

## LEGAL UPDATES

# Our Privacy and Security 2021 To-Do (and Not-To-Do) List Lessons Learned From a Year Like No Other

With each new year comes a host of bright new intentions. And, as each of us knows all too well, some stick and others will quickly be forgotten. Our 2021 To-Do (and Not-To-Do) list will serve as a reminder to stay the course when it comes to data privacy and security.

01/04/2021 | 5 minute read

by Céline Guillou & [Chiara Portner](#)

Happy new year from the Data Privacy & Security team at Hopkins & Carley!

With each new year comes a host of bright new intentions. And, as each of us knows all too well, some stick and others will quickly be forgotten. Our 2021 To-Do (and Not-To-Do) list will serve as a reminder to stay the course when it comes to data privacy and security.

Rather than focus on privacy and security predictions for 2021, we want to share a list of action items based on some of the hard-learned lessons from 2020, as well as trends that we expect to continue into 2021. 2020 was a very busy and tumultuous year in the privacy and security world, and this will certainly also be the case in 2021. Companies that handle personal information must juggle an increasing number of laws, regulations, business-mandated requirements and risks. With that in mind, here are a few things to keep in mind as we enter 2021:

- **Update your privacy policies.** If your company is subject to CCPA, companies must update their privacy notices yearly. CCPA aside, because a privacy policy must always be accurate and because business operations and practices evolve quickly, it is generally a best practice to review it at least annually.
- **Do not overstate (or overpromise) privacy practices in your consumer-facing notices, and make sure that the language is clear and accurate.** Regulators, and in particular the FTC, “love” to look at the disclosures that companies make to consumers. As a reminder, at a high level, Section 5(a) of the FTC Act empowers the FTC to enforce against “unfair or deceptive acts or practices” affecting commerce. Over the past two decades, the FTC has used this authority extensively to hold businesses to fair and transparent privacy and security standards, and has interpreted this to take jurisdiction for companies to provide accurate privacy notices – with high monetary fines. Being transparent and accurate while not overpromising is very important. As most regulators like to say, you must say what you do and do what you say. Over the course of this past year, we have fixed many privacy notices that contained inconsistent language, or misrepresented companies’

## Related People

### Chiara Portner, CIPP/US

Partner

Redwood Shores

650.804.7672

[chiara.portner@lathropgpm.com](mailto:chiara.portner@lathropgpm.com)

## Related Services

[Corporate & Business](#)

[Data Privacy &](#)

[Cybersecurity Compliance](#)

actual privacy practices. The most common misstep that we saw in 2020: companies including a California “Shine the Light” disclosure while also claiming in their consumer-facing notices that they do not “sell” personal information under CCPA. This obviously conflicting language is a big red flag for a regulator.

- **Do not cut and paste from or copy other companies’ policies.** Every company’s practices and obligations are different, whether it be as to the types of data collected, how the data is used and/or disclosed, and applicable laws. Likewise, beware of free privacy policy generators, or, at the very least, have a privacy professional review the final policy. We consistently see language in software-generated policies that simply does not align with companies’ actual practices or the laws that apply to them. Taking the CCPA as an example, determining whether a covered business “sells” information (and needs a “Do Not Sell My Personal Information” link) often requires a pointed analysis that these policy generators are not designed to undertake.
- **If you have a mobile app on iOS, do make sure that your “privacy nutrition” disclosures align with what your privacy notice states.** The iOS disclosures are typically filled out by developer teams, while privacy notices are generally created by legal or compliance teams, which can lead to inconsistencies. Teams should work together to ensure that the company’s practices, its iOS disclosures and its privacy notice(s) are consistent with one another.
- **Do not skip training your employees on security and privacy. Education is key.** With respect to privacy-specific laws, some, like the CCPA, specifically mandate employee training for consumer rights, but CCPA or not, it’s a best practice to make sure that employees understand individual rights. Insofar as security is concerned, training employees is critical, although many companies unfortunately tend to let this slide. We have seen multiple breaches – in some cases of information that is considered sensitive – because an untrained employee fell victim to a phishing scam or other malicious scheme. Having various policies in place is a first step, but this is simply not enough: internal policies must be circulated and enforced, and employees should be kept abreast of and periodically trained on evolving threats and changes in data protection requirements. In addition, pay attention to third-party vendors and their own security practices, including whether and how they train their own employees.
- **Do make security a priority.** This is a much bigger topic, and you can expect more on this from us in 2021. To share just one example (among so many) of what not to do, a proposed consumer class action has been filed against Petco (and its subsidiary PupBox) in California state court. The complaint alleges that over a period of nearly six months, an “unauthorized plugin” on the PupBox website captured and disclosed personal and credit card information of approximately 30,000 consumers. According to the complaint, the defendants acted in a reckless manner by failing to take reasonable steps to safeguard the data. Allegations in the complaint include the defendants’ failure to encrypt payment card data (PCD) at the point of sale, defendants’ improper or untimely installation of updates, patches, and malware protection, and the lack of internal access controls. The lawsuit also claims that because the defendants failed to properly monitor the website and information systems, the breach went undetected for quite some time. To top it all off, the defendants delayed providing notice of the data breach: despite becoming aware of it in August 2020; they only notified customers in early October 2020. While all of these missteps and fails may seem egregious, they happen all the time because companies are not paying attention to security (or their vendors’ security) as they should be. As a reminder, it is critical to safeguard sensitive data, including payment information.
- **Do destroy personal information that is no longer necessary (other than that which they are legally required to retain).** Companies should implement a data retention policy that balances their different legal obligations to retain data with the need to minimize it. Whether it is employee, consumer or customer data, know how long you are legally required to retain it and then destroy what should not or does not need to be retained. So many companies seem to hold onto data for so long and without any legal or business justification, and in doing so substantially increase the risks in the event of a data breach.
- **As we move into a world of increased reliance on biometrics, do pay attention to the Biometric Information Privacy Act (BIPA), which is a heavily litigated Illinois law that carries a private right of action (even if there is no actual harm to individuals).** BIPA has been around since 2008, but was essentially ignored until 2015, when consumers and employees filed a series of class actions for BIPA violations – including one against Facebook for face

scans. BIPA regulates fingerprints, retina scans, voiceprints and other biometric identifiers and information that identify individuals. It requires notice, consent and a specific policy for the use, disclosure and retention of biometrics, as well as strong security. Protecting biometric information is critical; if it is breached, an individual cannot simply modify it as he or she would a password, and its misuse presents much more significant risks. Texas and Washington also have specific laws geared toward biometrics, and more of these laws can be expected.

- **Do pay attention to new data protection laws and regulations being discussed and/or implemented across the U.S. and around the world.** In the U.S. (and following in California's footsteps), many states are considering more comprehensive privacy laws. The Federal government is also stepping up its efforts, and various privacy bills are being introduced and considered (whether the new Congress finally implements a Federal privacy law is another story). Outside of the U.S., companies operating globally or servicing customers in other parts of the world should monitor continued Brexit and post-Schrems II developments, and pay attention to Brazil's LGPD now in effect, as well as developments in Asia.
- **Finally, do not assume that privacy enforcement is non-existent.** In the EU, the CNIL just delivered massive fines for cookie non-compliance, and here in the US, the FTC and state AGs continue their enforcement, particularly with respect to kids. Lawsuits are also on the rise, even in the EU. Publicly, lawsuits and enforcement actions by regulators have focused on big tech, but there is plenty to go around for smaller companies, especially as we continue to see an increase in data breaches. In other words, in this ever-evolving world of data protection, it's always best to avoid the "it won't happen to me" mindset.

Please contact our experienced team to help with these and other data privacy issues.