US Data Privacy Law: Federal and State Legislation, Impact, and Risk Mitigation

By Frank C. Barile (Cornell Tech)

US Data Privacy Law: Federal and State Legislation, Impact, and Risk Mitigation

By Frank C. Barile (Cornell Tech)

Recently approved privacy legislation in the US indicates momentum for additional state privacy laws and perhaps even a general federal law. Subject businesses may be impacted and can mitigate risks by adhering to best practices.

INTRODUCTION

Recent Privacy Laws

Following the European Union's 2018 General Data Protection Regulation[1] ("GDPR"), state privacy laws have been levied in California and Virginia, and many more are proposed in other states and Congress. Momentum is building for more privacy laws.[2]

Scope

It varies by jurisdiction, but generally privacy laws apply to businesses that process (generally meaning collect, use, sell, distribute, etc.) personal information of consumers that are resident in a jurisdiction with an applicable privacy law.

Impact

If a business processes (collects, uses, sells, distributes, etc.) personal data in a jurisdiction that has a privacy law, it may be subject to such privacy law. Privacy laws can have a broad application, so businesses should equip themselves to know whether they are even in scope. Existing privacy laws generally impose obligations on subject businesses that process consumer information, such as required disclosures, creating policies and procedures, responding to requests, etc. **Businesses may also be subject to fines[3], corrective action[4], and private rights of action**[5]. Separately, businesses can suffer reputational damage from violations of data privacy laws.

[1] General Data Protection Regulation, 2016, OJ L 119, 04.05.2016
[2] Wendy Zhang, *Comprehensive Federal Privacy Law Still Pending*, Volume XI Natl. L. Rev. Number 77 (March 18, 2021)
[3] Cal. Civ. Code §§ 1798.155, 1798.199 (2018)
[4] Id. § 1798.106
[5] Id. § 1798.150

FEDERAL PRIVACY LAW

Current State

There currently is no general federal privacy law in the US. There are however federal privacy laws that focus on a particular "vertical" concern, called sectoral privacy laws.[6] A business may already be subject to these laws depending on what information it processes. For example, HIPAA[7] imposes privacy obligations for covered entities processing health-related information. For sectoral laws, the scope is generally limited to a specific purpose, whether an industry or type of consumer. Today, no current federal law simply covers *all* personal information.

In addition to federal sectoral laws, state laws exist to protect general privacy, notably the California Consumer Privacy Act[8] ("CCPA") and the recently-levied Virginia Consumer Data Protection Act[9]. **Thus, right now if a business processes data in the US, it must comply with a patchwork of the aforementioned federal sectoral laws *and* these state laws, to the extent applicable**.

Compliance with the medley of federal sectoral laws and state laws can be onerous. An additional burden is applying the varying extra-territorial reach of each state law.[10] For example, one state law may protect its own residents even if temporarily out of the state physically, or even based upon whether the processor does enough business into that state. Each of these raise further inquiries; if data is processed in a cloud, what is the touchstone that triggers the law- where the server is physically located? Where the consumer or processor is located? Perhaps any combination of the foregoing? It's even possible each state law can apply concurrently. This quandary can largely be resolved with a sweeping federal law that applies to all data; however, this solution has its own limitations, notably the pre-emption issue.

Pre-emption

A general federal privacy law may enhance protections for consumers in an ever-increasing digital world. The most contentious debate right now is pre-emption. Pre-emption simply means that a federal law will supersede state laws on a particular subject. If a federal law is created that does not pre-empt state law, it merely creates a bare minimum law and states can then pass stricter privacy laws. **Without pre-emption, a general federal privacy law may be tantamount to a mere minimum standard that each state must adhere to, and businesses *still* must navigate a patchwork of varying state law**

[6] Examples of sectoral privacy laws in the US include the Graham-Leach-Bliley Act (covering financial information) and the Children's Online Privacy Protection Act (focuses on children under 13 years of age).
[7] 45 CFR Part 164 (2000)
[8] Cal. Civ. Code § 1798
[9] Sarah Rippy, "Virginia passes the Consumer Data Protection Act", *International Association of Privacy Professionals*, March 3, 2021 https://iapp.org/news/a/virginia-passes-the-consumer-data-protection-act/
[10] The same argument could be made for the EU's GDPR, as it has extra-territorial reach to data processors that process data of EU residents.

obligations. Thus, while it perhaps protects consumers, a general federal privacy law that doesn't pre-empt state law doesn't resolve the patchwork issue for businesses. This may call into question the utility of such law.

Compliance with varying state and federal laws could materially increase costs and risks for businesses. As a result, businesses are likely to find non-pre-emptive federal privacy laws to be burdensome without actually resolving the patchwork issue. Consumers may oppose pre-emption, because without it, it can only serve to broaden their rights and recourse against subject businesses. Naturally, some consumers may be aware that businesses can simply pass on costs to consumers and such consumers may become ambivalent to pre-emption. Regardless, pre-emption allows businesses to have one comprehensive privacy program. Businesses may support pre-emption even if the federal law is perhaps stricter in some areas, because a pre-emptive federal law eliminates the patchwork of varying state laws[11] and also alleviates the aforementioned extra-territoriality issues.

Private Rights of Action

A critical question in any data privacy law is whether it allows a private right of action. Generally, data privacy laws allow for the government to investigate and censure businesses for violations of the law. However, some jurisdictions that have privacy laws, such as California, go further and provide a civil right for *consumers* to sue businesses for damages and injunctive relief. If a class action ensues, impacted consumers can number into the millions, each seeking damages.[12] **Private rights of action thus increase the stakes for businesses as their liability can be much greater, in addition to government action**. Where a private right of action exists, a business should be aware of exposure to both government and consumers, and even reputational risk.

Proposals

In the wake of the EU's GDPR, California's CCPA, and Virginia's Consumer Data Protection Act, Congress (and even many US states) have been busy proposing privacy laws of varying forms. Privacy laws, whether proposed or finalized, have also proliferated in other developed markets, such as China, Canada, and Brazil.[13] They also persist in many other countries in Asia, particularly in Japan, Singapore, and Korea. As a result, pundits think it's inevitable that Congress will pass a general federal privacy

[11] The question of whether a general federal privacy law would supersede existing sectoral laws is certainly possible, but would depend on how it is worded, and thus is yet to be determined.
[12] A data breach at Yahoo! impacted 194 million consumers and resulted in a $117,500,000 fine. *In Re: Yahoo! Inc. Customer Data Security Breach Litigation*, 2020 U.S. Dist. LEXIS 129939 (N.D. Cal. July 22, 2020)
[13] Jennifer Bryant, "2021 'best chance' for US privacy legislation", *International Association of Privacy Professionals* December 7, 2020 https://iapp.org/news/a/2021-best-chance-for-federal-privacy-legislation/

law.[14] **The momentum for more privacy law is clear and has never been greater**. Since 2019, a dozen bills have been introduced in Congress concerning general data privacy, with mostly Senate Democrats leading the way. Most notably, Senator Ed Markey (D-MA) sponsored the Privacy Bill of Rights Act[15], and Senator Maria Cantwell (D-WA) sponsored the Consumer Online Privacy Rights Act[16], and Senator Jerry Moran (R-KS) sponsored the Consumer Data Privacy and Security Act[17].

Additionally in 2019, Senator Ron Wyden (D-OR) sponsored Mind Your Own Business Act[18], Senator Catherine Cortez Masto (D-NV) sponsored the Digital Accountability and Transparency to Advance Privacy Act[19], Senator Marco Rubio (R-FL) sponsored the American Data Dissemination Act[20], Senators Amy Klobuchar (D-MN) and John Kennedy (R-LA) sponsored the Social Media Privacy and Consumer Rights Act[21], Representatives Anna Eshoo (D-CA) and Zoe Lofgren (D-CA) sponsored the Online Privacy Act[22], and Representative Suzan DelBene (D-WA) sponsored the Information Transparency and Personal Data Control Act[23].

In 2020, even more bills were proposed, such as Senator Kirsten Gillibrand (D-NY) introducing the Data Protection Act[24]. In September 2020, Senator Roger Wicker (R-MS) introduced a bill in conjunction with Senators John Thune (R-SD), Deb Fischer (R-NE), and Marsha Blackburn (R-TN)[25], entitled the Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act[26] ("SAFEDATA"). **Given that proposals are proliferating but now also becoming more bipartisan, it might indicate that Congress may act soon on a general federal privacy law**. While the bills may vary in content, most proposals define personal data broadly, provide rights to access, control, and delete data, and prohibit discrimination against consumers. The proposals largely do not create a separate regulatory agency to enforce the law.

The most contentious debate in SAFEDATA is the aforementioned pre-emption issue; will SAFEDATA supplant the varying state laws, or simply impose a minimum requirement? The pre-emption issue is split amongst party lines, with Republicans supporting pre-emption, and Democrats opposed. The exception

[14] Karen Schuler, "Federal data privacy regulation is on the way — That's a good thing", *International Association of Privacy Professionals*, January 22, 2021 https://iapp.org/news/a/federal-data-privacy-regulation-is-on-the-way-thats-a-good-thing/
[15] Privacy Bill of Rights Act, S.1214, 116th Cong. (2019)
[16] Consumer Online Privacy Rights Act, S.2968, 116th Cong. (2019)
[17] Consumer Data Privacy and Security Act, S.3456, 116th Cong. (2019)
[18] Mind Your Own Business Act, S.2637, 116e Cong. (2019)
[19] Digital Accountability and Transparency to Advance Privacy Act, S.583, 116e Cong. (2019)
[20] American Data Dissemination Act, S.142, 116th Cong. (2019)
[21] Social Media Privacy Protection and Consumer Rights Act, S.189, 116th Cong. (2019)
[22] Online Privacy Act H.R.4978, 116e Cong, (2019)
[23] Information Transparency & Personal Data Control Act, H.R.2013, 116e Cong. (2019)
[24] Data Protection Act S.3300, 116th Cong. (2020)
[25] Most recently, in January 2021 Senator Blackburn sponsored the BROWSER Act. Balancing the Rights of Web Surfers Equally and Responsibly Act, S.1116, 116th Cong. (2019)
[26] Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act, S.4626, 116th Cong. (2020)

is Representative DelBene (supporting pre-emption) from Washington State, a state government largely dominated by Democrats. It is notable that Washington State is home to some of the largest technology businesses that would be subject to a privacy law.

Another issue is whether SAFEDATA will contain the aforementioned private right of action – the right for consumers to pursue a business for damages under a violation of applicable privacy laws, which includes class action suits. Current proposed federal laws are mixed on whether a private right of action should be provided, with a slight majority omitting the right.

Lawmaking

Currently, the Democratic party has a slight advantage in Congress. While Republicans hold a 50-48 majority in the Senate, two independent senators caucus with Democrats[27], and the tiebreaker is decided by Vice President Kamala Harris, a Democrat. Democrats also have a slight majority in the House of Representatives, currently holding 220 seats to the Republicans' 211. If enough Democratic members of Congress defect, a bill could stall, particularly in the Senate where the majority is razor thin- so thin, it will likely require a tie breaker.

Also notable is that in 2010 the White House under President Barack Obama and then-Vice President Biden published a Consumer Privacy Bill of Rights ("CPBR"), predating existing data privacy laws.[28] While it is merely a listing of principles, it is aligned in spirit with current proposals. The 2020 Democratic party official agenda includes updating the CPBR, including "adding strong national standards to protect consumers…" from data breaches.[29] **With Democrats holding an edge in Congress, and President Biden in the White House, the path is theoretically cleared to install the Democratic agenda**.[30] The 2020 Democratic agenda is clear that data privacy is supported.[31]

Naturally, merely achieving a majority in government doesn't guarantee a law will pass. In fact, even if a bill is signed into law, the process could water it down the proposals or materially change its provisions. Regardless, the opportunity is available should Democrats seek to advance their agenda. As for leadership, House Majority Leader Nancy Pelosi (D-CA) represents California- the vanguard of state privacy rights. Also, the Senate Majority Leader, Charles Schumer (D-NY) has shown recent interest in

[27] Senator Bernard Sanders (I-VT) and Senator Angus King (I-ME) both caucus with the Democratic party.
[28] Press Release, The White House Office of the Press Secretary, We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online (February 23, 2012) https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights
[29] 2020 Democratic Party Platform, *Democrats.org*, August 2020 https://democrats.org/wp-content/uploads/sites/2/2020/08/2020-Democratic-Party-Platform.pdf
[30] Id. at 26
[31] Id. at 25.

data privacy in 2017.[32] Similar to Washington State, both California and New York have a notable presence of large businesses that are or will be impacted by data privacy laws.

Congress is likely preoccupied with pressing topics, such as the global pandemic and stimulus bills, so privacy may fall lower on the priority list. Since a general federal privacy law may be on the horizon, perhaps the only remaining question is what its contents are, specifically on the pre-emption issue.

STATE PRIVACY LAW

Both globally and in the US, **recent legislation and proposed laws may indicate a coming wave of state privacy laws**[33]. Because California is an early adopter of privacy law, and a strict privacy law at that, any resulting general federal privacy law could have elements of the California privacy law or even its nascent enforcement practices.

California

In 2018, California passed CCPA, the first comprehensive general privacy law in the US, effective January 1, 2020. It protects and provides rights for California residents.[34] The definition of personal information is broad. CCPA applies to businesses meeting one of three triggers – gross annual revenues of over $25m; processing personal information 50,000 California residents, households, or devices; or deriving 50% or more of annual revenues from selling California residents' personal information.[35] **CCPA is extra-territorial; it applies to businesses even if they don't have a physical presence in California but process data of California residents**.

In more detail, CCPA includes individual rights for consumers, for example, the right to know what personal information a business has or will process, the sources, the purposes of processing, and whether data is shared with third parties. Consumers can compel deletion, though, some exceptions do exist (whether a legal obligation, regulatory obligation, or the data is being kept for the purposes that it was shared). Consumers may opt out of the sale of their data. Notice must be given to consumers about their data being processed and their privacy rights.

[32] Press Release, Charles E. Schumer, Schumer: Privacy Rules Protecting The Most Sensitive Personal Information Stored On Your Computer Or Cell Phone Are About To Be Eliminated (March 26, 2017) https://www.schumer.senate.gov/newsroom/press-releases/schumer-privacy-rules-protecting-the-most-sensitive-personal-information-stored-on-your-computer-or-cell-phone-are-about-to-be-eliminated-senator-demands-house-of-reps-kill-attempt-to-undo-privacy-rules-before-info-on-your-health-family-finances-and-more-is-for-sale
[33] Sarah Rippy, "US State Comprehensive Privacy Law Comparison", *International Association of Privacy Professionals*, last updated March 22, 2021 https://iapp.org/resources/article/state-comparison-table/
[34] California Attorney General Op., CCPA Frequently Asked Questions, FAQ #2 https://oag.ca.gov/privacy/ccpa
[35] Id., FAQ #5

Statutory damages for certain violations can be $100-$750 for each instance. The California Attorney General can also enforce the law against any violation of CCPA resulting in civil penalties of $2500-$7500, per instance, depending on how intentional the violations are found to be. If subject businesses have data of tens of thousands of consumers (or even more), the penalties can multiply quickly.

CCPA currently has a private right of action for consumers. However, it's limited to claims for unauthorized access to personal information or failing to maintain security procedures.[36] In other words, there is no private claim a consumer can sue a business for under *other obligations* in CCPA, for example, not being given an opt out or statement of rights. If a California consumer requests a business remove an email address from its server, and the business fails to do so, the consumer cannot recover under CCPA. There may still be *government prosecution* of the business for such violation of the statute because the California Attorney General has the authority to enforce *all* violations of CCPA.

CCPA does have a cure provision whereby a business can take corrective action to cure its violation. Cure however requires the business to provide an express statement that the violation has been rectified and that no further violations will occur. If businesses haven't properly cured a violation, consumers will then have additional evidence against such business in the form of a documented broken promise. For now, the California Attorney General can also pursue businesses for breaching this express statement.

Less than a year after implementation, California voters – as opposed to the California legislature – approved the California Privacy Rights Act ("CPRA"), amending and strengthening the CCPA. Effective January 1, 2023[37], the CPRA strengthens the CCPA by adding new rights and obligations, such as enhanced opt out rights and disclosures.[38] In particular, CPRA also eliminates the cure period, though it remains for the private right of action. Consumers will be able to request correction of their personal information. CPRA creates a new regulatory agency to enforce the law, the California Privacy Protection Agency ("CPPA"). Perhaps most significantly, it contains odd language that requires future amendments to be "in furtherance of the law", which is an attempt to thwart weakening of the law in the future.

Other States

In 2021, Virginia passed a privacy law entitled the Consumer Data Protection Act. It is not as comprehensive as California's law. It does not contain a private right of action, nor does it create a new enforcement agency, leaving Virginia's Attorney General to be tasked with enforcement.

[36] Megan Gates, "CCPA Deep Dive: How California is Enforcing its Major Privacy Law", *ASIS Online*, December 1, 2020 https://www.asisonline.org/security-management-magazine/articles/2020/12/ccpa-deep-dive-how-california-is-enforcing-its-major-privacy-law/

[37] Despite an effective date of January 1, 2023, the CPRA will apply to data collected as of January 1, 2022.

[38] Cal. Civ. Code §§ 1798 (amended 2020)

About twenty states have proposed privacy laws in varying forms. Washington State is in its third attempt to pass a privacy law.[39] Both New York[40] and Florida[41] have proposals in play. New York even has its own cybersecurity law covering financial services information.[42] It is again notable that these states happen to generally be home to businesses that process much personal data.

IMPACT

Scope

Though few state privacy laws are in force, CCPA is instructive; it focuses its scope on the consumer's residence. For example, if a business in Texas (where there is no general privacy law) collects data from a consumer in California, the CCPA applies. If other states follow California's lead, extra-territoriality can create a web of obligations for a business to comply with. **Businesses therefore should be aware of where consumers are, what's collected and processed, and what law may apply**.

Risks

Privacy laws provide rights to consumers and impose many obligations on businesses that process data. Such obligations, in particular information security requirements, present many risks to businesses as it's a critical concern to protect consumers. **Recent security breaches have embattled some of the world's largest, most reputable companies, causing regulatory censure, fines, corrective action, and even reputational damage**.[43] The list includes Yahoo!, Facebook, Marriott, Twitter, LinkedIn, Adobe, Equifax, eBay, CapitalOne, Uber, and Home Depot.[44] Some events have affected billions of consumers, but in each case, tens of millions of consumers experienced a data breach. These are household names that most consumers have provided data to, which makes it is especially alarming.

Aside from regulatory risk and reputational risk, there is also legal risk in jurisdictions where a private right of action exists. Legal risk includes litigation from consumers, such as class actions. A California class action in 2020 against Amazon's Ring app is currently being litigated. The claim is that Ring violated CCPA by failing to maintain wholly adequate security measures, as evidenced by hackers tapping into Ring's video surveillance data. Plaintiffs also allege that Amazon failed to provide notices on what

[39] Katya Maruri, "Washington State Takes Another Run at Online Privacy Rules" *GovTech*, February 4, 2021 https://www.govtech.com/policy/Washington-State-Takes-Another-Run-at-Online-Privacy-Rules.html
[40] Kyle Faith and Melinda McLellan, "New York Legislature Introduces CCPA Clone with Private Right of Action", *JD Supra*, January 8, 2021 https://www.jdsupra.com/legalnews/new-york-legislature-introduces-ccpa-6501577/
[41] Hayden R. Dempsey and Kate Black, *Broad New Data Privacy Legislation Supported by Florida Governor and House Speaker*, Volume XI Natl. L. Rev. Number 77 (March 18, 2021)
[42] N.Y. Financial Services, 23 CRR-NY Part 500 (2017)
[43] California Attorney General, Privacy Enforcement Actions https://oag.ca.gov/privacy/privacy-enforcement-actions
[44] Dan Swinhoe, "The biggest data breach fines, penalties, and settlements so far", *CSO Online*, March 5, 2021 https://www.csoonline.com/article/3410278/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html

information was collected and how it would be used. CCPA's private right of action is limited to actual data breaches, and not notice failures or inadequate policies and procedures. While it appears that this complaint may have partially insufficient pleadings, it is still in the pleading stage and may test the limits of the private right of action in court.

Whether private rights of action under CCPA require an actual concrete injury (as opposed from just unauthorized disclosure), courts have left open the question whether mere unauthorized access, without actual harm, is sufficient for standing.[45] If courts interpret injury to include potential future loss, or even a violation of rules, **mere technical violations of CCPA could result in class action liability, even if no actual harm occurs**. This could materially increase litigation risk and costs of class actions for businesses.

Class action risk is distinct from administrative or criminal penalties, which are pursued and enforced by government. Administrative penalties can include fines and injunctions, the latter of which can materially interrupt business operations and impact immediate cash flow. Criminal penalties can be more severe.

Since many businesses process data in conjunction with service providers, vendor risk is potentially significant. Taking CCPA as an example, it defines "processing" of data to include "any operation or set of operations that are performed on personal information… whether or not by automated means". This definition captures businesses that process data and also vendors that process such data. **Further, a business can be liable for the acts of a vendor that violate a consumer's rights**.

Another risk is the cost of corrective action – efforts that rectify the wrongdoing, whether redrafting policies and procedures, implementing information security and testing, hiring staff, obtaining legal advice, performing vendor diligence, and anything else deemed necessary to prevent recurrences.

Enforcement

Because general data privacy laws are largely new, there has not been much enforcement. One could look to the sectoral laws for patterns, however, since they are administered by different agencies for different purposes, it may not be telling to look to sectoral enforcement practices. So far, California began CCPA enforcement actions starting July 1, 2020.[46] CCPA is particularly instructive here not just because it is a strict law, but because California has been a pioneer in this field, and other states may look to California for compelling precedent through enforcement.

[45] Robert Cattanach, Kent Schmidt, and Melonie Jordan, "CCPA Class Actions and Standing Requirements", *Dorsey & Whitney*, March 3, 2021 https://www.dorsey.com/newsresources/publications/client-alerts/2021/03/ccpa-class-actions-requirement-for-standing

[46] Gates, "CCPA Deep Dive"

Many of the existing enforcement actions for CCPA are in the pleading stage. **The current claims focus on unauthorized access or disclosure of data, and data collection without proper notice (or indicating consumer rights)**. California's AG indicated a focus on online providers, promising consumers the opportunity to exercise their rights. When the CPRA goes into effect, the CPPA will assume enforcement duties.

RISK MITIGATION

Proactivity

The pressure on states and Congress to create privacy laws has never been more intense. Businesses as a result should start to consider a data privacy program now. While data privacy laws are fragmented and varying at this time, there are many common elements in existing and proposed laws. **For simplicity, proactive businesses may be wise to adhere to the strictest law**, which is CCPA right now.[47]

Whether or not a business is even subject to CCPA (or any other privacy law), businesses should consider whether they do business with residents of various states. For example, in California, CCPA triggers where a business processes data of California residents. To the extent a business operates a public-facing website, businesses should consider whether they even are aware of processing data of California residents. In addition, there are murky cross-border issues surrounding e-commerce; how does a business – whether brick and mortar or entirely online – really know where a consumer resides?[48]

Privacy laws are largely united in purpose in that they promote transparency and intend to protect consumers by either providing notice or options to them. There are certainly gray areas. Thus, when in doubt, it may be wise to err towards privacy and transparency to avoid running afoul of privacy laws, but also to avoid reputational risk.

Benefits of a Privacy Program

Given the above challenges, and the likelihood of future data privacy laws, it may be wise to consider a data privacy program, whether required by law or not.

[47] The EU's GDPR is likely stricter in some aspects than CCPA.
[48] Joseph Duball, "Challenge accepted: Initial Virginia CDPA reactions, considerations", *International Association of Privacy Professionals*, March 4, 2021 https://iapp.org/news/a/challenge-accepted-initial-virginia-cdpa-reactions-considerations/

Beyond that, consumers may appreciate privacy practices even if not required by law. The sheer number of bills proposed into Congress and state governments likely indicate that consumers aspire to increased privacy. **It thus may represent sound business practice to implement a privacy program now, whether required by law or not**. Businesses may boast that they meet a standard of privacy, even if not obligated to do so. It can increase consumer confidence and enhance a business's brand.

As other states or Congress proliferate privacy laws (some of which appear inevitable), a proactive business taking action would be situated well to adapt to a changing environment. Getting ahead of the legislative curve now can result in savings later. Also, some privacy law is sector specific; following the strictest general privacy regime may alleviate the headaches of having to comply with each sectoral law.

Minimization

Businesses should have a hard look at whether they are collecting and processing more data than is absolutely necessary. Businesses should analyze what data they really need to run their business, and what data they need to process, and whether it makes sense to mitigate risk by minimizing processing. For example, if it's not necessary to collect social security numbers, which can be considered not just personal data but sensitive personal data (eliciting heavier burdens), businesses should consider stopping collection and retention to mitigate risk.

Due to increased automation, it's possible a business is collecting or even processing data and isn't largely aware. **If some data is not necessary to retain (or even collect), businesses should minimize their processing by not collecting it, or at least deleting or de-identifying it**. This is especially the case for sensitive personal data, where the stakes are higher. Without a proper accounting, businesses cannot be certain what data is necessary. To avoid unnecessary risks, businesses should certainly avoid a circumstance where it takes on liability and is not even getting the benefit of processing data.

For minors, some privacy laws have separate measures protecting children. In particular, the Children's Online Privacy Protection Rule[49] ("COPPA") is a sectoral law focused exclusively on protection children. Thus, if businesses process data of consumers that are under a certain age (usually in the 13-16 range depending on jurisdiction), they should consult legal advice as there may be requirements to obtain parental consent or even enhanced obligations and penalties for violations. Similarly, businesses can avoid processing data of minors to circumvent the issue altogether.

[49] 16 CFR Part 312 (1998)

Encryption

To the extent data is processed, businesses should consider encrypting the data. Naturally, once data is disclosed, it can be impossible to claw it back or be "unseen". Encryption will serve to protect consumers from harm; in the event of a security breach, encryption may prevent data being accessed or consumed by third parties or bad actors, minimizing risk.

Vendors

Businesses should put agreements in place with vendors to get representations and warranties.[50] Key terms include definitions of personal information, confidentiality clauses, data deletion and minimization, and backing up data. Vendors also should represent that they will assist with data access requests, entitlements, risk assessments, and penetration testing. Businesses and vendors should consider processes for determining what is a breach, which party will send notices in the event of a breach, and which party takes remedial measures and bears costs. Perhaps most importantly, vendor agreements can provide a remedy against a vendor that causes a loss for the business.

Certain laws may hold a business liable for a data breach occurring at a vendor. As a result, businesses should also perform due diligence on vendors before engaging them for services to ensure that their practices are sound, which can protect consumers and the business itself.

Policies and Procedures

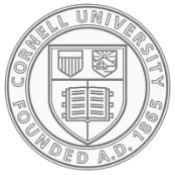
Businesses may want to implement data privacy policies and procedures now, whether because it is sound business practice or because it is required by law. Businesses should consider that future data privacy laws may be imminent, and action now can result in savings later. If operating a website, any links to policies and agreements should be conspicuous[51] and not obscured from view[52]. Consumers should have a reasonable opportunity to review policies and agreements for them to have effect.[53] Best practices also include obtaining manifested assent from consumers by requiring active acceptance of terms.[54]

[50] Bortstein Legal Group, "Navigating Regulatory Challenges in Cloud Infrastructure Services Agreements", *Securities Industry & Financial Markets Association*, October 2020 https://www.sifma.org/wp-content/uploads/2020/10/SIFMA-Cloud-White-Paper-BLG-October-23-2020.pdf
[51] *Specht v. Netscape Communs. Corp.*, 306 F.3d 17 (2d Cir. 2002)
[52] *Meyer v. Uber Technologies Inc.*, 868 F.3d 66 (2d Cir. 2017)
[53] *Feldman v. Google*, Inc., 513 F.Supp.2d 229 (E.D.Pa. 2007)
[54] *Id.* at 10

CCPA doesn't have a fully developed body of enforcement yet, so it is hard to gauge where the real regulatory or legal risks may lie. **As a result, given the uncertainty of enforcement and litigation, extra-territoriality, and the momentum of privacy laws, it may be best to err on the side of privacy and transparency when in doubt**. Policies and procedures should be accurate to avoid regulatory or reputational risk; do what you say and say what you do.

CONCLUSION

Privacy laws are gaining momentum and getting more burdensome. While there is no general federal privacy law at this time, many proposals are being considered. The key debate for a federal law will be whether it pre-empts state laws or simply appends them. State law is also proliferating, with California leading the way, followed by recent developments in Virginia and other states in various stages of proposals. If a business is in scope, risks include monetary fines, regulatory censure, criminal penalties, civil litigation, and reputational risk. It's somewhat early to understand how regulators may enforce existing laws – or even how civil litigation may pan out, though California has some developed case law. Impacted businesses should mitigate risk with best practices – not just to comply with existing laws, but to reflect sound business practice and also prepare for future applicable laws, which can save resources. Given the uncertain landscape, it may be wisest to err on the side of privacy and transparency when in doubt.



Frank C. Barile
Cornell Tech
New York, NY 10014
(347) 920-1637
fcb39@cornell.edu