SCTE•ISBE CABLE-TEC EXPO® VIRTUAL EXPERIENCE » OCTOBER 12-15 2020

2020 Fall Technical Forum SCTE·ISBE • NCTA • CABLELABS®

Fraud Prevention and Privacy Law

Emerging Conflicts Between Privacy Law and Fraud Prevention

A Technical Paper prepared for SCTE•ISBE by

Will Bracker
Corporate Counsel, Privacy
Cox Communications
Atlanta, GA
Will.Bracker@cox.com

Steve Goeringer
Distinguished Technologist
CableLabs
Louisville, CO
s.goeringer@cablelabs.com

Simon Krauss
Deputy General Counsel
CableLabs
Louisville, CO
s.krauss@cablelabs.com

Table of Contents

List of Figures

1. Introduction

Laws and regulations protecting privacy are not new. In Western civilization, case law on privacy extends back to the early 1400's, when the law prohibited eavesdropping. But what is new is the emergence of comprehensive privacy laws and their supporting regulations. These statutory schemes create broad rights for citizens and impose significant obligations on businesses with respect to collection, use and protection of personal information. Steep non-compliance penalties and short implementation timelines require businesses to build robust compliance programs.

In a global economy, building these new compliance functions is no easy task: each new comprehensive privacy law is different from the last, creating a challenging environment for multi-state or multi-national enterprises. New rights and obligations also have the potential to provide new lines of attack for fraudsters and can limit the ability to detect and prevent fraud. Finally, the global pandemic brings a heightened challenge and creates even more opportunities for bad actors to compromise privacy and evade consequences.

This paper examines two specific privacy requirements in light of an operator's need to conduct fraud detection, mitigation, investigation, and prevention. Considerations include anti-fraud information collection, sharing, and action. These areas, indeed anti-fraud operations in general, are often overlooked as risk and legal departments draft compliance program guidelines.

2. Comprehensive Privacy Laws

On May 25, 2018 the General Data Protection Regulation (GDPR) came into effect in the European Union, ushering in a new era for privacy protection: The Age of the Comprehensive Privacy Law. Rather than addressing privacy and data protection in an individual business sector or activity, a comprehensive privacy law grants citizens global control over the collection and use of their personal information. Broadly speaking, these rights allow citizens to access their data, understand how it is used and who it is being shared with, correct errors, restrict use, and require deletion.[1] New business obligations are also part of the landscape, generally requiring greater transparency as to data held by the business, limitations on processing and use, and enhanced duties on those who would use the personal data of their citizens.[2]

These laws require new regulations and new regulators, which in turn requires that businesses create new compliance programs to ensure that they do not fall afoul of another commonality of these laws: substantial penalties for non-compliance.[3]

In the United States, comprehensive privacy law at the state level is moving quickly. California's Consumer Privacy Protection Act of 2018 (CCPA) was the first such law to see the light of day – but more are coming. According to the International Association of Privacy Professionals (IAPP), sixteen

[1] The International Association of Privacy Professionals (IAPP) has identified commonalities that apply to these privacy laws: Access to collected data, access to shared data, right to correct data, delete data, restrict the use of personal data, data portability, the right to opt out of use, prohibit automated decision making, and whether or not a consumer can sue for violations of the law, also referred to as a private right of action.
[2] These obligations as identified by IAPP include: Age based opt-in, notice and transparency requirements, data breach notifications, risk assessments, prohibitions on discrimination, purpose limitations, processing limitations, and heightened or fiduciary duties for storage and use of personal data.
[3] General Data Protection Regulation, Chapter VII, Article 83; California Consumer Privacy Act of 2018 1798.150, .155

states have a comprehensive privacy bill at some stage of their legislative process. In addition to California (which is likely to revise the 2018 CCPA Act, which just became effective, via the California Privacy Rights Act of 2020), Maine and Nevada have already passed legislation. Other states with legislation in progress are Arizona, Connecticut, Hawaii, Illinois, Iowa, Louisiana, Maryland, Massachusetts, Minnesota, Nebraska, New Hampshire, New Jersey, New York, North Dakota, South Carolina, and Texas. Many of these states have more than one bill under consideration. Legislation was raised in eleven other states. This is summarized in Figure 1 (used with permission of IAPP). See the IAPP website for current details (https://iapp.org/resources/article/state-comparison-table/).

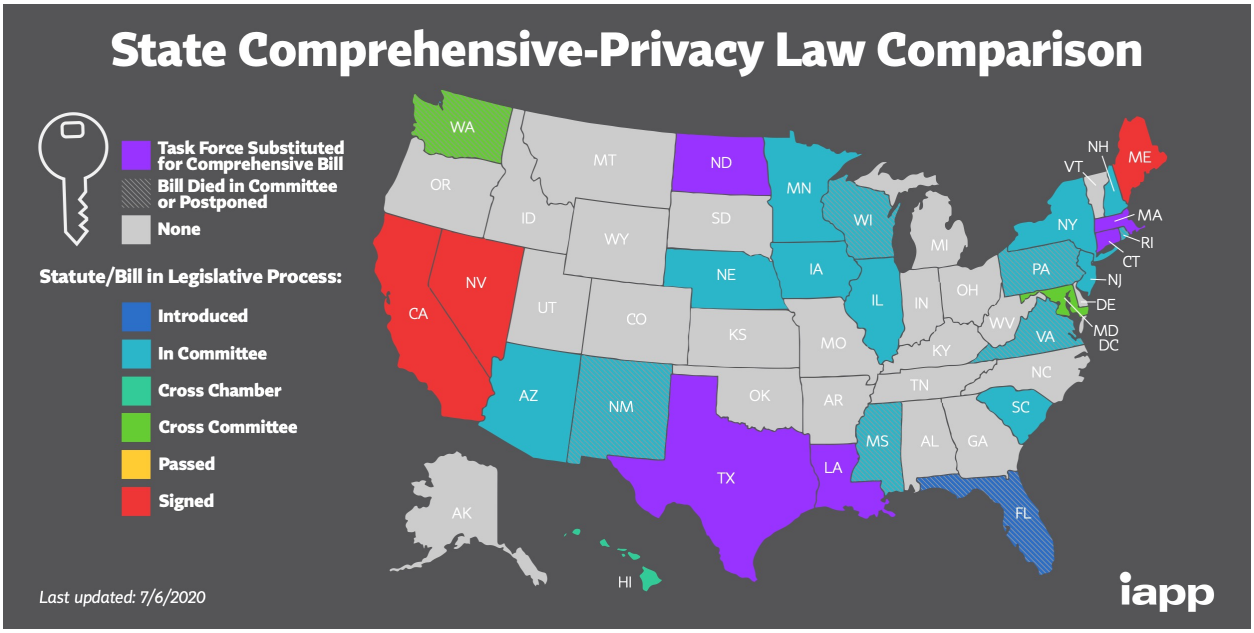

Figure 1 - Status of US state level comprehensive privacy legislation

Simply put, merely keeping up with all of the state legislative activity is a daunting task.

One of the challenges operators face is that different jurisdictions (*e.g.*, Europe, Canada, different states, etc.) have enacted and are in the process of drafting and/or enacting different laws, so there will be multiple frameworks to apply depending on the context of the private information being protected and the regions in which it applies or exists. For example, consider a seemingly simple concept like the definition of personal information. The GDPR defines personal data as:

any information relating to an identified or identifiable natural person ('data subject');

PIPEDA is equally brief in its definition of personal information:

information about an identifiable individual.

CCPA is considerably more verbose:

"Personal information" means 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.

in fact, the full text of the CCPA definition extends to some 238 words, reproduced in the footnote below.[4]

The regulatory process that follows the enactment of the law adds to the complexity of the compliance landscape. The rulemaking process for the CCPA recently came to a close, six months after the underlying law came into effect.

In California, the cost of initial compliance with the law was estimated at a staggering $55 billion. Depending on the number of firms ultimately deemed to be covered by the CCPA, the ongoing annual compliance is estimated to be between $466 million and $16.4 billion.

In addition, once laws are enacted, court interpretations of those laws will doubtless vary. This paper provides examples of the challenges of compliance with the variety of privacy laws found in the CCPA (which may change again in November), the GDPR (which, while focused on data protection, does address privacy), and Canada's Personal Information and Electronic Documents Act (PIPEDA).

Complexities aside, the intent of a comprehensive privacy law is to allow a citizen greater visibility and control over the use of their personal data and to require businesses to focus attention and resources on the protection of that personal information. However, as written, these laws may actually make that task more difficult.

3. Comprehensive Privacy Law vs. Fraud Detection and Prevention

> Fraud (n): *deceit, trickery.* Wrongful or criminal deception intended to result in financial or personal gain.[5]

The data ecosystem of privacy law between company and citizen customer has a third actor lurking in the shadows: fraudsters. Such individuals, criminal rings, and nation-state actors all use the same basic

---

[4] '(o) (1) "Personal information" means 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, the following:
(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
(B) Any categories of personal information described in subdivision (e) of Section 1798.80.
(C) Characteristics of protected classifications under California or federal law.
(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
(E) Biometric information.
(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.
(G) Geolocation data.
(H) Audio, electronic, visual, thermal, olfactory, or similar information.
(I) Professional or employment-related information.
(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).
(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

[5] https://www.lexico.com/en/definition/fraud

approach to access the value contained within that ecosystem: they lie about their identity. Using a combination of personal data gathered from public and stolen private sources as well as purely synthetic identities, fraudsters attempt to deceive one side of the transaction into believing that they are the other expected actor, and then extract the value in the transaction for themselves.

Preventing such attempted deception is at once simple and complex: the key lies in having sufficient personal information about the other actor in the transaction to distinguish a fraudster from a legitimate actor. Techniques for accomplishing this range from a simple picture ID check by a retail clerk to sophisticated big data solutions that evaluate the risk of a transaction based on hundreds or thousands of data points processed by sophisticated algorithms. Simple or complex, the core component of every prevention technique is the use of personal information to disprove the fraudster's impersonation of the legitimate actor.

Comprehensive privacy laws can be used as both sword and shield to a fraudster. Offensively, the right to know can be used to gain information about an individual to make impersonation harder to detect. Defensively, fraudsters can use the transparency, opt-out, and deletion rights of the new laws to hinder or evade detection and to determine what data is being used to detect them.

3.1. Right to know

Citizen rights under comprehensive privacy laws start at a common point: in order to exercise the other rights granted, it is important for the citizen to know what personal data a given company is storing about them. Therefore, the first right granted under a CPL is the right for a citizen to require a company to provide a record of that data to the citizen. This represents a brand-new opportunity for fraudsters to accumulate the information necessary to impersonate their targets.

How this is done was documented by James Pavur and Casey Knerr at Blackhat 2019. In their seminal white paper, *GDPArrrrr: Using Privacy Laws to Steal Identities,* they show the weaponization of privacy tools and laws, using GDPR "right to know" requests on 75 companies, and providing only publicly available information about the subject as authentication. The GDPR right to know is one of the basic data subject rights; willful failure to comply with this requirement can subject a company to a penalty up to the greater of 20 million euros or 4% of the firm's annual worldwide gross revenue. Given the severity of the penalty for non-compliance, it is perhaps unsurprising that some companies erred on the side of compliance and divulged at least a subset of the requested personal information.

James and Casey then used the data from the responses to craft 75 additional right to know requests. Enriched with the data from their initial harvest, these requests were much more productive. They received 10 digits of credit card numbers, expiration date, login credentials for websites, educational test scores, complete hotel records, dating profiles, purchase histories, and much more.

3.2. Right to be forgotten

> Fool me once, shame on you. Fool me twice, shame on me… but what if I had to forget that you fooled me?

Some of the citizens' rights and business obligations created by new comprehensive privacy laws are being misused by bad actors to both further their fraud schemes and to escape or evade fraud detection. Fraudsters can leverage new consumer rights that commonly include access to collected data, access to shared data, correct data, deleting data, opting-out of use, and prohibited automated decision making. Business obligations can also be abused including notification and transparency requirements, purpose limitation, and processing limitations.

For example, under GDPR, bad actors use the right to know in order to gather personal information of their targets. They also have used the right to be forgotten to conceal their identities and reduce the effectiveness of notice, public safety, and fraud prevention tools.

Part of the challenge is that consumers don't have a specific, immutable identifier on which operators can tie personal information. Thus, it's very hard implement consumer interfaces to provide privacy management features that are secure – that is, hard to misuse.

In addition, privacy laws limit fraud investigations by limiting both what information is collected and how an operator may use it. For example, GDPR contains a limited exception to share information without consent when "processing is necessary for the purposes of legitimate interests pursued by the controller or by a third party". Preventing fraud has been defined as a legitimate interest. However, the sharing exception language was not carried over into the subscriber's right to have their information deleted.

The CCPA also includes several exceptions for the collection, retention, and disclosure of personal information that intersect with anti-fraud efforts. These are:

- To detect data security incidents, or protect against fraudulent or illegal activity;
- To comply with laws;
- To comply with government investigations;
- To cooperate with law enforcement; and
- To exercise the defense of legal claims, including evidentiary privilege.

Moreover, there are additional areas that must be considered that are not well defined within current laws. Privacy is transitive. So, as fraud investigations are conducted, while information that is shared with law enforcement and other governmental agencies may be in compliance with governmental investigations, does information shared with private entities that may benefit from receiving the information in relation to their own fraud investigations (such as other operators) give rise to privacy law violations? Other laws may also govern the disclosure and use of private information, such as the U.S. Fair Credit Reporting Act, which may govern how an operator may use information about prior fraudulent activity to deny a person service.

An awkward question is whether fraudsters themselves enjoy privacy protection. A clear example of contention, for example, is the case where fraudsters are also customers or even business partners (such as channel sales companies). However, many cases are not so clear. Is a fraudulent customer's personal data (which may not even be legitimate) protected? Is personal information from cyber-attacks protected?

4. Fraud Prevention and Privacy Law in a Pandemic

Finally, the COVID-19 pandemic has made the task of fraud prevention more complex while simultaneously raising the payoff for fraudsters.

Distanced communication makes the process of investigation more difficult. Interviews are being conducted via video or teleconference, depriving investigators of the ability to observe their subjects. In the pre-COVID world, many exception processes to web- or phone- based provisioning or identity flows would direct the individual to go to a physical location and present themselves with one or more forms of government issued identification for visual comparison by a human being. But in the present circumstances, consumers are unable to go to a physical service location and interact with an in-person

representative of an agency or a business. All parties in a transaction are instead left reliant on telephone or digital verification methods to measure the risk of a transaction and decide whether or not to proceed.

This weakening of in-person verification processes has not gone unnoticed by fraudfeasors. The FTC reports that, as of June 28th, U.S. citizens have reported losses more than $108 million to COVID-19 related scams and fraud schemes. Identity theft of both individual and business entities is on the rise as bad actors take aim at enriched unemployment benefits and small business support programs.

5. Conclusion

This article provides just a short survey of the issues that intersect privacy and fraud. It does not purport to provide any prescriptive approaches or formulas for how to address those issues. That is because it cannot do so—such solutions are simply too complex. Moreover, compliance is jurisdictionally specific. The requirements and obligations that drive compliance for one operator will not fully apply to another operator operating in states, let alone countries. Nevertheless, it is important that compliance teams consider fraud detection, investigation, mitigation, and prevention efforts as they develop and evolve guidelines and procedures for their companies.

Abbreviations

CCPA	The California Consumer Privacy Act
GDPR	The General Data Protection Regulation
PIPEDA	The Personal Information and Electronic Documents Act
IAPP	The International Association of Privacy Professionals

Bibliography & References

California Consumer Privacy Act, State of California Department of Justice, online, https://oag.ca.gov/privacy/ccpa

Data protection in the EU, European Commission, online, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

The Personal Information Protection and Electronic Documents Act (PIPEDA), Office of the Privacy Commissioner of Canada, online, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

US State Comprehensive Privacy Law Comparison, IAPP, online, downloaded July 20, 2020. https://iapp.org/resources/article/state-comparison-table/

"GDPArrrrr: Using Privacy Laws to Steal Identities", James Pavur and Casey Knerr, Blackhat USA 2019 White Paper.

