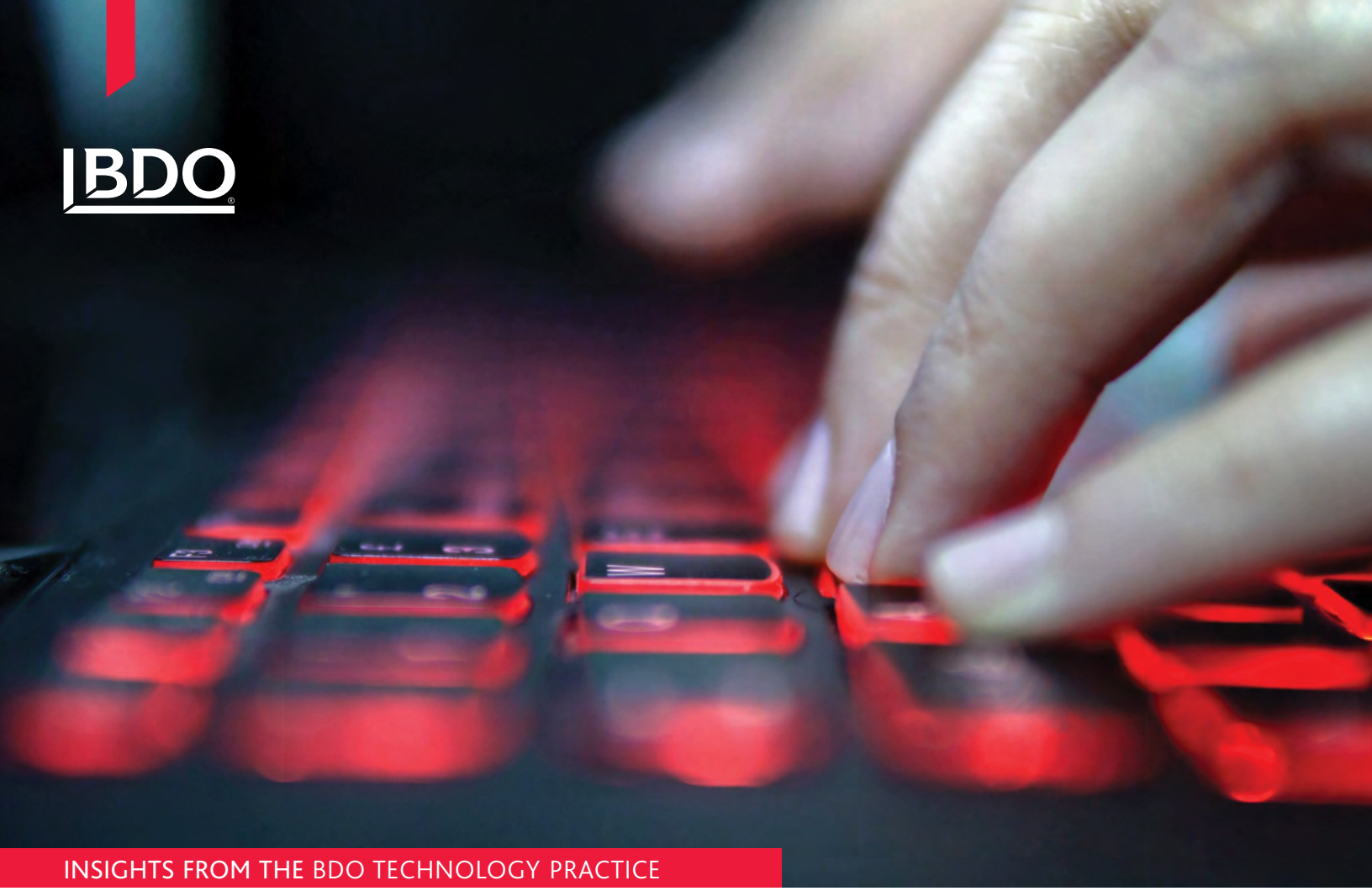

INSIGHTS FROM THE BDO TECHNOLOGY PRACTICE

WEBINAR RECAP

TECHNOLOGY COMPANIES' GUIDE TO DATA PRIVACY

By Sangeet Rajan, Managing Director, Data & Information Governance Practice at BDO and Steve Bunnell, Partner, Co-Chair Data Security & Privacy Practice at O'Melveny

Tech companies are increasingly facing reputational risk, enhanced scrutiny and legal and financial consequences for mismanaging consumer data.

A recent BDO webinar, "Tech Companies' Guide to Data Privacy," explored what technology companies can do to identify and mitigate their organization's data privacy risks. Here are a few of the key takeaways.

SETTING THE STAGE – WHY SHOULD TECH COMPANIES PRIORITIZE DATA PRIVACY NOW?

There are a myriad of reasons, most notably:

Digitalization and Personalization: Data is the lifeblood of an increasingly digital economy. Increased digitalization and personalization leveraging user data has made our world more connected and convenient. However, this can come at, literally, a significant cost. Personal data is a prime target for cybercriminals. It has real monetary value on the dark web. Banking credentials, health information, drivers licenses, credit cards, social media, social security and other personal data can be bought and sold on the dark web. The prices per record range from $10-12 dollars for credit card information to $1,000 plus for banking credentials. This makes technology companies, retailers, hospitals, health care providers, insurance companies and financial institutions prime targets—no industry is immune.

Shifting Consumer Sentiment: Recent news of high-profile data breaches and data misuse, such as U.S. election tampering, has impacted consumer attitudes towards personal data collection

and use by companies. There's been a steady and significant shift in U.S. consumer sentiment towards a more conservative data privacy policy: SAS reports that 73 percent of consumers say their concern over privacy of personal data has increased in the last few years. And they're taking action: **66 percent** of consumers have changed privacy settings, removed a social media account or declined terms of service. Consumers expect companies to do more to protect their data privacy.

Increased Regulatory Scrutiny: Regulators have taken up the cause and passed a flurry of data privacy regulations in reaction to data breaches. The General Data Protection Regulation (GDPR) and California Consumer Protection Act (CCPA) being recent examples, with many other U.S. states also considering their own version of privacy legislation.

Innovative New Uses of Data: The new data privacy laws are coming about as technology companies continue to find new and innovative uses of personal information. The proliferation of artificial intelligence and machine learning applications to collect and analyze consumer data is a double-edged sword without fully established data privacy and security controls. If this technology is used properly, it enables organizations to make more meaningful business decisions, but in the wrong hands, and if breaches go undetected, this technology becomes a weapon and can create untold operational chaos.

OF THE EXISTING CYBERSECURITY THREATS, WHICH ONES ARE TECH COMPANIES MOST VULNERABLE TO? WHY?

There is a conglomerate of destructive effects coming together to create a more challenging threat landscape than we've seen in the past. While the majority of cyberattacks previously focused on monetizing stolen data, such as through the sale of credit card numbers or commercial secrets, many data breaches today have more sinister—and far-reaching—goals.

Nation-state actors, organized crime groups or business insiders, for example, can disrupt entire organizations by holding their data for ransom until a fee is paid—commonly known as ransomware. Governments from around the world are deeply concerned about cyberattacks directed at critical infrastructure, such as electric and telecommunications grids, pipelines and national infrastructures—outages that would not only cause business interruption and monetary loss, but potentially human loss, as well. Increasingly, "deep fake," which targets the integrity of data, is becoming an all too common cyber threat. Through a deep fake threat, technology leaders base decisions on undetectably false information—creating chaos, especially for organizations where data underpins their service offerings.

FACTORS DRIVING AWARENESS OF DATA PRIVACY RISKS

Regulations

New privacy and data protection laws and regulations (with teeth) are being drafted and taking effect in the U.S., EU and across the world

Data Breaches & Hacks

Data breaches & hacks lead to adverse media attention, business disruption, customer trust erosion, goodwill and reputation loss, criminal and civil penalties and costs, complaints and lawsuits and loss of revenues

Innovation

Implementations of AI, Blockchain, Robotic Process Automation, Internet of Things, etc. are bringing about new and different uses of personal data and privacy concerns

The best way to deal with all of these damaging encounters is by strengthening your cybersecurity and data security strategy, and preparing resources in advance to mitigate the likelihood of a successful cyberattack. Tech companies who have failed to adequately prepare against data breaches may find themselves subject to legal exposure in addition to damage to their operations and reputations. On the legal front, companies are not always considered "innocent victims" of cyberattacks, opening up a path for remuneration to aggrieved parties.

HOW CAN TECH COMPANIES EFFECTIVELY PLAN TO ENSURE THEY ARE MEETING ALL REGULATORY COMPLIANCE REQUIREMENTS?

There is a myriad of state, country and global regulations when it comes to protecting consumer data. All 50 states have cybersecurity or data breach laws, with Alabama being the most recent and final state to pass regulation in June 2018.

It can certainly be challenging to identify and comply with the expectations of varying regulations spanning 50 states and the global marketplace. From different data breach notification times to varying definitions of what constitutes a "breach" and which compromised data qualifies for notification protocol, provisions can vary widely by state and by country. However, they do have one thing in common: The onus is on the company to protect consumers' data privacy through internal cybersecurity measures.

NEED TO KNOW: COMPLIANCE WITH GDPR AND THE UPCOMING CCPA

The European Union (EU)'s implementation of GDPR in May 2018 provides data privacy coverage for EU citizens and residents and applies to all organizations doing business in this region. With the ratification of this bill, the EU has demonstrated its commitment to protecting the rights and freedoms of those living within its jurisdiction, in a nutshell, declaring data privacy as a fundamental right. GDPR grants individuals the:

- Right to Know
- Right to Access
- Right to Data Portability
- Right to Rectify
- Right to Restrictions
- Right to Object to Automated Decisions
- Right to be Forgotten

The CCPA is the next major milestone that companies are focused on in terms of data privacy compliance. As noted above, all states have data privacy regulations in one form or another, though the difference with California is that it's the fifth largest economy in the world and home to a tremendous concentration of tech companies—meaning that the CCPA's implications reach far beyond its borders. While companies can continue to collect consumer data under the CCPA, they have to disclose what information they have and who it's shared with or sold to. Its definition of "personal identifiers" encapsulates a broad sense of personal information, such as commercial, electronic, behavioral, biometric, financial and educational information, amongst others.

Are you impacted by CCPA? Find out with these questions:

- Does your company collect personal identifiers?
- Does your company transfer personal information to third parties?
- Does your company collect electronic network activity data?
- Does your company determine the purposes and means of processing personal information?
- Is your company a for-profit California business meeting one of the following criteria:
  - Does your company have annual revenues greater than $25 million?
  - Does your company make 50% of its annual revenue from sales of personal information?
  - Does your company buy, sell or share personal information of more than 50,000 California residents?

One key differentiator between GDPR and CCPA is that the CCPA offers individuals the right to object to the sale of their information. Additionally, CCPA doesn't overtly speak to privacy principles. There's no requirement for a Data Protection Officer under CCPA, nor a written record of data processing. Despite its silence on these issues, the CCPA does require an ethical use of data for when consumers request the information that's been collected on them. Thus, the transparency process is set to reveal data gathering and storing practices, which implicitly necessitate a fair and lawful way of managing personal information.

In June, House Minority Leader Kevin McCarthy backed the idea of national legislation to safeguard consumers' data privacy, adding a prominent voice to the bipartisan support in Congress for tackling how technology companies amass and use their information. With the federal government gearing up to roll out a blanket privacy law, tech companies need to continue their innovative development and stay ahead of the curve by enhancing their data management policies.

WHY IS AN ENTERPRISE-WIDE INFORMATION GOVERNANCE STRATEGY SO CRITICAL TO TECH COMPANIES, AND WHERE ARE THEY IN TERMS OF DEVELOPMENT AND IMPLEMENTATION?

What is information governance? Information governance is about leveraging enterprise data as an asset while simultaneously managing it as a liability. When done right, data securely and effectively applied can have a direct impact on the company's bottom line, yield competitive advantage and foster market differentiation. Conversely, data in the wrong hands can lead to stark reputational, financial and legal consequences.

Information governance is the framework of policies, processes, technologies, accountabilities and controls that are the guardrails for managing data across its whole lifecycle; from data collection/creation, use, protection, storage, disclosure, transfer, archiving and destruction. BDO has helped technology companies set up the framework on generally accepted information governance principles below:

- **Fair, lawful and transparent processing** – Collect data ethically and lawfully with full disclosure to individuals and regulators on what information is collected and how it will be used
- **Purpose limitation** – Limit data use to only the specific purposes disclosed
- **Data minimization** – Minimize the data collection to only what is needed
- **Accuracy** – Ensure data is accurate, complete and up to date
- **Storage limitation** – Retain the data for only as long as necessary, actively destroy expired data
- **Confidentiality, integrity and availability** – Protect and secure the data from unauthorized access, tampering/corruption and service disruptions
- **Transfers/disclosures** – Establish proper controls to monitor data transfers/disclosures to third-parties and across borders
- **Accountability** – Set the tone at the top. Assign ownership and accountability to an information governance office/leader and to individual business owners

Having an information governance program anchored on the principles above will not only enforce the discipline in managing data and reducing cybersecurity threats, it will also improve the availability of quality data that tech executives can use to make more meaningful and timely operational decisions.

According to BDO's Inside E-Discovery & Beyond Survey, 93 percent of companies are either currently acting, or considering taking action in regard to developing an internal information governance council or leadership team.

WHAT ARE STEPS THAT COMPANIES SHOULD TAKE NOW TO 'FUTURE PROOF' THEIR PRIVACY PROGRAM?

"Future proofing" consumers' privacy in your organization starts with the core set of principles mentioned above. Your privacy/information governance principles should establish procedures to

identify and monitor the flow of consumer data within and outside your organization to ensure that it adheres to all relevant data privacy regulations and "best practice" frameworks such as GAPP, Privacy Shield, ISO and/or ISACA.

Bearing in mind that any cyber breach will follow a chain of liability, you should look to establish an internal structure to be prepared for the domino effect of accountability, culminating in a leadership role in a designated privacy office, such as a Chief Information Officer, who would manage data security and privacy challenges.

TAKING IT A STEP FURTHER: DATA ETHICS

Based on a series of high profile data breaches and fines related to data privacy regulation non-compliance, it shouldn't come as a surprise that there is a lot of attention by the public and government alike when it comes to how technology companies are using consumer data. The U.K. and Canadian governments have been vocal in advocating for greater transparency by technology companies and have popularized the term, "data ethics." In a nutshell, it's the expectation that tech companies will act morally when it comes to managing consumer data. Implementing a data ethics philosophy in your own organization begins with taking a measured and mindful approach to understanding the data needs of a given project and only collecting the information that is needed.

Companies also should be accountable for their user data. Prioritizing a sense of proportionality will be instrumental in identifying the necessary data that can be relevant and usable, and simultaneously engaging with the potential limitations of accessible data. Considering questions such as, "Where is this data coming from?" and, "Are there errors or biases in it?" will support credibility and enable you to gain trust as you develop your next product or service.

The time to act is now. Technology companies must take a conscientious approach to data use. Data ethics begins with first adopting a principles-based approach to information governance so that it becomes ingrained in the very DNA of the company.

WHAT ARE COMPANIES DOING TO BALANCE THE USE OF DATA TO GROW WHILE SIMULTANEOUSLY PROTECTING CONSUMERS' PRIVACY?

With so many new opportunities for data to drive revenue, tempered by increasingly tough data privacy regulations, tech companies are in a challenging position.

The data privacy strategy selected will underwrite the rights and freedoms you intend to incorporate into your practice and, ultimately, into your customer relationships. Your approach to data privacy sets the tone for your companies' privacy culture, be it data minimization or purpose limitation (only collecting data you need for the purpose initially disclosed). Going forward, your actions will demonstrate a conscious effort of your company's core principles on data use.

This "privacy by design" approach means incorporating these processes into the DNA of your company. Consequently, as you develop new products and services, a privacy assessment will come automatically in sync with production development, thus mitigating data compromise risk and reducing your liability.

CONCLUSION

A notable 87 percent of tech CFOs express high or moderate concern over data privacy, according to BDO's 2019 Technology Outlook Survey. In light of increasingly tough data privacy regulations and the regular occurrence of data breaches and cybersecurity attacks, creating a robust data privacy program is, simply put, a 'must.'

A measured and purposeful approach to data privacy and information governance will not only help reduce your risks of cyberattacks and regulation non-compliance, but also may win you some new customers, who have become much more discerning about who they share their data with and for what purpose.

For more information, visit:

WEBINAR RECORDING

INFORMATION GOVERNANCE HUB

DATA ETHICS ARTICLE

CCPA RESOURCES

People who know Technology, know BDO.

www.bdo.com/**technology**

CONTACT:

AFTAB JAMIL
Assurance Partner & Global Technology Practice Leader
408-352-1999 / ajamil@bdo.com

SANGEET RAJAN
Managing Director, Data & Information Governance
415-490-3001 / srajan@bdo.com

ABOUT THE TECHNOLOGY PRACTICE AT BDO USA, LLP

BDO has been a valued business advisor to technology companies for over 100 years. The firm works with a wide variety of technology clients, ranging from multinational Fortune 500 corporations to more entrepreneurial businesses, on myriad accounting, tax and other financial issues.

ABOUT BDO

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 650 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi national clients through a global network of more than 80,000 people working out of nearly 1,600 offices across 162 countries and territories.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.