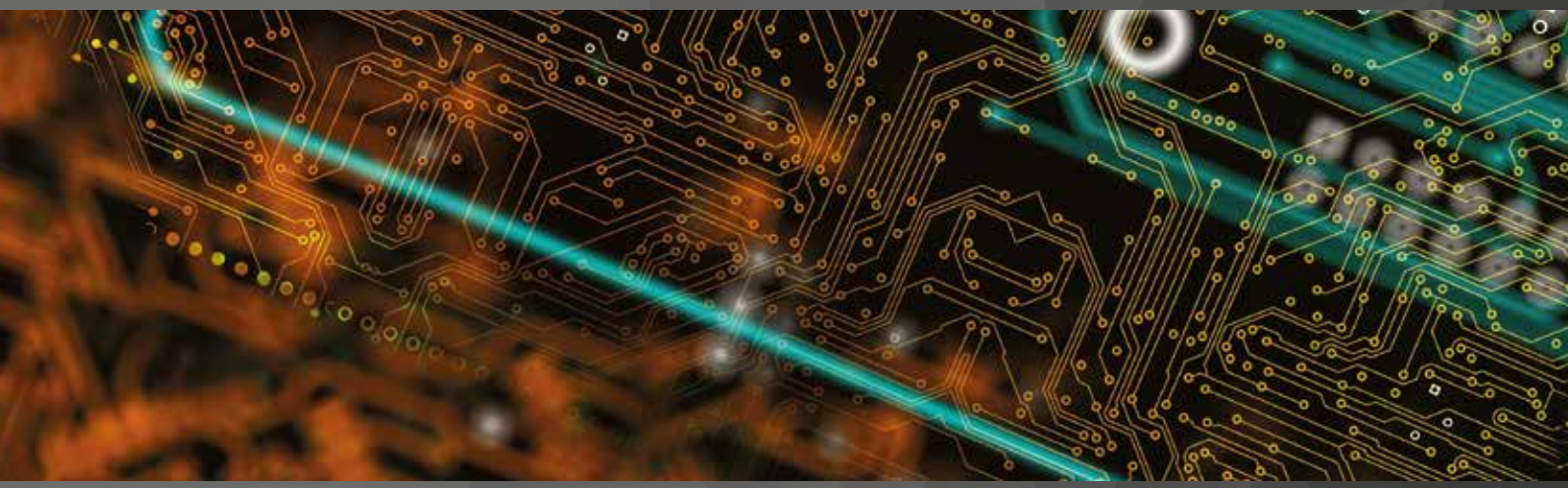
International Comparative Legal Guides



Cybersecurity 2021

A practical cross-border insight into cybersecurity law

Fourth Edition

Featuring contributions from:

Alburhan
Allen & Overy LLP
Ankura Consulting Group
Creel, García-Cuéllar, Aiza y Enríquez
Drew & Napier LLC
Eversheds Sutherland (Germany) LLP
Hamdan AlShamsi Lawyers & Legal Consultants
Ince
Iwata Godo
Kellerhals Carrard
King & Wood Mallesons
Kluge Advokatfirma AS
Lee & Ko
Lee and Li, Attorneys-at-Law
Leśniewski Borkiewicz & Partners (LB&P)
Maples Group
McMillan LLP
Mori Hamada & Matsumoto
Nikolinakos & Partners Law Firm
Nyman Gibson Miralis
Pearl Cohen Zedek Latzer Baratz
R&T Asia (Thailand) Limited
Ropes & Gray LLP
Rothwell Figg
Rubino Avvocati
Schönherr Rechtsanwälte GmbH
Simion & Baciu
Sirius Legal
Stehlin & Associés
TIME DANOWSKY Advokatbyrå AB

ICLG.com

Expert Chapters

Q&A Chapters

Phantom Responsibility: How Data Security and Privacy Lapses Lead to Personal Liability for Officers and Directors

Rothwell Figg

Christopher Ott

Boards of directors ignore data security and privacy risks to companies at the peril of their companies and – increasingly – their own personal liability. A business has its operations halted by ransomware approximately every 10 seconds. Billions of records are exposed every fiscal quarter. The global costs of these breaches and online crime reaches the trillions every year. These potential costs have elevated data security and privacy issues from mere "IT issues", or compliance *minutiae*, to the centrepiece of strategic risk management. The law has grown to match this reality. As a result, boards face expanding personal legal liability for the company's data security and privacy failures.

This upwards liability trend is not new. As early as 2014, the National Association of Corporate Directors' (NACD) *Handbook on Cyber-Risk Oversight* provided core cybersecurity principles to members of public companies, private companies, and nonprofit organisations of all sizes and in every industry sector. The NACD directed board members to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an issue for the IT team. As an established enterprise-wide risk, cybersecurity therefore began triggering boards' existing legal obligations. In the same year as the NACD handbook's admonition, 2014, SEC (Securities and Exchange Commission) Commissioner Luis Aquilar stated that "boards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility do so at their own peril".

Those perils are changing in real time just as cybersecurity and privacy threats are changing. However, we can identify certain concrete areas of established liability and strategically identify the emergent risks. Right now, the main liability risks to boards include:

- SEC liability for cyber risks;
- SEC liability for privacy risks;
- officer and directors' civil liability for breached fiduciary duties;
- direct liability for violation of state data security and privacy statutes, with special emphasis on California;
- criminal liability for cybersecurity and privacy failures; and
- global civil and regulatory liability, with special focus on the New York Department of Financial Services (NYDFS) and European Union (EU) regulations.

In the following pages, we attempt to explore all of these current trends. To end, we will also tackle a few harder-to-classify risks related to United States national security oversight of cyber readiness.

United States: Officer and Directors' Personal Liability for Cybersecurity and Privacy Failures

On February 21, 2018, the SEC "voted unanimously to approve a statement and interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents".[1] The SEC did not wait long for the public to absorb this guidance. On April 24, 2018, the SEC "announced that the entity formerly known as Yahoo! Inc. has agreed to pay a $35 million penalty to settle charges that it misled investors by failing to disclose one of the world's largest data breaches in which hackers stole personal data relating to hundreds of millions of user accounts".[2] In the space of two months, the SEC went from "[c]ompanies also may have disclosure obligations" for breaches, to paying $35 million for failure to disclose.[3] When the expectations change so quickly, it is important for officers and directors to understand both the current and developing state of cyber and privacy risks, especially when it comes to personal liability.

SEC liability

The SEC maintains broad (and expanding) authority over directors. This authority begins the moment that a director is named. SEC proxy disclosure rules, among other requirements, mandate that companies disclose, for each director and nominee, the specific experience, qualifications, attributes, or skills that led to the conclusion that the individual should serve as a director of the company in light of its business and structure.[4] This disclosure must be made on an individual basis, and be specifically linked to the biographical description of each director and nominee. These new disclosure requirements theoretically expose directors to greater potential liability if they are identified in an SEC filing as having a particularly valuable skill or expertise that is valued and relied upon by the company.

The pitfalls of director "cyber hype"

Directors and their companies often tout directors' particular skills that they bring to the board. It makes sense, therefore, that a director may tout their particular cybersecurity *bona fides*. However, overselling one's cyber skills can bring individual

liability. In 2003, the SEC amended the proxy disclosure rules to require that a company disclose whether it has at least one "audit committee financial expert" on its audit committee.[5] Prior rules indicated that identifying a director as an expert did not increase their liability for registration statements pursuant to Section 11 of the Securities Act of 1933 (Securities Act), dealing with liability in connection with registration statements. The safe harbor covered more than merely directors' financial expertise. However, the entire safe harbor language was removed in the wake of the Sarbanes-Oxley Act. Therefore, real individual liability risks flow from whenever a board member touts their expertise in any field, including cybersecurity and privacy.

Section 11 of the Securities Act imposes civil liability on directors of an issuer if "any part of the registration statement, when such part became effective, contained an untrue statement of a material fact or omitted to state a material fact required to be stated therein or necessary to make the statements therein not misleading". Therefore, directors face a real dilemma in that they feel that they should tout their material skills to current and potential shareholders, but responsibility and liability flow from those representations. Fortunately, there are many defences available to directors that turn on their level of knowledge.[6] These same defences could be utilised to defend against a Section 11 claim levelled against a director.

Board cybersecurity and privacy risk oversight

Item 407(h) of Regulation S-K and Item 7 of Schedule 14A require a company to disclose the extent of its board of directors' role in the risk oversight of the company, such as how the board administers its oversight function and the effect this has on the board's leadership structure.[7] The Commission has previously said that "disclosure about the board's involvement in the oversight of the risk management process should provide important information to investors about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company".[8] The SEC has expressly stated that cybersecurity risks are among those that must be reported to directors, with all of the criminal and civil liability that may flow from that notice.[9]

Cybersecurity risks and scrutiny of board trading activities

Directors also will face scrutiny for their trades after they are advised of cybersecurity risks. In the wrong situation, a trade could be considered to be an insider trade on non-public information. There is a delicate balance that must be reached here. After all, directors should righteously be informed of significant risks, such as cybersecurity or accounting matters. However, directors must internalise that their cybersecurity briefings can be every bit as material as their regular briefings on accounting controls or other vintage risks. Currently, however, director understanding may be lagging behind their responsibilities.

In the recent massive Equifax breach, multiple insiders have been charged for trading on the breach information.[10] The SEC has indicated that it will make this type of trading a particular focus.[11] For this reason, the SEC advises that "[c]ompanies should assess whether they have sufficient disclosure controls and procedures in place to ensure that relevant information about cybersecurity risks and incidents is processed and reported to the appropriate personnel, including up the corporate ladder, to enable senior management to make disclosure decisions and certifications and to facilitate policies and procedures designed to prohibit directors, officers, and other corporate insiders from trading on the basis of material non-public information about cybersecurity risks and incidents".[12] That may be easier said than done.

As a practical matter, companies can start to protect their officers and directors from this type of scrutiny (and prevent the underlying suspect behaviour) by establishing policies and procedures in place that: (1) expressly address trading blackouts or similar procedures that will prevent directors, officers, and other corporate insiders from trading during the heightened period between the company's discovery of a cybersecurity incident and public disclosure of the incident to trade on material non-public information about the incident; (2) provide regular training to all insiders about cybersecurity risks that must be treated like any other material enterprise risks; and (3) ensure that the company makes quick and timely disclosure of any material non-public cybersecurity information.

Officer and director fiduciary duty law and personal civil liability

Officers and directors can face civil liability if they breach their fiduciary duties, which can lead to a shareholder derivative action wherein the shareholders sue the officers and directors for breaches that harmed the company. Technically, every state has its own standards regarding the fiduciary duties that officers and directors owe to companies and, by extension, the shareholders. Because so many companies are incorporated there, Delaware generally leads the way of fiduciary duty issues. Under Delaware law, directors owe fiduciary duties of care and loyalty to the company.[13] This fiduciary duty of care requires directors to act with a degree of care that ordinary careful and prudent men would use in similar circumstances.[14] Under this standard, directors must act on an informed basis, in good faith, and in the honest belief that the action was in the best interests of the company.[15] Courts have interpreted this duty of loyalty further to include a duty of oversight, which will be breached if directors "utterly fail" to implement any reporting or information systems or controls or if, after implementing these systems, directors fail to monitor or oversee the operation of these plans.[16] Therefore, Delaware law clearly establishes that officers and directors must set up informational and reporting systems and monitor the results of those systems.

It does not take much imagination to see how these standards could be applied to the new information technology and cybersecurity systems that boards oversee in various companies. A number of derivative actions have been filed following high-profile data breaches. These actions are typically based on claims that, by failing to implement adequate information security policies, the directors allowed a breach to occur which damaged shareholders through decreased stock prices. Although claimants in these cases face a high pleading standard, which we will discuss below, the cases remain expensive and disruptive. Indeed, they can often to lead to resignations by officers and directors.

Civil liability for false and misleading public cybersecurity statements

Companies' public cybersecurity statements or even certain kinds of silence can also create officer and director liability. Exchange Act Section 10(b) and Rule 10b-5 prohibit, *inter alia*, making untrue or misleading statements of material fact. These laws further prohibit selective silence about these material facts. Therefore, omitting material facts must not be left unstated if

they are necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading. This last requirement is a mouthful. However, in more accessible language: one has to tell the truth about anything that is important to the company, and one must volunteer facts wherever silence on those facts will actually mislead someone. These requirements to be truthful and forthcoming with the public could conceivably create significant officer and director cyber liability in civil class actions. However, this type of liability will not attach merely when someone wishes to second-guess the content and omissions of companies' cybersecurity statements. As with many liability issues, the quantum of one's knowledge matters.

Unlike Section 11 of the Securities Act, which we discussed earlier when it comes to exaggerating directors' cybersecurity skills, Section 10(b) requires the intent to deceive, manipulate, or defraud, otherwise known as "*scienter*". Without proof that the director acted with corrupt *scienter*, there can be no Section 10(b) liability. This proof of *scienter* will be absent for many, although not all, officers and directors.

Expert experience and director liability

Experience and context matter when it comes to *scienter*. Directors with particular technical or cybersecurity expertise may have difficulty getting Rule 10b-5 claims dismissed because it may be easier for plaintiffs to plead *scienter* as to them. The *In re U.S. Bioscience Securities Litigation*[17] involved a class action by purchasers of a company's stock against the directors. The judge denied a motion to dismiss Section 10(b) claims against certain outside directors of the company for alleged misstatements, contained in the annual Form 10-K, suggesting that one of the company's products was more effective and further along in clinical trials than was warranted by the facts. In rejecting the motion, the judge explained that "[o]utside directors can be of two very different kinds", those whose role is not intended to be hands on and those who have valuable expertise in the industry.[18] In the latter case, the directors' "valuable expertise in [the company's] industry" made it reasonable to assume that the directors had inside director knowledge for which they could be held liable.[19]

Similarly, in *Tischler v. Baltimore Bancorp*,[20] a class action brought by purchasers of Baltimore Bancorp stock, the plaintiff alleged, in relevant part, that the outside directors were liable under Section 10(b) of the Exchange Act and Rule 10b-5 for a purportedly false press release about the adequacy of an offer for the company. In evaluating the defendants' motion to dismiss, the Court dove into the different types of directors and their level of regular briefings. For this reason, the audit committee members substantively briefed about the purchase offer had liability. The judge did not stop there, however. Where the outside directors had special knowledge of the company's field, the judge concluded that they knew, or should have known, of the risks to the company.[21]

Second-guessing board decision-making

As mentioned above, some of these risks flow directly from the content of public disclosures, but others come from evaluating the objective quality – in light of the attendant circumstances – of officer and director decisions. Officers and directors have a duty of care to the corporation. "Duty of care" refers to a fiduciary responsibility held by company directors to live up to a certain baseline standard of care. This ethical and legal duty requires officers and directors to render their decisions in good faith and in a reasonably prudent manner. That second clause, "reasonably prudent manner", provides the legal ammunition to second-guess failed decisions. Shareholders can probe the reasonableness of officer and director decision-making by bringing shareholder derivative actions. These derivative actions argue that officers and directors violated their duty of care when it comes to one or more decisions and therefore injured the company itself. The areas of decision-making failures have run the gamut, from poor business decisions, to accounting fraud, bribery, rampant officer looting, and – increasingly – to failures to provide adequate cybersecurity safeguards.

The Delaware Chancery Court held in *In re Caremark International Inc. Derivative Litigation*[22] (*Caremark*) that the board has an obligation to at least attempt in good faith to invest in or implement a monitoring system that is sufficient to identify legal breaches by the corporation. In *Caremark*, shareholders brought derivative suits against the company, alleging that Caremark's directors breached their duty of care by failing to adequately oversee the conduct of Caremark's employees regarding kickback payments to doctors for Medicare or Medicaid referrals, which is a crime, thereby exposing the company to significant civil and criminal penalties. *Caremark*'s holding outlined director liability for a breach of the duty to exercise appropriate care in two distinct contexts: (1) "from a board decision that results in a loss because that decision was ill advised or 'negligent'"; or (2) "from an unconsidered failure of the board to act in circumstances in which due attention would, arguably, have prevented the loss."[23] The *Caremark* Court further held that: "it is important that the board exercise a good faith judgment that the corporation's information and reporting system is in concept and design adequate to assure the board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations, so that it may satisfy its responsibility." While all of these individual parts of the *Caremark* decision are important, the board must have failed to provide reasonable oversight in a "sustained and systematic fashion", or the information reporting system must be an "utter failure".

Cybersecurity crises of all stripes, including (but not limited to) ransomware response, have now become a staple of derivative lawsuits. Indeed, these claims have become so prevalent that we now have formal court opinions holding that derivative actions against boards for ransomware failures constitute the types of central case that must be covered by director and officer liability insurance.

This does not mean that these cases are always successful. For example, in *Corporate Risk Holdings LLC v. Rowlands*,[24] the court concluded that the case solely "amounts to an allegation that the Board knew about the risk posed by a cyberattack, but did not adequately monitor [the company]'s cybersecurity efforts".[25] Where plaintiffs "focus on a specific, industry-wide risk [the allegations are] . . . not sufficient to support a *Caremark* claim".[26] For example, directors of banks who failed to recognise the risks associated with the subprime lending market could not be found, merely by ignoring the publicised risks, to have acted in bad faith.[27]

Still, there must be a reporting system so that the board can exercise oversight, and companies often have weak reporting systems. Recently, the *Marchand v. Barnhill, et al.* (*Marchand*)[28] case concerned a listeria outbreak involving Blue Bell ice cream that made many consumers ill and resulted in a total product recall. The *Marchand* court held that the board failed to provide adequate oversight of a key risk area and thus breached its duties. Consistent with *Caremark*: (a) the directors must have utterly failed to implement any reporting or information system or controls; or (b) having implemented appropriate compliance controls, the directors consciously failed to monitor or oversee the operation of that system. In *Marchand*, the court found a lack of board oversight because the Blue Bell board failed to implement any system

for Blue Bell's food safety performance or compliance. It does not take much imagination for this same analysis to apply in the cybersecurity context, especially if the company's products are particularly vulnerable to cyberattack. After all, a reasonableness standard will always move and change over time, and accounting fraud oversight was not the responsibility of the board a generation ago. Now, account committees and special risk committees roam the corporate boardrooms in giant herds. The goal of a company is not to hope that things stay the same. Rather, a dynamic, forward-thinking company tries to anticipate the next risk before their directors face personal liability.

However, for now, directors can and should allege that all such allegations of the breach of cyber duty of care constitute "a classic example of the difference between allegations of a breach of the duty of care (involving gross negligence) as opposed to the duty of loyalty (involving allegations of bad-faith conscious disregard of fiduciary duties)".[29] These standards are even more daunting for plaintiffs when "the claims involve a failure to monitor business risk, as opposed to legal risk".[30]

Special director knowledge, Delaware law, and the Section 141(e) "safe harbor"

Delaware case law paints a slightly different outlook as to whether independent directors will be held to a higher fiduciary duty standard because of their special expertise. The *In re Citigroup Inc. Shareholder Derivative Litigation*[31] involved the fact that that audit committee financial experts on the board violated their fiduciary duties by allowing the company to engage in subprime lending. The Delaware Chancery Court stated that "[d]irectors with special expertise are not held to a higher standard of care in the oversight context simply because of their status as an expert".[32] Rather than a failure of management oversight, the Court viewed the operative issue as a failure to recognise a business risk, emphasising that "[e]ven directors who are experts are shielded from judicial second guessing of their business decisions".[33]

A similar "business decision" deference did not apply to the court's decision regarding *In re Emerging Communications, Inc. Shareholders Litigation*,[34] wherein a director with financial expertise was held to have a duty to voice concerns about the fairness of a proposed transaction's price. The meaning of this case has been widely debated. One interpretation is that, although directors possessing special expertise might not be held to a higher standard under Delaware fiduciary duty law, they may lose the safe harbor protection afforded by Section 141(e) of the Delaware General Corporation Law.

Section 141(e) provides that a director's good faith reliance upon "such information, opinions, reports or statements presented to the corporation . . . as to matters the member reasonably believes are within such other person's professional or expert competence and who has been selected with reasonable care. . . " will be afforded legal and factual deference. However, if a director has a particular expertise, then they may be unable to rely in good faith on an expert's report (or omission). As companies' SEC proxy disclosures expand upon directors' particular qualifications and expertise, they also effectively limit the scope of Section 141(e) deference. Where a director's cyber *bona fides* are trumpeted, even under Delaware law, they will enjoy less "business decision" deference in matters involving cybersecurity.

There is currently a tension developing between these director disclosures, which grow ever more elaborate and more prominent, and the protections of the "business decision" deference. If nothing else, civil plaintiffs may endeavour to weaponise a director's publicly touted expertise to argue that the same director either violated the federal securities laws or their fiduciary duties. While all such claims require proof (in this specific context) of the director's knowledge about specific cybersecurity risks, a company's own admissions about a director's cybersecurity knowledge and expertise make the cases easier to allege and prove. Drafting these director cybersecurity disclosures has, therefore, become a high-stakes balancing act: companies must provide truthful and informative disclosures while also taking care to keep those disclosures lean enough to not create greater litigation risks.

The changes in legal risks appear in *National Ink and Stitch, LLC v. State Auto Property and Casualty Insurance Company*,[35] in which a federal court held that a ransomware attack was covered by standard business loss language in a contract. In other words, the risks of a cyber event are so commonplace that any mention of business risk should contemplate these types of losses.

California liability

The California Consumer Privacy Act (CCPA) went into effect on January 1, 2020. The CCPA gives California residents expansive rights[36] over businesses' collection, use and sharing of their personal information. The CCPA: (1) vests general enforcement authority with the California Attorney General;[37] and (2) creates a private right of action that can only be brought to certain data breach incidents "and shall not be based on violations of any other section of" the CCPA.[38] *More than 50 lawsuits were filed in the first six months after the CCPA went into effect.* Roughly half of these lawsuits related to data breaches. The CCPA created no other types of civil or regulatory liability. However, the CCPA has been used to augment certain existing civil liability theories.

Plaintiffs in the other cases premise claims on alleged violations of consumer rights, often asserting that non-compliance with the CCPA, by extension, constitutes a violation of California's Unfair Competition Law (UCL), Consumer Legal Remedies Act (CLRA), or other causes of action. Many of the suits, whether for data breach or hybridised with another theory, were filed as class action lawsuits.

CCPA enforcement against directors

As mentioned above, the California Attorney General has broad authority to enforce all violations of the CCPA. Businesses that violate the CCPA will be subject to civil enforcement actions by the Attorney General. Violating businesses will be given a notice of non-compliance and a 30-day opportunity to cure the non-compliance. Businesses who fail to comply within the 30 days will be subject to an injunction and a civil penalty: $2,500 for each unintentional violation; and $7,500 for each intentional violation. Because of the nature of privacy and cybersecurity events, these violations, and the related penalties, can compound quickly.

The California Attorney General has exercised broad authority to enforce California laws against directors in the past.[39] However, enforcement of the CCPA only began on July 1, 2020. The regulations issued after enforcement began.[40] These regulations provide no insight as to whether the California Attorney General will seek to hold officers and directors personally liable for a company's violations. Furthermore, active enforcement is still so new that we have few cases to examine that would suggest such authority will be exercised in the future. In general, officers and directors should be aware of the risk that the California Attorney General will seek to utilise the CCPA against them if there are systemic failures under that statute.

CCPA civil suits filed in connection with data security incidents

Most CCPA civil cases allege a data breach and then generally contend that the breach was a violation of the CCPA without offering additional details.[41] The CCPA claims usually join negligence, breach of contract, unjust enrichment, and violation of the California Unfair Competition Law claims.[42] Other cases include greater factual and procedural specificity.[43] However, thus far, none of these cases have sought to hold the officers or directors personally liable.

A number of cases also assert a violation of California's Unfair Competition Law *based upon* a data breach violating the CCPA.[44] The Unfair Competition Law defines "unfair competition" broadly to "mean and include any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising and any act prohibited by [California's false advertising law]". While these cases may seek injunctive relief and restitution, they, like the pure CCPA cases, have not yet articulated any claims against the officers and directors.

These class action cases are not the only types of civil liability that may draw upon the CCPA. One recently filed case is between competing businesses engaged in market research that involves the collection and sale of personal information.[45] The plaintiff alleges that the defendant (the plaintiff's former business partner and now competitor) violated the CCPA by failing to provide sufficient notice of its privacy practices to consumers, and as a result, has gained an unfair and unlawful advantage in violation of the Unfair Competition Law. It is not hard to see insider directors wrapped up in similar theories.

Alleging compliance with the CCPA could even form the basis of some of the derivative actions based upon the fiduciary duties discussed earlier. Basically, such cases would allege that violating the CCPA constitutes a gross dereliction of oversight that amounts to a breach of fiduciary duties. Cases utilising these theories are coming, but as we shall see below, the cases filed thus far have not reached a high level of sophistication.

Privacy litigation under the California Consumer Privacy Act 2018

In March 2020, plaintiffs filed *Cullen v. Zoom Video Comm., Inc.*[46] Since filing, the judge in this Northern District of California federal civil action related and consolidated separate actions. This recaptioned Frankenstein monster of a class action lawsuit claims that Zoom illegally shared millions of users' personal information with Facebook and failed to protect their personal information, thus violating the CCPA. Plaintiffs also allege that Zoom's privacy policy contained misrepresentations, that Zoom made inadequate privacy notices about its data collection and use, and that Zoom failed to implement and maintain reasonable security procedures and thus committed fraud in violation of California's Unfair Competition Law. The lawsuit also alleges violations of California's Consumers Legal Remedies Act and of California consumers' constitutional privacy rights. The viability of these claims will not be tested soon: a hearing on class certification is scheduled for May 27, 2021.

The "*Consolidated Ambry Genetics Cases*"[47] is the collective name for the consumer class action cases filed against genetic testing company Ambry Genetics for a January 2020 data breach. Plaintiffs allege that the breach resulted in unauthorised access to customer personally identifiable information and protected health information, and that Ambry failed to timely report the breach to the government or to customers. These cases were consolidated in June 2020. Despite the wide variety of legal theories on display here, none of the *Consolidated Ambry Genetics Cases* articulate personal liability claims against the officers or directors. The same is true for *Gupta v. Aeries Software, Inc.*,[48] wherein plaintiffs allege that Aeries did not adequately safeguard the personally identifiable information of thousands of vulnerable students, resulting in unauthorised third parties accessing that data. *G.R. v. TikTok*[49] provides yet another CCPA lawsuit that fails to bring claims against the officers and directors. While this case does not directly impact them, officers and directors should take note of the data security and privacy issues that are explored in this case, which alleges unlawful harvesting of biometric identifiers from minor and adult users. These types of issues do not seem to involve data security or privacy, but the laws and regulations – including the CCPA – increasingly cover both biometrics and the protection of minors. The lawsuits will follow the same path as these laws and regulations.

Other state liability

New York State

The New York Department of Financial Services, which is responsible for the regulation of banks, insurers, and other financial institutions that do business in New York, has a growing role in pushing cybersecurity standards. The NYDFS also possesses an expansive view of its own jurisdictional limits, the entities that it regulates, and their respective officers and directors.

New rules developed by the NYDFS under 23 NYCRR Part 500 (the "Regulation"), which went into effect on March 1, 2017, require entities that NYDFS regulates to implement specific cybersecurity standards. These standards include establishing a comprehensive cybersecurity policy, completing a written incident response plan (focusing upon reporting breaches within 72 hours to the NYDFS), and promulgating security policies for third-party vendors. The rules require officers and directors to not only designate a chief information security officer (CISO), but also to certify to the NYDFS that the company is in compliance with the regulations.

The CISO must prepare an annual report to the board of directors of the regulated entity regarding its cybersecurity programme. The report must: (1) specifically address the identification of material cyber risks to the regulated entity, including any past material cybersecurity event; and (2) report on penetration testing and vulnerability assessments. The CISO must also report to the board of directors about, *inter alia*, multifactor authentication and cyber awareness training for all personnel. In short, the boards of covered companies likely received far more cyber information than they ever received prior to the NYDFS rules. With this deep cyber information in hand, officers and directors were required to submit the first cybersecurity compliance certification to the NYDFS by February 15, 2018. This is an annual requirement[50] that will, each year, put directors into the cybersecurity weeds. Moreover, by certifying compliance with these detailed cybersecurity requirements, directors become the primary targets of these regulators if a breach occurs.

Other states

A number of other states are considering enhanced cybersecurity and privacy regulations. In the privacy sphere, many states are considering adopting aspects of California's sweeping CCPA. Other states, like Washington, are likely to adopt a framework similar to that utilised by the European Union,[51] which is discussed in further detail below. In any case, the two main risks to directors are the same as they are in California: (1) enforcement actions against officers and directors brought

by individual state attorneys general; and (2) private actions alleging either substantive violations of the statute or qualitative violations of the duty of care premised upon a failure to comply with the statute.

Global Personal Cyber Risks for Officers and Directors

New legislation in a range of jurisdictions – most notably in the EU, under the new General Data Protection Regulation (GDPR)[52] – will hold organisations to higher cybersecurity and cyber standards than ever. With those growing risks in mind, it is useful to consider the potential liability landscape in all jurisdictions in which they are active.

The United Kingdom

In the United Kingdom (UK), directors' fiduciary duties to the company are largely codified under the Companies Act 2006 (the 2006 Act).[53] Among other things, directors of UK companies possess a duty to promote the success of the company and to exercise reasonable care, skill, and diligence in the conduct of their role.[54] Similar to United States civil liability theories, the board's failure to understand and mitigate cyber risks could constitute a breach of these duties. In evaluating these types of claims, UK law requires that we consider the standard of a reasonably diligent person with the knowledge and skill of the director in question. These standards will be tested, as in the United States, via derivative actions.

Recent UK case law has established that civil lawsuits may be brought against violations of the UK Data Protection Act 1998.[55] Perhaps most concerning to companies assessing their civil cyber risks in the UK is that these Data Protection Act cases can proceed even when the plaintiff has not suffered pecuniary loss. Stated differently, companies face civil losses even where they did not cause anyone to actually lose money. These UK cybersecurity and privacy lawsuits may be brought against the company or the individual directors.

Doing business in the UK will also expose companies to the GDPR. The UK's "Brexit" from the EU will not alter the applicability of the GDPR. The GDPR imposes broad regulations upon companies that control or process personal data. Penalties for GDPR violations can be staggering: non-compliance penalties extend up to the higher of €20 million or 4% of the organisation's worldwide revenue. Moreover, directors of public companies bear the responsibility for compliance with the GDPR and personal liability for any fines and penalties.[56] In addition, the Information Commissioner's Office, the UK's data privacy regulator, can compel future conduct from senior board members to ensure that the company complies with its ongoing data protection obligations.

Directors of regulated entities also need to be aware of their UK personal regulatory obligations. In the financial services sector, the Financial Conduct Authority closely scrutinises directors, and will take action if a director fails to discharge their regulatory duties as a result of not properly managing the organisational cyber risks. Similarly, directors of publicly traded companies must appropriate disclosures under the UK Listing Rules. These disclosures may include a wide range of adverse cyber events. Directors face personal liability for any failure to disclose such events.

The EU

In addition to the GDPR, which we discussed with regard to the UK, the EU is developing a number of new laws and regulations regarding cybersecurity and privacy. For example, the EU Network and Information Security Directive (NIS Directive)[57] will require companies in certain industries (including such far-flung industries as financial services and "water transport"[58]) to implement certain minimum cyber security standards. While enforcement of the NIS Directive is still unclear, and its effectiveness is under review as of October 2020, the mere fact that the NIS Directive will be implemented in the EU should alter the way that directors think about cybersecurity implementation.

Germany

German law provides similar personal liability pitfalls for directors. Under German law, directors can be held liable for breach of their duties. These cybersecurity duties include, *inter alia*, a duty to ensure that adequate IT infrastructure is in place to protect data security and avoid cyber risks. Directors must therefore ensure that certain technical standards are met, which are actually spelled out in the German Data Protection Act (*Bundesdatenschutzgesetz*) and the German IT Safety Act (*Bundessicherheits- und Informationstechnikgesetz*). The German laws also require a high level of ongoing systems monitoring. This can mean that the failure to note intrusions, which can sometimes last months, can itself constitute an organisational failure. While all of these regulatory responsibilities should concern directors, it bears noting that German law generally only permits director liability to the company, and not to third parties, although the risk exists.

United Arab Emirates

Under United Arab Emirates (UAE) law, officers and directors of a company can face personal liability for matters relating to cyber risk. The board of directors of a public joint stock company is liable to the company, its shareholders and third parties for certain acts, including fraud, misuse of power, breach of the UAE Commercial Companies Law or the company's articles of association, or an error in management.[59] While little case law exists on how these provisions may be applied, it is possible that cybersecurity and privacy failures may fall under the law.

Of more concern should be potential criminal liability under UAE law. Officers and directors should be mindful that potential criminal liability exists for the unauthorised disclosure of personal information. Reportedly, in March 2015, three executives in the UAE were all temporarily imprisoned on the grounds of a breach of privacy in connection with the installation of CCTV. Jail time is therefore a real possibility in the UAE.

Canada

Canadian law can impose personal liabilities upon officers and directors of a company for matters relating to cybersecurity and privacy risk under Canadian law. The Canada Business Corporation Act RSC 1985 (CBCA) requires every director to exercise their powers and duties honestly and in good faith, with a view to the best interests of the corporation, and exercise the care, diligence, and skill that a reasonably prudent person would exercise in comparable circumstances.[60] The CBCA provides for shareholder derivative actions for breaches of duties owed by directors to the company and the recovery of monetary damages on behalf of the company.[61] Thus, in theory, companies operating in Canada bear many of the same litigation risks for their cybersecurity and privacy failures.

As in the United States, Canada imposes liability upon directors for omissions or misrepresentations in public disclosures. Moreover, since September 2013, the Canadian Securities Administrators have instructed that issuers should expressly disclose their cyber-crime risks, any cyber-crime incidents, and characterise their cyber-security controls in a prospectus or a continuous disclosure filing.[62]

Officers and directors also face statutory liabilities under privacy statutes in Canada, although these statutes only exist in certain discrete Canadian jurisdictions. Breaching Quebec's privacy statute can lead to monetary fines against directors who ordered or authorised the breaches.[63] Likewise, Ontario's Personal Health Information Protection Act 2004 contains penalties imposed on officers and directors for the wilful collection of health information without reasonable protections.[64]

South Africa

South African law also creates personal liabilities for officers and directors in connection with cybersecurity and privacy risks under South African law. As in other countries utilising a derivation of the English legal system, the failure to implement reasonable cybersecurity measures could constitute a breach of directors' fiduciary duties. As in countries like the United States and England, these fiduciary duties were established by way of the common law, and have later been codified. Just as in these other countries, officers and directors have a duty to maintain certain minimal cybersecurity and privacy procedures and oversight. Officers and directors could theoretically face personal liability to the company and to third parties for a breach of these duties. A breach of directors' fiduciary duties could lead to claims being brought against officers and directors. Similarly, just as in the UK and the United States, directors may face personal liability in contract or tort. This risk is even more acute in South Africa, where the governing laws permit great personal liability, even when working through the "legal fiction" of a corporation.

Moreover, a breach of fiduciary duty could lead to South African regulators taking action against officers and directors. For example, the Companies and Intellectual Property Commission (CIPC) can investigate these complaints, and various mechanisms allow action to be taken against a company or its directors.

Common law, not a statute, primarily protects the South African right to privacy. However, South Africa has also passed the Protection of Personal Information Act, of 2013 (POPI).[65] Under POPI, regulatory action may be taken against an organisation or person for any violation. Therefore, depending on the nature of each violation, a director may face civil fines, administrative fines, penalties, and even a period of imprisonment. POPI does not fully become effective until July 2021, which is when the "grace period" ends.

Australia

As in the UK, United States, and South Africa, officers and directors face certain familiar personal liability risks for a company's cybersecurity and privacy failures. All officers and directors have a key responsibility to ensure that companies adopt appropriate risk management strategies to protect the company and its shareholders via their duty of care and due diligence, both under Section 180 of the Corporations Act 2001[66] and the common law. The Australian corporate regulator, the Australian Securities and Investments Commission (ASIC), has the power to bring an action against officers and directors for a breach of their duties. The consequences are potentially serious, and include a declaration of contravention, pecuniary penalties, compensation orders, and disqualification of the director or officer from managing a corporation. ASIC Report 429[67] states that: it considers board participation important to promoting a strong culture of cyber resilience; and a failure to meet obligations to identify and manage cyber risks may result in stiff penalties. Finally, a failure by officers and directors to take reasonable steps to prevent, or respond appropriately to, a cyber or privacy incident may also give rise to Australian civil proceedings, either via derivative action brought by the shareholders or by affected individuals.

Emergent Areas of Special Cybersecurity and Privacy Concern to Officers and Directors

Data and privacy security is not just the target of criminals. Foreign governments utilise their military and intelligence resources to actively attack the privacy and data assets of private companies. These state actors carry special risks that officers and directors must acknowledge. For example, Chinese military hackers stole U.S. Steel's trade secrets and gave them to Chinese steel companies so that they could better compete in western markets.[68] U.S. Steel attempted to meet this threat by filing an action in the International Trade Court.[69] After a long and costly fight, U.S. Steel withdrew its cybertheft action, but the legal fight is far from over.[70] Whenever nations endeavour to interfere with businesses, the officers and directors should take note.

State actor privacy and data security concerns can even lead to the forced liquidation of assets. The saga of TikTok is well known at this point. However, it bears repeating that the United States' insecurity about the state of TikTok's privacy and data security procedures and controls has led directly to a likely "forced" liquidation of United States assets. Russia's potential control over private data led to similar insecurity over the viral "FaceApp".[71] In other words, state actors are now colliding with privacy and data security in a manner that provides an existential threat to many companies. Where the risks to companies are great, the personal liability risks to officers and directors can be correspondingly large.

Certain business sectors can also face outsized risks of which officers and directors must be aware. If a company services sensitive or classified governmental contracts, they will be both a target of bad actors and also subject to increased regulatory oversight. The dimensions of those standards, whether under the Defense Federal Acquisition Regulation Supplement (DFARS) cybersecurity requirement, or under government contracting requirements that National Institute of Standards and Technology guidelines be met, should be the subject of a different chapter. However, for our purposes, we should acknowledge that officers and directors must be aware that these standards exist – and work to satisfy them – or else they face the loss of extremely valuable contracts.

Not only traditional defence and governmental industries face these threats: state-sponsored hackers hacked Yahoo![72] and the World Anti-Doping Agency.[73] Zappos was hacked by a hacker who works for the successor to the KGB.[74] While Zappos is a very cool online commerce company, one would not usually think of it as a geopolitical target. That is all changing. Officers and directors must address these risks now or they face the prospect of personal liability for their failures later.

Endnotes

1. https://www.sec.gov/news/press-release/2018-22.
2. https://www.sec.gov/news/press-release/2018-71.
3. https://www.sec.gov/rules/interp/2018/33-10459.pdf; see also 17 CFR 243.100. Final Rule: Selective Disclosure and Insider Trading, Release No. 34-43154 (Aug. 15, 2000) [65 FR 51716 (Aug. 24, 2000)].
4. Proxy Disclosure Enhancements, SEC Release Nos 33-9089, 34-61175, IC-29092; 74. Fed. Reg. 68334 (Dec. 23, 2009).
5. Disclosure Required by Sections 406 and 407 of the Sarbanes-Oxley Act of 2002, SEC Release Nos 33-8177, 34-47235; 68 Fed. Reg. 5110 (Jan. 31, 2003).
6. Director liability under the operative sections of the federal securities laws turns on the director's knowledge or the reasonableness of their beliefs in a specific situation presumably being impacted by their particular qualifications, background or expertise. A director has a "due diligence" defence to liability under Section 11 if they sustain the burden of proof that, with regard to any part of the registration statement not made under the authority of an expert, the director "had, after reasonable investigation, reasonable ground to believe and did believe, at the time such part of the registration statement became effective, that the statements therein were true and that there was no omission to state a material fact". Federal courts have generally taken the view expressed in *Feit v. Leasco Data Processing Equipment Corp.*, 332 F. Supp. 544, 577 (E.D.N.Y. 1971), that "[w]hat constitutes 'reasonable investigation' and a 'reasonable ground to believe' will vary with the degree of involvement of the individual, h[er] expertise and h[er] access to the pertinent information and data". Thus, directors who are insiders, or directors who are attorneys involved in preparation of the registration statement, generally are expected to make a more complete investigation and have more extensive knowledge of the facts at issue.
7. 17 CFR 229.407(h); 17 CFR 240.14a-101 – Schedule 14A.
8. Final Rule: Proxy Disclosure Enhancements, Release No. 33-9089 (Dec. 16, 2009) [74 FR 68334 (Dec. 23, 2009)], available at http://www.sec.gov/rules/final/2009/33-9089.pdf.
9. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release Nos 33-10459, 34-82746 [Feb. 26, 2018], available at https://www.sec.gov/rules/interp/2018/33-10459.pdf.
10. https://www.sec.gov/litigation/complaints/2018/comp-pr2018-40.pdf; https://www.sec.gov/litigation/complaints/2018/comp-pr2018-115.pdf.
11. https://www.sec.gov/news/testimony/testimony-oversight-us-securities-and-exchange-commission.
12. *Id.* at 3–4.
13. Section 141(a), Delaware General Corporation Law.
14. *Graham v. Allis-Chalmers Mfg Co.*, 188 A 2d 125, 130 (Del 1963).
15. *Smith v. Van Gorkom*, 488 A 2d 858, 872 (Del 1985).
16. *Stone v. Ritter*, 911 A 2d 362, 370 (Del 2006).
17. 806 F. Supp. 1197 (E.D. Pa. 1992).
18. *Id.* at 1203.
19. *Id.* at 1204.
20. 801 F. Supp. 1493 (D. Md. 1992).
21. *Id.* at 1501.
22. 698 A.2d 959 (Del. Ch. 1996).
23. *Id.*
24. No. 17-cv-5225(RJS), 2018 WL 9517195 (Sep. 29, 2018).
25. *Id.* at *6.
26. *Id.* (citing *In re Citigroup Inc. S'holder Derivative Litig.*, 964 A.2d 106, 128 (Del. Ch. 2009)) ("[A] showing of bad faith is a necessary condition to director oversight liability").
27. *In re Citigroup Inc. S'holder Derivative Litig.*, 964 A.2d at 112 ("[A] showing of bad faith is a necessary condition to director oversight liability").
28. No. 533, 2018 (Del. Sup. Ct. 2019).
29. *In re Gen. Motors Co. Derivative Litig.*, C.A. No. 9627-VCG, 2015 WL 3958724, at *17 (Del. Ch. June 26, 2015).
30. *Wayne Cty. Emp.'s Ret. Sys. v. Dimon*, 629 F. App'x 14, 15 (2d Cir. 2015).
31. 964 A.2d 106 (Del. Ch. 2009).
32. *Id.* at 128 n.63.
33. *Id.*
34. C.A. No. 16415, 2004 BL 1814 (Del. Ch. May 3, 2004).
35. 435 F. Supp.3d 679 (D. Md. 2020).
36. The Act provides California residents with the right to seek access to, or deletion of, their personal information, as well as the right to object to the sale or sharing of such information with third parties.
37. See Cal. Civ. Code § 1798.155(b).
38. See Cal. Civ. Code § 1798.150(c) ("The cause of action established by this section shall apply only to violations as defined in subdivision (a) [regarding data breaches] and shall not be based on violations of any other section of this title. Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law. This shall not be construed to relieve any party from any duties or obligations imposed under other law or the United States or California Constitution").
39. https://oag.ca.gov/news/press-releases/attorney-general-sues-remove-stakeholder-members-iso-board.
40. https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf.
41. See, e.g.: Complaint, *Albert Almeida, Mark Munoz, and Angelo Victoriano v. Slickwraps Inc.*, No. 2:20-at-00256, at 28, 48 (E.D. Cal. March 12, 2020); Complaint, *Daniela Hernandez v. PIH Health*, No. 2:20-cv-01662, at 6, 19, 38 (C.D. Cal. Feb. 20, 2020); Complaint, *Bernadette Barnes v. Hanna Andersson, LLC, and Salesforce.Com, Inc.*, No. 4:20-cv-00812-DMR, at 3, 15 (N.D. Cal. Feb. 3, 2020); and Complaint, *Juan Maldonado v. Solara Medical Supplies, LLC*, No. 3:19-cv-02284-H-KSC, at 3, 21 (S.D. Cal. Nov. 29, 2019).
42. See, e.g.: Complaint, *Slickwraps* at 39, 44, 46 and 48; Complaint, *Hernandez* at 22, 27, 30 and 37; Complaint, *Barnes* at 16 and 22; and Complaint, *Maldonado* at 23, 30, 33 and 34; see also *Rahman v. Marriott International, Inc.*, Case No. 8:20-cv-00654 (C.D. Cal., Apr. 3, 2020) (this putative class action on behalf of California residents against Marriott for a data breach that was announced on March 31, 2020 alleges violation of the CCPA and California's Unfair Competition Law, as well as breach of contract and implied contract, negligence, and unjust enrichment).
43. See, e.g.: Complaint, *Michele Pascoe v. Ambry Genetics*, No. 8:20-cv-00838, at 50 (C.D. Cal. May 1, 2020) at 50; and Complaint, *Lopez* at 44.
44. See, e.g.: Complaint, *Slickwraps* at 48; and Complaint, *Hernandez* at 37–38.
45. See Complaint, *Bombora v. ZoomInfo*, No. 20-cv-365858 (Cal. Super. Ct. June 10, 2020).
46. Case No. 20-cv-02155 (N.D. Cal. Mar. 30, 2020).
47. Case No. 8:20-cv-00791 (C.D. Cal.).
48. Case No. 8:20-cv-00995-FMO-ADS (C.D. Cal., May 28, 2020).

49. Case No. 2:20-cv-04537 (C.D. Cal.).
50. https://www.dfs.ny.gov/industry_guidance/cyber_filings/requirements.
51. https://fpf.org/2020/01/13/its-raining-privacy-bills-an-overview-of-the-washington-state-privacy-act-and-other-introduced-bills/#:~:text=The%20Act%20would%20be%20a,creates%20a%20nuanced%20approach%20to.
52. https://eur-lex.europa.eu/eli/reg/2016/679/oj.
53. https://www.legislation.gov.uk/ukpga/2006/46/contents.
54. *Id.* (Sections 172 and 174, 2006 Act).
55. *Google Inc v. Vidal-Hall and other* [2015] EWCA Civ. 311.
56. Per the first and second paragraphs of Article 169, the members of the management board must act as thorough and diligent owners, and they are jointly and severally liable for the damage inflicted on company by their actions.
57. https://eur-lex.europa.eu/eli/dir/2016/1148/oj, 2016/1148/EU.
58. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC.
59. Article 162, UAE Federal Law No. 2 of 2015 on Commercial Companies.
60. https://laws-lois.justice.gc.ca/eng/acts/C-44/page-21.html?txthl=duties+duty#s-122.
61. https://laws-lois.justice.gc.ca/eng/acts/C-44/page-41.html?txthl=derivative#s-239.
62. https://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20130926_11-326_cyber-security.htm#:~:text=To%20manage%20the%20risks%20of,and%20their%20clients%20or%20stakeholders.
63. http://legisquebec.gouv.qc.ca/en/showdoc/cs/P-39.1.
64. https://www.ontario.ca/laws/statute/04p03.
65. https://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf.
66. http://www5.austlii.edu.au/au/legis/cth/consol_act/ca2001172/s180.html#:~:text=Care%20and%20diligence%2D%2Dcivil%20obligation%20only,-Care%20and%20diligence&text=The%20director's%20or%20officer,in%20their%20position%20would%20hold.
67. https://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf.
68. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.
69. https://www.wsj.com/articles/u-s-steel-accuses-china-of-hacking-1461859201.
70. https://www.wsj.com/articles/u-s-steel-withdraws-hacking-claim-against-chinese-rival-1487183293.
71. https://www.pbs.org/newshour/science/is-faceapp-a-security-risk-3-privacy-concerns-you-should-take-seriously.
72. https://www.nytimes.com/2017/03/15/technology/yahoo-hack-indictment.html.
73. https://www.nytimes.com/2019/10/28/sports/olympics/russia-doping-wada-hacked.html.
74. https://www.forbes.com/sites/thomasbrewster/2017/03/20/alexsey-belan-yahoo-fbi-hacker-allegations/#bc236cd76f24.

Christopher Ott, CIPP/US, leads data security, privacy, and white-collar litigation and investigations. Leveraging his experience from more than 13 years at the U.S. Department of Justice (DOJ), including successfully litigating complex data security matters, conducting hundreds of investigations, and winning dozens of appeals, Mr. Ott works with clients on disputes and strategy relating to data security, privacy, blockchain, and AI issues. Mr. Ott has handled hundreds of matters involving the intersection between white-collar matters (accounting, securities, money laundering) and cybercrimes (from international criminal gangs to state actors). In his most recent governmental role, Mr. Ott acted as Supervisory Cyber Counsel to the National Security Division of the DOJ. Mr. Ott consulted extensively with the intelligence community and coordinated extensively with regulators such as the U.S. Treasury Department, the Federal Communication Commission (FCC), the Federal Trade Commission (FTC), and the Securities Exchange Commission (SEC).

Rothwell Figg
607 14th Street N.W.
Suite 800
Washington, D.C. 20005
USA

Tel: +1 202 783 6040
Fax: +1 202 783 6031
Email: cott@rothwellfigg.com
URL: www.rothwellfigg.com

The Privacy, Data Protection & Cybersecurity team at Rothwell Figg helps clients understand and navigate these rapidly evolving areas of law. We work with our clients to prepare, integrate, and implement compliance strategies, frameworks for risk management, and best practices. We have experience working closely with our clients to: build data inventories and assess their legal obligations; to implement back-end and structural changes that are not only compliant, but also workable; to prepare written policies, assessments, forms, and notices to effectuate legal requirements and best practices; to negotiate, draft, and review agreements for compliance; and to help train staff. We can assist with the design and implementation of incident response plans, and if there ever is an incident, we can serve as trusted advisors, from the investigation stages through to litigation, helping you navigate disclosure requirements to public authorities. Most of the attorneys in the practice group are experienced litigators with deep technical backgrounds and have represented clients in a wide variety of venues, including before numerous government agencies and in state courts, federal district courts and courts of appeal, and the United States Supreme Court.

www.rothwellfigg.com

ROTHWELL FIGG
IP Professionals

ICLG.com

Other titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Outsourcing
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by: global legal group