

**Market  
Intelligence**

# PRIVACY & CYBERSECURITY 2022

Global interview panel led by WilmerHale

LEXOLOGY

**Getting the Deal Through**

**Publisher**

Edward Costelloe  
edward.costelloe@lbresearch.com

**Subscriptions**

Matthew Bridgewater  
matthew.bridgewater@lbresearch.com

**Head of business development**

Adam Sargent  
adam.sargent@gettingthedealthrough.com

**Business development manager**

Dan Brennan  
dan.brennan@gettingthedealthrough.com

**Published by**

Law Business Research Ltd  
Meridian House, 34-35 Farringdon Street  
London, EC4A 4HL, UK

Cover photo: shutterstock.com/spaintervfx

This publication is intended to provide general information on law and policy. The information and opinions it contains are not intended to provide legal advice, and should not be treated as a substitute for specific advice concerning particular situations (where appropriate, from local advisers).

No photocopying. CLA and other agency licensing systems do not apply. For an authorised copy contact Adam Sargent, tel: +44 20 3780 4104

© 2022 Law Business Research Ltd  
ISBN:978-1-83862-999-1

Printed and distributed  
by Encompass Print  
Solutions

# PRIVACY & CYBERSECURITY 2022

Global Trends.....	3
Armenia .....	9
Greece.....	21
India .....	41
Italy.....	51
Japan.....	65
Netherlands.....	81
Switzerland .....	99
Taiwan .....	115
United States .....	127



# United States

Jason Chipman is a WilmerHale partner who advises companies on complex regulatory matters associated with data security, cyber incident response, the Committee on Foreign Investment in the United States and related export controls. He has assisted companies in most sectors of the economy on data security best practices and frequently assists with corporate due diligence. Mr Chipman currently serves as a non-resident fellow at the National Security Institute.

Benjamin Powell is a WilmerHale partner who has advised companies on major cybersecurity incidents and preparedness across virtually every sector, including banking, investment management, retail, defence and intelligence. He is recognised as a leading attorney in international investment and mergers, including the Committee on Foreign Investment and the Defense Security Service.

Arianna Evers is a WilmerHale special counsel who advises clients on complex privacy, data security and consumer protection issues arising under rapidly evolving federal and state requirements. She regularly assists clients on privacy-related issues, including legal requirements and best practices in emerging and changing areas of the law, and also represents them in regulatory investigations.

Shannon Togawa Mercer is a WilmerHale senior associate who advises clients on matters related to cybersecurity, privacy, and US and European data protection. She joined WilmerHale from the London location of a large global law firm where her practice focused on transactional work, including the cybersecurity and data protection aspects of capital markets transactions and mergers and acquisitions.

## 1 | What were the key regulatory developments in your jurisdiction over the past year concerning cybersecurity standards?

There is a growing trend toward more proscriptive cybersecurity requirements in economic sectors perceived as playing a critical role in the US economy or for US security. For example, in March 2022, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 was signed into law, which requires critical infrastructure entities to report material cybersecurity incidents and ransomware payments to the Cybersecurity and Infrastructure Security Agency (CISA). Additionally, in April 2022, a final rule issued by the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System and the Federal Deposit Insurance Corporation took effect, which requires banking organisations and their bank service providers to report any significant cybersecurity incident within 36 hours of discovery. The Securities and Exchange Commission has also proposed rules that are intended to enhance disclosures about cybersecurity risk management, strategy, governance and incident reporting by public companies. These recent developments align with President Biden's Executive Order on Improving the Nation's Cybersecurity (the Cybersecurity EO), which sets out to improve cybersecurity, particularly in relation to federal government systems, and followed several high-profile cyber incidents in 2020 and 2021. Companies that do business with the United States government face increasingly strict data security requirements for how they manage, store and process sensitive government information, with mandatory reporting of data breaches and standards for safeguarding sensitive data. For example, the Cybersecurity EO includes updates to federal contracting language involving cybersecurity incident reporting, which may eventually be implemented through Federal Acquisition Regulatory Council rules. Under the Cybersecurity EO, the National Institute of Standards and Technology (NIST) also issued guidelines related to source code testing for software developers acting as government vendors.

At the same time, legislators at the state and federal level are exploring the creation of privacy rules that include mandatory data safeguarding requirements for personal information. There are five US states with comprehensive privacy laws – Colorado, California, Virginia, Utah and Connecticut – and many other states are exploring potential new laws as well; these laws generally require that entities provide reasonable administrative, technical and physical security practices to protect personal information. Congress held multiple hearings in 2021 and early 2022 to investigate a perceived need to pass a comprehensive federal data protection law. We anticipate these trends will ultimately (although perhaps not expeditiously) lead to more uniform and clear cybersecurity standards, along with



**“States are continuing to expand their definitions of covered information.”**

related privacy rules. In the meantime, federal agencies in the United States are likely to continue efforts to aggressively police cybersecurity regulatory compliance applicable to particular economic sectors and to seek to impose new requirements on companies responding to breaches.

- 2 | When do data breaches require notice to regulators or consumers, and what are the key factors that organisations must assess when deciding whether to notify regulators or consumers?

The United States does not have a uniform data breach notification law. Rather, all 50 states, as well as the District of Columbia and a number of territories, have individual data breach notification laws. At the federal level, sector-specific laws for government contractors, certain financial institutions and certain businesses handling health records also impose special breach notification rules. In general, data breaches mandate notification to regulators and consumers when specific categories of sensitive personally identifying information are compromised through a cyber intrusion, inadvertent disclosure or other loss of data. For example, in many

jurisdictions, the unauthorised acquisition of or access to data that includes name combined with a social security number, financial account number, driver's licence number, health record or passport number would likely trigger a mandatory breach notification obligation to the consumer and may also trigger notification obligations to regulators. States are continuing to expand their definitions of covered information, with username or email address in combination with a password or security questions and answers as well as biometric data becoming subject to breach notification requirements. State regulators are also increasingly investigating cyber incidents and bringing enforcement claims for perceived lapses in reasonable cybersecurity controls.

### 3 | What are the biggest issues that companies must address from a privacy perspective when they suffer a data security incident?

Data security incidents, particularly cyber intrusions, may raise many significant challenges. For companies handling substantial amounts of sensitive personal information, such incidents may trigger:

- communications challenges for companies that want to provide consumers or other customers with reassurance while also investigating the scope of a particular incident;
- reputational and financial challenges as incidents can impact brand stability, stock price, and a company's relationship with customers and other third parties that do business with it;
- remediation challenges in taking steps to further safeguard sensitive data to both stop a cyber intrusion and to help bolster existing security; and
- investigative challenges to determine the scope of the intrusion, what data was taken and whether the attacker has been removed from the company's networks.

Managing these sorts of challenges, often while also coordinating with law enforcement authorities, regulators, stakeholders and affected individuals, requires all components of a business to work together. Such incidents are not just the province of the information technology team. They are, rather, problems that require senior attention to manage and address.

### 4 | What best practices are organisations within your jurisdiction following to improve cybersecurity preparedness?

Incident response requires an immediate, coordinated effort to gather the facts through forensic analysis and to execute an incident response plan that enables the



company to address multiple work streams simultaneously in a coordinated fashion. The response generally prioritises remediation, reputational harm, communication with all the relevant constituencies (including, critically, customers) and preparing for the range of potential regulatory inquiries and litigation.

Companies can take several steps to best prepare for and improve their ability to respond to such issues, including:

- reviewing existing incident response plans, benchmarking against industry best practices on a regular basis, and proposing changes. Plans should also be reviewed after any serious incident to incorporate lessons learned from the company's response to that incident;
- developing and participating in tabletop exercises to help those with implementation responsibilities understand how the incident response plan would work in practice;
- engaging third-party firms in advance, through counsel, to ensure that the right resources are available to address critical issues in a time-sensitive manner and under attorney–client privilege;
- conducting regular risk assessments of a company's information technology infrastructure, systems and controls to identify and mitigate risk to the extent that risk does not align with the entity's business goals;
- providing regular updates on, and analysis of, legal and regulatory developments that would influence response plans and practices; and
- training employees, not just those involved in information security, to recognise potential security risks.

## 5 | Are there special data security and privacy concerns that businesses should consider when thinking about moving data to a cloud hosting environment?

Cloud services trigger a variety of risks that should be carefully balanced as part of the decision to outsource data storage or other information technology functionality. Although cloud computing is somewhat new for many organisations, the risks associated with cloud computing are similar to other types of IT outsourcing. Those risks include the following:

- third-party access to data. When company information is outsourced for storage or other processing by third parties, that information may no longer be solely within the control of the information owner. The cloud provider may be compelled to release it to third parties in litigation or to government agencies inside or outside the United States. Moreover, absent appropriate prohibitions in the parties' agreement, a cloud provider may be entitled to share customer data



(or data derived from customer data) with third parties for the cloud provider's own business purposes;

- data security. Evaluating the security of data in a cloud environment and ensuring the use of appropriate safeguards can be very challenging. Many cloud providers will not provide full visibility into their own network security posture;
- location of data. Data entrusted to a third party may be stored or otherwise processed in a jurisdiction that gives rise to unique legal or regulatory concerns. Moreover, some cloud providers do not provide transparency or assurances concerning where the data will be located;
- privacy and consumer notice. Processing of consumer data by a third-party cloud provider may necessitate special notices to consumers or employees and it may trigger a number of privacy and data protection obligations with respect to how their data will be handled, retained and distributed; and
- business continuity or provider lock-in. Cloud providers and sub-processors may go out of business or otherwise experience a disaster or other incident that results in the loss, corruption or temporary inaccessibility of their customers' data. Further, it may be difficult to extricate data from a software as a service

**“Legislators at the state and federal level are exploring the creation of privacy rules that include mandatory data safeguarding requirements for personal information.”**

solution at the end of the parties' engagement, at least in a format that does not require substantial processing before the data can be ingested into a competitor's software as a service product.

There are a wide range of different regulatory regimes that impact cloud outsourcing. Some regulations that are agnostic about whether data is outsourced in a cloud environment or remains within a company's firewall, impose general obligations that have the effect of imposing rules that data owners must satisfy in a cloud scenario (such as National Institute of Standards and Technology requirements to track and specially secure sensitive data). Other regulations are cloud-specific, such as ISO 27017, an independent security standard that provides guidance on the information security aspects of cloud computing and is often used by organisations to judge their ability to manage data in a cloud environment. Certain sectors, particularly the financial services and government contracting sectors, are subject to more stringent requirements on their use of cloud services to host consumer or government data.

## 6 | How is the government in your jurisdiction addressing serious cybersecurity threats and criminal activity?

Cybersecurity remains a substantial focus of federal and state law enforcement efforts in the United States and is an area of particular concern as destructive ransomware events become more common and more substantial. The Federal Bureau of Investigation has grown its cyber capabilities substantially over the past several years, and President Biden's administration is increasingly focused on efforts to combat ransomware groups.

Specific laws that address criminal activity in the cyber context include the Computer Fraud and Abuse Act, which outlaws intrusions into or interference with the security of a government computer network or other computers connected to the internet. In addition, several federal surveillance laws prohibit unauthorised eavesdropping on electronic communications, which can limit a variety of cybersecurity activities. For example, the Electronic Communications and Privacy Act prohibits unauthorised electronic eavesdropping. The Wiretap Act prevents the intentional interception, use or disclosure of wire, oral or electronic communication, unless an exception applies. The Stored Communications Act precludes intentionally accessing without authorisation a facility through which an electronic communication service is provided and thereby obtaining, altering or preventing authorised access to a wire or electronic communication while it is in electronic storage.

7 | When companies contemplate M&A deals, how should they factor risks arising from privacy and data security issues into their decisions?

Cybersecurity and privacy is increasingly a significant topic for M&A due diligence because of potential regulatory or litigation exposure that a company may take on through an acquisition. Acquirers often seek special assistance to evaluate the scope of exposure by examining the nature of the target business, the type of data it collects, maintains and shares about customers or third parties and the regulatory environment in which it operates. Acquirers may also evaluate the types of controls the company has in place to protect its systems, limit data sharing to permissible means and otherwise ensure compliance with regulatory requirements. After the transaction is complete, acquirers need to pay close attention to ensure that the target company is either fully integrated or that the target's privacy and data security practices are brought into line with the acquirer's risk tolerance.

**Jason Chipman**

[jason.chipman@wilmerhale.com](mailto:jason.chipman@wilmerhale.com)

**Benjamin Powell**

[benjamin.powell@wilmerhale.com](mailto:benjamin.powell@wilmerhale.com)

**Arianna Evers**

[arianna.evers@wilmerhale.com](mailto:arianna.evers@wilmerhale.com)

**Shannon Togawa Mercer**

[shannon.mercer@wilmerhale.com](mailto:shannon.mercer@wilmerhale.com)

**Wilmerhale**

Washington, DC

[www.wilmerhale.com](http://www.wilmerhale.com)

# The Inside Track

When choosing a lawyer to help with cybersecurity, what are the key attributes clients should look for?

Legal advice around cybersecurity issues requires counsel that is experienced at addressing and managing the wide range of issues that cybersecurity incidents and related preparation activities may trigger.

What issues in your jurisdiction make advising on cybersecurity and privacy complex or interesting?

Cybersecurity is an evolving and changing field that requires lawyers to provide a mix of legal, policy and business guidance to clients navigating new and often challenging issues. An increasingly large number of federal and state regulatory agencies, categories of litigation plaintiffs and business partners are interested in understanding how companies are protecting their data, resulting in an increasingly complex web of risks.

How is the privacy landscape changing in your jurisdiction?

Privacy is becoming a critical part of contracting arrangements between parties, with greater focus on compliance with state, national and international laws. Greater regulation of the handling, securing and transfer of data is resulting in an increasing focus by companies on privacy issues, particularly on specifying the obligations that must be met in the handling of data between parties. The California Consumer Privacy Act of 2018 went into effect in 2020, and new laws in California, Utah, Connecticut, Virginia and Colorado will go in to effect in the near term.

What types of cybersecurity incidents should companies be particularly aware of in your jurisdiction?

Understanding about cyberthreats is generally increasing in the United States. High-profile incidents involving espionage and criminal actors receive frequent public attention. But companies need to be constantly on guard for the latest threats. In the recent past, incidents involving tax fraud were on the rise and today ransom and extortion demands associated with cyber intrusions are becoming more common.

Lexology GTDT Market Intelligence provides a unique perspective on evolving legal and regulatory landscapes.

Led by WilmerHale, this Privacy & Cybersecurity volume features discussion and analysis of emerging trends and hot topics within key jurisdictions worldwide.

Market Intelligence offers readers a highly accessible take on the crucial issues of the day and an opportunity to discover more about the people behind the most significant cases and deals:

**Regulatory trends**  
**Cloud hosting**  
**M&A risks**  
**Selecting counsel**