R. § 681, app. A (2009).

[46] 15 U.S.C. § 1681s(a)(1) (2009); 15 U.S.C. § 1681m(h)(8) (2009).

[47] *Consumer Sentinel Network*, FEDERAL TRADE COMMISSION (Feb. 2019), https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2018/consumer_sentinel_network_data_book_2018_0.pdf.

[48] Hoofnagle, *supra* note 30, at 19.

Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.232 ● http://tlp.law.pitt.edu

not spot emerging fraud trends as quickly as those working inside the industry. Since agency generated Red Flags are likely to lag behind the realities of the industry, the success of the system depends on creditors fulfilling their obligation to identify additional Red Flags.

A theoretically logical solution to this problem is that the FTC or Congress could enact more detailed rules that remove the ambiguity in the current Red Flag system. However, this approach will ultimately fail for the same reasons that the original Red Flag rules failed. No piece of legislation can foresee and cover every facet of authentication that might cause identity theft, especially since new fraud trends are constantly emerging as technology evolves. Therefore, even with more detailed rules, identity theft will continue so long as ignoring Red Flags or minimal compliance is the least expensive option.

IV. Proposed Solutions to Identity Theft

The aforementioned attempts to prevent identity theft prioritize maximizing the speed and minimizing the cost of the credit application process over actually ending identity theft. Such approaches assume that identity theft will continue to some degree because fully preventing identity theft would require creditors to thoroughly review credit applications, which would increase the time and cost of the process. Consequently, such approaches are limited to security measures that do not create a heavy burden for creditors, which will inevitably be insufficient to fully prevent identity theft. For example, the Red Flag rules provide creditors with enough flexibility that they can escape costly authentication procedures.[49] This dynamic explains the total lack of authentication in the current credit application process. Creditors have not instituted authentication procedures because it is cheaper for creditors to assume that the applicant is who she claims to be than it is to authenticate her request. Any future attempts to prevent identity theft will be similarly doomed if they, once again, prioritize minimizing the creditor's burden. Instead, future policies must incentivize creditors to institute robust authentication by making it the financially pragmatic choice. Even though this fundamental change in the creditor's incentives will burden creditors, it is necessary to ensure diligent authentication, which is necessary to substantially reduce the incidence of identity theft.

The identity theft solutions explored in this section attempt to change the creditor's incentives to motivate creditors to enact robust authentication processes. These approaches differ substantially in how they approach the problem. The magnitude of difference between these proposals demonstrates the breadth of potential strategies that legislatures can utilize in altering the creditor's incentives.

[49] *Id.* at 20.

Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.232 ● http://tlp.law.pitt.edu

Ultimately, the strengths and weaknesses of each approach are also a helpful starting place for building a robust access right verification processes, as discussed in the next section.

A. Solove Approach

According to Daniel Solove, identity theft is the result of a deeper issue with society's understanding of privacy harms in today's information age.[50] The "traditional model" understands privacy protections as individual rights, and privacy harms as "a series of discrete wrongs to specific individuals."[51] This model fails to address systemic privacy problems, such as identity theft, that are "caused by a particular social or legal structure, rather than by a few isolated actors."[52] Thus, identity theft results from architectures created by public and private bureaucracies that minimize individual data control, avoid accountability, and perpetuate insecure systems.[53]

Solove proposes an architectural reform based on the theory of privacy protections embodied in the Fair Information Practices (FIPs).[54] FIPs allocate the burden of addressing identity theft to the entities that cause it by increasing individual involvement in personal information systems and strengthening information processing controls.[55] To improve individual participation, Solove suggests an opt-in credit reporting system, which would force CRAs to establish relationships with those they report on at the point of report creation. The opt-in system would make it possible for CRAs to establish a system in which people access their reports through password protected accounts rather than through an SSN or other personal data.[56] To improve information processing controls, "the collection and use of personal information" should be considered "an activity that carries duties and responsibilities."[57] For example, CRAs should be subject to minimum-security practices.[58]

---

[50] Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1232 (2003).

[51] *Id.* at 1230.

[52] *Id.* at 1232.

[53] *Id.* at 1256.

[54] *Id.* at 1266–68.

[55] *Id.* at 1266.

[56] *Id.* at 1266–67.

[57] *Id.* at 1267.

[58] *Id.* at 1267–70.

Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.232 ● http://tlp.law.pitt.edu

B. Hoofnagle Approach

According to Chris Hoofnagle, "an analysis of incentives in credit granting elucidates the problem: identity theft remains so prevalent because it is less costly [for creditors] to tolerate fraud."[59] Like Solove, Hoofnagle frames identity theft as an architectural issue; however, his proposed solution differs by targeting the underlying incentives. Hoofnagle argues that creditors should be free to dictate their own verification processes, but that they should be subject to *strict liability* for incidents of identity theft.[60]

According to Hoofnagle, the imposition of strict liability on the creditor for identity theft is defensible for several reasons. First, "ultrahazardous" activities have historically been subject to strict liability because they are necessary but extraordinarily dangerous.[61] The same logic could be applied to granting credit, which is necessary in the current economy, yet extraordinarily damaging to victims. Also, the creditor is in the best position to prevent identity theft because she controls the use and protection of PI, and she has strategies to mitigate the financial losses associated with identity theft.[62] These means give the creditor more control to prevent identity theft than the consumers who have no reasonable means to address the identity theft. Thus, strict liability would result in a more efficient allocation of cost among the creditors and victims.

Damages could be keyed to the average expense consumers endure for victims who cannot prove damages. Victims who can prove damages would have the opportunity to plead those damages.[63]

C. LoPucki Approach

According to Lynn LoPucki, creditors continue to use SSNs and personal data as passwords despite security concerns because they lack the means and incentives to improve verification procedures.[64] LoPucki's solution is a novel verification system accompanied by legal incentives for applicants and creditors to utilize the system.[65] The first step in LoPucki's system is the applicant voluntarily registers her

---

[59] Hoofnagle, *supra* note 30, at 1.

[60] *Id.* at 19.

[61] *Id.* at 22.

[62] *Id.* at 22–23.

[63] *Id.* at 23.

[64] LoPucki, *supra* note 27, at 89, 94.

[65] *Id.* at 120–34.

Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.232 ● http://tlp.law.pitt.edu

identity with the designated government agency.[66] Next, the agency conducts a rigorous authentication process in which the applicant is required to produce government issued documents (license, SSN card, passport, etc.) during an in-person appointment.[67] Once the agency confirms the applicant's identity, the applicant's identifying information (SSN, name, birth date, etc.) is posted on a public, read-only website along with contact instructions dictated by the applicant. During credit checks, the creditor uses the applicant's personal information to locate her profile on the portal and then uses the corresponding contact instructions to get confirmation from the person listed on the database before extending credit.[68]

Creditors are incentivized to check the database and follow the specified procedures because they lose their statutory exemption from liability if they issue credit to a registered individual without obtaining permission in accordance with the individual's instructions.[69] Even though the system would be optional, individuals are incentivized to register with the system because of the transparency it brings to the verification process and the enhanced credit security.[70]

V. CREDIT THEORIES IN THE ACCESS REQUEST VERIFICATION CONTEXT

The prior analysis demonstrates that the only way to prevent identity theft is to make it more cost effective for creditors to establish identity theft prevention mechanisms than to tolerate identity theft. Similar logic applies to access rights. The only way to create a system in which companies strike a balance between confidentiality and control that maximizes consumer privacy is by aligning consumer privacy interests with the company's profit maximization interests. This is no easy feat. Absent government intervention, compliance with access requests is more expensive than either not complying with requests by claiming they are unverifiable or complying with requests without diligent authentication procedures. However, while this is a difficult task, it is not impossible. The strengths and weaknesses of three identity theft approaches are a helpful starting point for developing an approach to incentivize companies to develop access request verification systems that further consumer privacy interests.

[66] *Id.* at 115.

[67] *Id.* at 115–17.

[68] *Id.* at 119.

[69] *Id.* at 120.

[70] *Id.* at 134–35.

Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.232 ● http://tlp.law.pitt.edu

A. An Architectural Framework and the Limitations of "Participation and Responsibility"

As a foundational matter, it is helpful to apply Solove's architectural understanding of privacy harms to the access request verification issue. Approaching access rights under the "traditional model" does not accurately capture the nature of the problem because the access request issues are not attributable to one malicious actor. Rather, the issues stem from the flaws in the overall architecture that subordinates consumer privacy interests to corporate profit-maximization.

In Solove's analysis, the first step is to identify the broken architecture.[71] In the access right system, the broken architecture is the bureaucracies that prevent consumers from participating in the verification process and that fail to allocate duties to companies as a condition of handling personal data. One barrier to consumer participation is that consumers are not given information about whether their request will be verifiable before the collection of their data. This prevents consumers from participating in the verification process because they cannot withhold data from companies that are unable to verify access requests. To make matters worse, under the CCPA the first party data collector is only obligated to inform the consumer about the categories of companies to whom they may sell their data, not the actual company.[72] Therefore, even if verification information was available, there is no opportunity for the consumer to inform herself about the verification policies of the third-party AdTech companies to whom her data will be sold.[73]

Furthermore, companies have no affirmative responsibilities to make any specific efforts to ensure that requests will ultimately be "verifiable." The main strength of Solove's FIPs-driven analysis is his willingness to put the burden on the companies that hold data. Understanding data processing as a privilege helps to overcome the assumption in the credit industry that identity theft will continue. As for the CCPA access request, there are no assumptions yet because the right is brand new. Therefore, starting the system off with an underlying assumption that it is the responsibility of companies to have secure and effective verification procedures could help avoid the issues that arose in the credit context.

While the architectural framework that Solove provides is useful, his actual proposal largely relies on market forces to change company behavior. Architectural changes that focus on participation and responsibility do not address the company incentives to undercut access request verification. Responding to access requests can

---

[71] Solove, *supra* note 27, at 1227, 1250.

[72] CAL. CIV. CODE §§ 1798.100–1798.199 (Deering 2018).

[73] CAL. CIV. CODE § 1798.100(a) (Deering 2018).

Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.232 ● http://tlp.law.pitt.edu

be costly, so companies save money by disposing of them under the guise of "unverifiability." The "participation and responsibility" verification structure makes it more difficult (and more costly) to argue a request is unverifiable, which could change the calculus to some degree. However, companies subject to legislative "responsibility" requirements will still be incentivized to interpret the requirements in a way that reduces their obligations.

Not only does the approach not consider the incentives to avoid the cost of responding to access requests, it also fails to consider the big-picture incentives to avoid all control right obligations. Companies are incentivized to collect as much data as possible, meaning they have an interest in avoiding CCPA deletion and opt-out rights. Thus, even if it was cheaper for a company to respond to an access request than to fight it, the company might still be incentivized to not respond because access requests facilitate deletion and opt-out rights. Therefore, companies may ignore participation and responsibility enhancing measures or implement them in a way that frustrates their ultimate goal. For example, companies could respond to access requests but provide the data in a format that is incomprehensible to most consumers.[74]

Since the administration of data control rights is an area that is rapidly evolving, legislation will be unable to address all relevant circumstances when drafting "responsibilities." Thus, as was the case with the Red Flag rules, there will be substantial ambiguity in any attempt to craft a set of defined responsibilities. This leaves room for companies to interpret the rules in a way that minimizes their responsibility. Inevitably, lawmakers and companies will find themselves in a game of cat and mouse, with regulators constantly trying to end the latest regulatory circumvention as companies develop new tactics to stay one step ahead.

This may seem like a pessimistic view of ad tech company behavior. However, I anticipate that companies will both follow the law and act in their own best economic interest, which is permitted and encouraged through capitalism. Under this theory, companies will only follow the *spirit* of the law if the market demands it. It is far from certain that consumers will pressure companies to follow verification processes and that consumer confidence will impact company behavior. Thus, the consumer protections guaranteed by the obligations imposed on companies in the "participation and responsibility approach" may be limited. Therefore, legislatures should limit their use of Solove's theory to his view of architecture and his reallocation of burden to the data holder, rather than draw on his specific approach.

---

[74] Making an access request on the Weather Channel is complicated as the data is not in plain language and would therefore be incomprehensible to anyone without computer programming experience. THE WEATHER CHANNEL, *How Do I Manage Data Related to my Usage of Weather.com*, https://feedback.weather.com/customer/portal/articles/2938935-how-do-i-manage-my-data-onweather-com- (last updated May 20, 2019).

Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.232 ● http://tlp.law.pitt.edu

B. Strict Liability Approach

Hoofnagle's approach could apply to access request verification by imposing strict liability on companies when they refuse access requests and when they disclose data to someone other than the rightful data subject. Damages would be difficult to quantify, but not impossible. As in Hoofnagle's proposal, those with demonstrable economic injuries would be able to plead that amount. For those without demonstrable economic injuries, administrative penalties could be instituted. The most important figure in the calculus of administrative penalties would be the amount of money it would take to impact the behavior of companies developing verification processes. It is also critical that enforcement of the penalties is adequate.

Under this system, companies would independently dictate their verification systems and would be free to deem requests unverifiable with any degree of frequency. However, the imposition of strict liability incentivizes companies to respond to as many requests as possible, as accurately as possible. This system would incentivize companies to invent creative new solutions to verification challenges that are tailored to their business practices.

The strength of this approach is that it successfully aligns a company's profit-maximization interests with a consumer's privacy interests. However, there are several potential issues with the strict liability regime. First, it is possible that the total cost to companies of maximizing verification procedures is more than the aggregate cost to victims of rejected access requests and verification data breaches. If this is the case, it means that, unlike in Hoofnagle's original proposal, the strict liability system is economically inefficient. The net increase in costs will inevitably be passed onto the consumers, leaving most consumers worse off than they would have been with a weaker verification system.

The cost of the verification system likely exceeds the demonstrable economic savings of consumers because there are not clear costs associated with a rejected verification requests. However, demonstrable economic savings are not the only or the best way to calculate costs in this context. Unauthorized access to data and loss of data control are both privacy harms. Privacy harms do not necessarily correspond with economic loss, instead they relate to the peace of mind associated with controlling one's personal information.[75] Therefore, the calculus of whether strict liability is economically rational depends on the value placed on the ability to keep information confidential, which is highly discretionary. Thus, the decision presents a policy issue more than a strictly economic calculus.

A final issue is that the system could lead to frivolous lawsuits. Even if the recovery is small, requests could be made to hundreds of companies. This is not a

[75] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 200 (1890).

Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.232 ● http://tlp.law.pitt.edu

serious issue in the identity theft context where a claim can only be made if there is actually a fraudulent disclosure. Even if this concern can be mitigated by statutory exemptions for obviously frivolous or excessively frequent requests, it is still inevitable that strict liability will lead to an increase in requests. Thus, companies will not only have to bear the costs of improving their systems but will also have to account for an increased number of requests. These increased costs will not correspond with improved consumer data control because the requests are being used as lawsuit vehicles rather than as a means to learn about data and exercise of other data control rights. This activity is creating additional costs to the verification system that would not exist but for the strict liability regime.

C. Government Control of Verification Procedures

LoPucki effectively removes companies from the verification design process and puts the government in charge. By adopting this approach, the government decides the burden that the government, companies, and applicants will endure in exchange for improved verification. Thus, for the impacted portion of verification—i.e. verification of those who choose to enroll—the government has made all of the trade-off decisions. Under this system, companies will rarely be liable for issues relating to access request verification because following the contact procedures is a modest sacrifice for *de facto* legal immunity. The security benefits of this system, assuming it works, are obvious. However, the major flaw with this system is that it reallocates the verification costs to the government, and thus the taxpayers. Therefore, companies that collect personal data are on equal ground in terms of paying for the verification of the data that they hold with every taxpaying citizen. Thus, Solove's idea that data processing comes with responsibilities is unrealized.

Another issue is that, since companies have no incentive to improve verification, consumers will bear the responsibility of any further data security measures. Thieves will inevitably shift their attention towards breaking into email accounts, phones, and mail boxes to intercept verification communications. Thus, to protect their data, consumers will invest time and money in increasingly creative and impenetrable contact methods. Moreover, this dynamic will inevitably lead to a wealth gap, in which the data of those who can afford superior protections is safer than the data of those who cannot. This might be less problematic in the context of credit where, as a group, wealthier people are more valuable identity theft targets because they generally have better credit ratings, which arguably justifies heightened protections for the wealthy. However, in the context of access requests, a situation in which the PI of the wealthy is more secure than the PI of the poor is unjust.

Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.232 ● http://tlp.law.pitt.edu

CONCLUSION

The CCPA access right has the potential to give Californians a level of control over their personal information that is unprecedented in the United States. However, full realization of these rights hinges on the implementation of effective verification systems. An effective privacy policy must both protect consumers' control over their data and the confidentiality of their data. Consumer control and confidentiality are often in tension so, absent further legislation, companies will balance control and confidentiality interests in whatever way is the least costly. The results of such balancing will inevitably fail to protect consumer interests. Thus, access rights will only avoid the pitfalls of the credit verification system if there are legislative safeguards that force companies to prioritize consumer interests in their implementation of verification systems. While the road remains unclear, the proposed solutions help identify potential resolutions to identity theft in a system that incentivizes companies to protect privacy.

Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.232 ● http://tlp.law.pitt.edu