A Tech Checkup

In order to keep up with a changing world, each company must periodically assess how technological changes impact legal its requirements and liabilities. Review the following list each year to keep up to date.

May 14, 2021

Categories:

Blogs
Private Equity Industry Blog
Technology Blog

Authors:

Daniel A. Murray

Data Privacy and Security

GDPR in Europe, CCPA in California, PIPEDA in Canada, and other data privacy laws are in effect and always changing. Even companies not operating in these jurisdictions may have customers who live there. And these laws may apply. IT and data security teams need to be up to date on applicable regulations and how companies and their vendors are in compliance. Because new laws come out every year, technology contracts from last year may already be out of date. When these contracts were negotiated, there may have been provisions in place regarding GDPR. But CCPA may not have been in force yet, or a company's operations may have expanded into Canada wherein PIPEDA rules. Revisit vendor contracts every year and make sure they mandate compliance with applicable data privacy laws. There are also laws about the reporting of security breaches if customer or employee data is exposed. Make sure all these provisions are up to date.

For companies that are not in compliance with data privacy laws, the first step toward compliance may be the pseudonymization of data. For example, GDPR in Europe does not apply to data that "does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the data subject is no longer identifiable." GDPR, and other laws, contains many complicated provisions. But a first step to avoid regulation can be starting the process to pseudonymize all customer data.

Cloud Computing

Many companies are moving functionality into the cloud. Along with great technical advantages, the cloud also brings challenges. Security protocols should be checked at least once per year. This

FBT Gibbons

includes procedures for employees to access cloud-based tools and also for third-party vendors who may be interfacing with the cloud. Security teams should review multi-factor authentication needs, whether on the employee or vendor side.

Part of reviewing cloud services includes knowing where cloud tools are located. Cloud services based in the European Union might have different legal requirements from those based in the United States. Some companies may need to mandate that cloud vendors maintain all data in the United States, for example, in order to avoid extra-territorial regulation.

When transitioning from an on-premises solution to a cloud product, carefully consider which agreements are impacted. Office software, VPN, database, software development tools – these may all be impacted. Compatibility must be confirmed between a new cloud solution and any interfacing tools. Sometimes contracts must be renegotiated.

Data Ownership

Besides protecting data, companies should consider ways to monetize their data, or take a close look at how it's already being monetized. Software vendors may be collecting and monetizing data without a company's knowledge. This data can be valuable, and companies shouldn't give it away for free. It is common to allow software vendors to only collect and use anonymized data. If a vendor is extracting further value out of the data it collects from a company, it should give compensation. Better yet, companies should innovate ways to monetize data. Even if analyzing and monetizing data isn't in a company's current business plan – it could be.

Brexit

Any company with operations in Great Britain needs to understand how Brexit impacts its business. New technology regulations may apply. Patents, copyrights, or trademarks may be affected, and new filings may be required to maintain intellectual property rights. Make sure Europe or UK-based personnel know how Brexit impacts

company operations and can react accordingly.

Contract Updates

Every few years standard agreements, such as employment or vendor agreements, should be reviewed to keep up with current law. For example, the Defend Trade Secrets Act was passed by Congress in 2016. Yet many agreements still lack the DTSA whistleblower language that allows companies to seek enhanced damages when trade secrets are stolen.

Additionally, force majeure language has come under increased scrutiny in the past year. The pandemic may have taught companies lessons about what specific force majeure language best serves their interests.

Open-Source

Open-source software is publicly available software code that can be accessed and used by developers. Open-source may seem free – but watch out. Open-source code comes with licensing requirements, some friendly and not so friendly. The worst-case scenario is when use of open-source code requires that any such software be then freely available to the public. Most open-source code does not carry such stringent licensing terms, but companies should review all open-source code used by their developers. Maintain a list of known open-source products and whether they're approved for use or not. Audit the list, and developers' uses, every year. And make sure developers know to seek approval for any open-source code they use.

One good place to review the basic terms of popular open-source licenses is ChooseaLicense.com. While this resource is good for reviewing the basics, when confronting whether to use a specific open-source license, have a lawyer review it.

Covid Issues

Many companies have begun tracking employee health data, such as daily temperature or symptoms, vaccination history, and more.

FBT Gibbons

This kind of personal health data is subject to HIPPA and should not be treated like other confidential data. Company security infrastructure may be secure from a confidentiality perspective, but still fail HIPPA standards. On site storage, cloud-based software solutions, teleworking solutions – all of these need to be considered from a HIPPA perspective if they're involved in collecting or storing employee health data.

Telecommuting

Telecommuting has grown during the pandemic. This brings up many issues related to privacy, security, and wages. The appropriate type of enterprise software may change depending on whether employees, and which employees, are using employer-provided devices or personal devices. Monitoring and security software will differ, for example. Telecommuting may implicate different legal jurisdictions as well. Are some employees located in California or Europe? If so, consider what law applies and how it changes company strategy. How companies measure hours or wages may change in the telecommuting world. Also consider approaches to work-related injuries. It may be necessary to draft new employment agreements or policies related to injuries and obtain proof of receipt of such new policies.

For additional guidance on any of the topics discussed above, contact Daniel Murray of Frost Brown Todd's Intellectual Property and Technology Industry teams.

FBT Gibbons