quinn emanuel trial lawyers
quinn emanuel urquhart & sullivan, llp

Legal Concerns Clients Are Having About Covid-19

U.S. Outlook: Cybersecurity Legal Implications For Businesses Amid New Coronavirus Outbreak

March 25, 2020

Jennifer J. Barrett
jenniferbarrett@quinnemanuel.com
Phone: +1 212-849-7155

Viola Trebicka
violatrebicka@quinnemanuel.com
Phone: +1 213-443-3243

Allison Que
allisonque@quinnemanuel.com
Phone: +1 650-801-5076

Anil Makhijani
anilmakhijani@quinnemanuel.com
Phone: +1 212 849 7334

Among the myriad challenges faced by businesses arising out of the global COVID-19 pandemic is the amplification of cybersecurity vulnerabilities and resulting increased risk of data breach and malware incidents. Throughout the world, employees are working from home via remote access technology and on personal devices, giving rise to unprecedented and likely unanticipated cybersecurity risks. Compounding this effect, malicious actors are out in force, preying upon the system and human insecurities created by the current COVID-19 climate. Not surprisingly, cybersecurity experts are warning of a new wave of cyberattacks aimed precisely at the working-from-

home population.[1] Not even the World Health Organization is safe: just yesterday its Chief Information Security Officer confirmed that cyberattacks against it have doubled and, most recently, elite hackers connected to cyber-espionage operations tried to break its cyber-defenses.[2]

In this article, we explore the new cybersecurity challenges and vulnerabilities businesses face as a result of the pandemic, consider the current situation in the context of the existing regulatory regime and potential private litigation exposure, and offer some practical advice to businesses and their employees related to remote work in this new business reality.

* * *

1) The COVID-19 Pandemic Has Created New Cybersecurity Challenges And Vulnerabilities

With the new normal of a global workforce working from home comes new cybersecurity risk. Malicious actors love a crisis and are actively deploying schemes to exploit the general anxiety related to COVID-19 and the system vulnerabilities associated with remote work.[3] Phishing, hacking, and malware attempts are on the rise and expected to get worse. Of particular concern are cyberattacks specifically related to COVID-19 and government health agencies.[4] For example, hackers have sent phishing messages posing as the Centers for Disease Control and Prevention ("CDC") or the World Health Organization to access sensitive information and compromise security systems.[5] In another scheme, an interactive map tracing COVID-19 infections and deaths was used to spread password-stealing malware.[6]

Unfortunately, this uptick in malicious cyber activity is compounded by the system and hardware challenges created by employees working from home. Businesses are facing a cyber-risk perfect storm arising out of this scenario, including:

- *Increased Use of Personal Devices.* Personal devices and unsecured networks are more vulnerable to malware than enterprise devices and infrastructure due to the lack of strong encryption, commercial grade malware protection, lost device tracking, remote wipe capabilities, and ability for remote administration. Further, personal computers may be shared with family members, who may accidentally view confidential data and may not be trained to use the device in a safe way.

- *Increased Use of Unsecured Networks.* Communication through unsecured networks may be vulnerable to eavesdropping and man-in-the-middle (MITM) attacks. Also, if a device is infected with malware through an external network and then connected to the company's network, the malware may spread across the company's internal network.

- *Overloaded Systems.* Some companies may already have secured networks set up for remote access. Many companies, however, have historically limited the use of remote access and not conducted stress testing targeted to the current situation. The sudden spike in remote access activity may overload the system or expose opportunities for unauthorized activity.

- *Social Engineering.* Given that remote-work policies tend to encourage communication over email, phone, and other media, employers face an increased risk of social engineering attacks such as "phishing" or "vishing" attacks. These attacks are not just confined to the coronavirus-themed ones described above. Rather, malicious actors may also leverage

interactions with employees by posing as reputable or trustworthy entities or the employees' coworkers, obtaining sensitive information or passwords.

- *Lack of Comprehensive Training*. Employees who are regularly allowed remote access have likely already been trained on best practices for remote cyber access. But companies now have had to make very quick decisions to convert a large portion of their workforce to work from home. In many instances, there has been simply no time or resources to extend that training to the entire remote access population.

- *Deficient Incident Response Plans*. Most businesses have an Incident Response Plan ("IRP"). It is reasonable to assume, however, that IRPs do not generally contemplate a situation where virtually all employees work from home. Therefore, a company's IRP may not be flexible enough to run an effective incident response in a remote fashion, leading to delayed remediation of cyber incidents.

- *Employees' Innocuous Circumvention of Security Protocols*. When employees work from home, they tend to let their guard down. For example, employees who experience technical difficulties in activities such as printing documents or accessing data may be tempted to use less secure means to accomplish work tasks, such as emailing confidential documents to their personal email accounts or downloading data to their personal devices, thus unwittingly creating opportunities for hackers.

2) Regulatory Exposure: The Overlapping Federal And State Cybersecurity Regime

There is no single set of cybersecurity laws. Nor is there a single government agency responsible for enforcing cybersecurity practices or investigating data breaches. Instead, enforcement of data security related issues is conducted by different agencies, depending on the nature of the violation and the location and industry of the target company. This legal and regulatory regime is no different during this public health crisis.

At the federal level, the major government agencies that are involved in cybersecurity issues include the Federal Trade Commission, the Securities and Exchange Commission, the Department of Homeland Security, the Department of Commerce, the Federal Bureau of Investigation, the Department of Justice, and the Department of Health and Human Services Office for Civil Rights. Some of these agencies have published guidelines that include specific cybersecurity measures for companies to adopt when implementing remote access policies. Because these measures are particularly relevant to the surge in work-from-home, we provide a short overview below:

The **Federal Trade Commission** protects consumer privacy through enforcement actions under the FTC Act, which prohibits unfair and deceptive acts or practices—including privacy practices—that affect commerce. The FTC has published various informational materials on reasonable cybersecurity practices, including a guide titled "Start for Security Guide for Business,"[7] which provides lessons based on past FTC enforcement actions. There are many practical guidelines included in the document regarding securing employee work environments. Further, it has also published specific guidelines[8] intended to give employers direction on how to secure remote access for employees who may need to connect to the company network remotely. The FTC blog also recently posted a list of online security tips for employees who work from home.[9]

The **Securities and Exchange Commission**, whose involvement in cybersecurity breaches relates to its oversight of public companies' disclosure of material risks and incidents to potential investors as well as financial institutions' possession of customer account data, has published guidance on cybersecurity measures that public companies should follow.[10] These guidelines specifically discuss precautions to be taken on remote access mobile devices, including the use of virtual private networks ("VPNs"), two-factor authentication, and encryption. Further, in January 2020, the SEC's Office of Compliance Inspections and Examinations issued its examination observations related to cybersecurity and operational resiliency practices taken by market participants. These practices cover various topics relating to remote-working practices, including access rights and controls, data loss prevention, mobile security, incident response and resiliency, and training and awareness.[11]

The **Department of Homeland Security** is involved in the investigation of cybercriminals through its different agencies. For example, the Secret Service is charged with conducting criminal investigations related to the nation's financial and other critical infrastructure. The recently established Cybersecurity and Infrastructure Security Agency (CISA) is a non-regulatory agency that focuses on preventing and stopping cyberattacks against critical infrastructure through information sharing and technical assistance. It has issued a COVID-19 risk management guidance, which covers cybersecurity precautionary measures, and in particular, recommendations relating to maintaining secure and robust remote-access solutions.[12] The CISA also provides timely alerts about current security issues, vulnerabilities, and exploits.[13] For example, on March 13, 2020, it posted an alert regarding enterprise VPN security, encouraging organizations to adopt a heightened state of cybersecurity.[14] We advise all businesses to subscribe the CISA's alerts.

The **Department of Commerce** is tasked with enhancing cybersecurity awareness and protections. Its non-regulatory agency, the National Institute of Standards and Technology (NIST) implements practical cybersecurity and privacy through outreach and effective application of standards and best practices. In March 2020, NIST issued a bulletin on "Security for Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Solutions."[15] The bulletin summarizes key concepts and recommendations from NIST SP 800-46 (Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security), recommending that organizations consider the "balance between the benefits of providing remote access to additional resources and the potential impact of a compromise of those resources."[16] For employees, the NIST's blog recently posted an article introducing "telework security basics."[17]

In addition to the federal regime summarized above, a majority of the states require a person or business who "owns or licenses" data containing personal information to issue security breach notices to state-resident consumers affected by a data breach when certain categories of personal identifying information ("PII") are impacted.[18] Recently, several states have introduced far more restrictive elements to their data breach statutes, including broadening the definitions of PII and adding private rights of action. The California Consumer Privacy Act (CCPA), which went into effect at the beginning of the year, is an exemplar of this trend.[19] Likewise, New York's amended Stop Hacks and Improve Electronic Data Security ("SHIELD") Act, which went into effect on March 21, 2020, broadens the PII definition and implements steeper penalties for noncompliance. Among other things, the amended SHIELD Act requires companies to implement "reasonable" security measures, including implementing procedures to train employees and "adjust[ing] the security program in light of business changes or new circumstances."[20] It also permits the attorney general to levy a fine of up to $5,000 for each failure to adhere to reasonable security standards under Section 350(d) of the New

York General Business Law.[21] (This is in addition to fines that may be levied in the event of a data breach.)

Guidance as to what states view as reasonable cybersecurity measures can be found in the standards and best practices promulgated by many states as part of their task forces to fend off cyber threats and attacks against their state government and local agencies. For example, the California Department of Technology has posted extensive training guidance, best practices, and standards for its state agencies and entities,[22] including those on telework and remote access security (SIMM 5300-A),[23] endpoint protection (SIMM 5355-A),[24] and email threat protection (SIMM 5315-A).[25] Similarly, New York's Office of Information Technology Services has taken the role of promoting best practices and standards on cybersecurity to its state and local agencies, including those on remote access (NYS-S14-010),[26] authentication tokens (NYS-S14-006),[27] identity assurance policy (NYS-P10-006)[28] and standard (NYS-S13-004),[29] cyber incident response standard (NYS-S13-005).[30] Although these policies and standards apply to state/local agencies and their contractors and vendors, these resources can also serve as a guide for private businesses and entities. In fact, the New York Office of Information Technology Services also provides cybersecurity training and toolkits for small businesses and the public.[31]

There has never been a comparable situation from which we can predict how the various federal and state regulatory agencies will respond in the current COVID-19 environment. But history shows that regulators expect businesses to maintain appropriate data security regardless of where their employees are working.[32] The FTC's enforcement action against Lifelock in 2010 illustrates the point. The FTC alleged that Lifelock "[f]ailed to employ sufficient measures to detect and prevent unauthorized access to the corporate network or to conduct security investigations, such as by installing antivirus or anti-spyware programs on computers used by employees to remotely access the network or regularly recording and reviewing activity on the network."[33] The FTC ultimately settled with Lifelock for $100 million for this and other security violations. Similarly, the FTC issued an administrative complaint against LabMD, Inc., alleging the company had committed an unfair act or practice by "fail[ing] to provide reasonable and appropriate security for personal information on its computer networks."[34] Among other allegations, the FTC claimed that the company failed to "require employees, or other users with remote access to the network, to use common authentication-related security measures, such as periodically changing passwords, prohibiting the use of the same password across applications and programs, or using two-factor authentication."[35] In that case, the Eleventh Circuit struck down the FTC's order in June 2018 as unenforceably vague.[36] Although the company prevailed eventually, it won at the cost of half a decade's litigation. More importantly, the *LabMD* decision prompted the FTC to make "significant improvements to its data security orders" in 2019, underscoring the FTC's unabated role in the enforcement of companies' cybersecurity measures, including measures related to remote work.[37]

3) Private Litigation Exposure As A Result Of The Increased Cybersecurity Risks

Consumer Litigation

The increased cybersecurity risks from the COVID-19 outbreak will likely increase the risks of data breaches, therefore exposing businesses to potential consumer. As mentioned above, the CCPA grants a private right of action to any consumer whose PII has been subject to a data breach "as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices."[38] The statutory damages under the CCPA are up to $750 *per consumer per*

incident (or actual damages, if greater than $750).[39] Several other states are also considering new private-right-of-action statutes over data breach, including Connecticut,[40] Illinois,[41] Massachusetts,[42] Minnesota,[43] New Hampshire,[44] New York,[45] and Virginia.[46] Because data breaches often affect large numbers of customers, the total impact for companies can be astronomical.

In addition to statutory claims, plaintiffs have brought class actions under common law theories, with varying degrees of success. These potential claims include negligence, negligence per se, breach of express contract, breach of implied contract, breach of the covenant of good faith and fair dealing, bailment, civil conspiracy, fraud, constructive fraud, unjust enrichment, and breach of duty of confidentiality.[47] Plaintiffs also have brought actions under state business fraud and consumer protection statutes.[48] Historically, the primary challenge to these claims has been showing actual harm caused by the data breach to establish standing.[49] Recent decisions, however, suggest that courts are becoming more forgiving to plaintiffs on this issue, perhaps as a result of the concurrent strengthening of state regulatory protections for consumers.[50] For example, in February 2020, in a case stemming from Marriott's significant data breach of hotel-guest credit card numbers and other sensitive information, a federal court denied Marriott's motion to dismiss on most causes of action, allowing the multidistrict litigation to move forward.[51] Specifically, the court held that the guests had adequately claimed injuries traceable to the hotel's failure to detect a previous hack which resulted in a data breach involving at least 383 million guest records.[52]

The risk of civil litigation is not limited to the United States. In the EU and UK, courts are increasingly sympathetic to private rights of action. For example, the UK's Supreme Court soon will hear an appeal related to a mass opt-out consumer class case against Google for breach of UK data privacy laws. Google is also facing a consumer claim in France. While the Supreme Court's decision to hear the appeal leaves open the viability of mass consumer claims in the UK, at least, there is an increased focus in the EU on consumers ability to bring such actions. Cyber breach related actions are an obvious focus for consumer groups and claimant-focused law firms; and given the globalization of business claims, litigation that starts in the US may have a global effect and also give rise to mirror claims in the EU and UK.

Business-To-Business Litigation

In addition to claims being brought by individual consumers, security breaches can lead to potential claims from business customers, vendors, or any other entity from which a business receives sensitive information. Most business-to-business commercial agreements (including non-disclosure agreements) that contemplate the exchange of sensitive information contain, at a minimum, provisions requiring the recipient of the information to implement reasonable security precautions. More sophisticated commercial contracts lay out specific security precautions that must be implemented and security certifications that are subject to regular security audits. Further, companies that have data controller/data processor relationships with companies in the EU likely have accompanying data processing agreements that set forth parties' data security obligations under the General Data Protection Regulation ("GDPR").

These contractual arrangements can form the basis for direct contract claims between businesses in the event of a cyber breach. Last year, for example, Delta Air Lines sued its chat bot provider, alleging that the vendor's lax cybersecurity caused a 2017 data breach that resulted in the exfiltration of the names, addresses, and payment card information of more than 800,000 Delta customers. In that case, a third-party hacker was able to steal administrative credentials that Delta had

provided to the vendor and then use the stolen information to access Delta's systems. Delta alleged the vendor had breached contract provisions which required the vendor to use adequate security measures, including encryption, to protect customer data.[53] As of the date of this writing, there has been no resolution of the dispute.

Whether or not a data breach arising out the currently uncharted territory of COVID-19 work-from-home requirements or other pandemic-driven circumstances would give rise to liability under a company's commercial contracts will depend upon the specific contract language. But we advise, at a minimum, that all businesses revisit their commercial agreements to ensure that all agreed-to security measures are still being followed given the current practical limitations on operations, including but not limited to a work-from-home period.

Even where two businesses may not have a direct contractual relationship, businesses that operate as part of the same supply chain or rely on each other may attempt to bring claims based on alleged data breaches. Plaintiffs have tried to fashion those claims under theories of negligence, negligence per se, breach of implied contract, breach of contract as a third-party beneficiary, unjust enrichment, or based on consumer fraud or deceptive practice statutes.[54] In these circumstances, courts for the most part have rejected non-contractual tort theories—even when the parties have no direct contractual relationship but are instead interacting through a network or chain of contracts formed by other market participants.[55] "When parties enter into a chain of contracts, even if the two parties at issue have not actually entered into an agreement with each other, courts have applied the 'contractual economic loss rule' to bar tort claims for economic loss, on the theory that tort law should not supplant a consensual network of contracts."[56]

Finally, companies should closely review their customer and client facing statements—including terms and conditions, FAQs, and marketing materials (including websites and blogs)—to ensure that representations about their security methods and commitments continue to be true following crisis-related operational changes.

Securities Fraud Litigation

For public companies, there has been an increasing trend of shareholder lawsuits for securities fraud related to cybersecurity disclosures. For example, Equifax,[57] PayPal,[58] Yahoo, Chegg,[59] and Marriott,[60] all have faced securities lawsuits related to their cybersecurity practices or for having suffered cyber breaches. These lawsuits typically allege one of two theories: (1) failure to disclose the breach in a timely manner; or (2) failure to comply with disclosed cybersecurity policies or best practices.

Notably, the SEC has not publicly signaled that companies will be given more latitude with respect to disclosures and insider trading during this national emergency. Quite the opposite, in the most recent Conditional Relief Order in response to the COVID-19 outbreak, the SEC reiterated the necessity of revisiting and updating material disclosure.[61] The uncertainty of the COVID-19 outbreak's impact on each filing company's business and market, however, will likely make it more challenging for companies to decide whether, when, or what to disclose, thus exposing companies to potential shareholder litigation.

4) Whether A Company Implemented "Reasonable Security" Remains The Key Inquiry In Assessing Liability For A Cyberbreach During The COVID-19 Pandemic

Whether dealing with regulatory enforcement or private litigation, the key inquiry in assessing whether a company will face exposure for a cyberattack is whether it had adopted "reasonable security" measures to safeguard its systems and valuable information. There are few, if any, bright lines here, as with any reasonableness test. The fact that a breach arises in the midst of a public health emergency will not change the inquiry, but it likely will provide context for the fact-intensive assessment that a court or governmental agency will undertake.

For example, the FTC has endorsed a risk-based approach to its definition of reasonableness. Under this approach, "reasonableness" depends on (1) the size and complexity of the business; (2) the information that it holds, including the volume and sensitivity of the data; and (3) the tools the company has to address the risks.[62] Similarly, courts evaluate "reasonableness" by engaging in fact-intensive inquiries to consider, among other factors, the type of data being protected (more sensitive data requires more protection), the current practices in the industry for similar companies, and the feasibility of implementing certain measures.[63]

Due to the peculiar risks and operational challenges brought by the COVID-19 outbreak, however, what used to be reasonable or adequate prior to the outbreak may no longer suffice. The answer will likely involve weighing several factors, such as sensitivity of the data, the size of the company, the resources available for deploying IT solutions for remote workers, and the business history of the company, including historical cybersecurity threats it has received. Given the pressing need of controlling the COVID-19 spread, one may even argue that businesses should be given more leeway in adapting to this urgent and novel situation. However, unless and until the federal or state regulatory agencies provide updated guidance to address this special situation, businesses should still abide by the existing regulatory or legal requirements and strive to maintain as secure a system environment as if it was business as usual.

5) Practical Advice For Businesses And Their Employees To Minimize Cybersecurity Exposure During the COVID-19 Pandemic

In light of the context discussed above, we have prepared the following non-exhaustive list of practical measures to supplement a company's existing internal policies or practices.

- ***Maintain an effective and open communication channel.*** It is critical that business managers and IT personnel have an effective means of communicating updates concerning system limitations, information security measures, and malicious schemes, including COVID-19 related attacks. All businesses should ensure that employees' contact information, especially mobile numbers, is up to date. With many employees electing to shelter-in-place outside of their resident cities, original contact information may no longer be accurate. Official COVID-19 and IT security updates to employees should have a consistent format and should preferably be sent during a fixed time period. This uniformity will minimize the risk that employees will miss important messages or unwittingly follow instructions in malware attacks that may be disguised as official communications from their employer.

- ***Revisit and adjust the Incident Response Plan.*** All companies should promptly revisit their Incident Response Plans to assess whether the existing response plan is flexible enough to deal with the current emergency situation when key IT, privacy, and legal employees are themselves working remotely. While most businesses now maintain their IRPs online, if yours still resides in binders on key employees' office shelves, make sure that everyone has a copy on hand at home. And any communication protocols set forth in plans (such as contact trees by which cyber incidents are initially reported and escalated up to appropriate senior IT, privacy, in-house and outside counsel, and outside forensic consultants) should be updated to ensure that remote contact information is up to date and readily available.

- ***Refresh or provide security awareness training for all employees***. Given the novel risks that arise from remote working, it is important to remind all employees of the company's security policies and system limitations and protections. Refresher training can be done through interactive video conferencing. Alternatively, companies should at least update and redistribute electronic versions of company policies that cover the use of personal computers, smartphones, tablets and WiFi networks for work, and the importance of following the company's security protocols.

- ***Anticipate remote-working challenges and plan accordingly***. All remote-access policies should be based on the assumption that external environments contain hostile threats. IT personnel should develop and conduct stress testing designed to ensure that all systems and system security measures function properly in an environment where most or all employees are working remotely simultaneously. If weaknesses are identified, companies should consider upgrading the system capacity or offering alternative secure remote-access options. Businesses should consider a tiered approach for remote access that would allow the most controlled devices, for example, organization-owned devices, to have the most access and the least controlled devices, for example, personal mobile devices, to have minimum access required for work.

- ***Increase available IT resources***. Companies should anticipate an additional burden on the IT help desk and make sure those employees have the policies, training, and tools they need to handle the requests for technical assistance from remote-working employees. Make sure the IT staff has methods to verify the identity of employees seeking technical assistance. Another helpful precaution is to set up a reliable shortcut for employees to report phishing emails, for example, a "phish alert" add-on to the company's email exchange application that forwards suspicious emails to IT staff who can assess their legitimacy.

- ***Revisit agreements with third-party data vendors***. Businesses should make sure vendors have robust cybersecurity contingency plans. Companies should review their vendor agreements to make sure the agreements are clear about parties' obligations, risk allocation mechanisms, and mitigation measures if a cyber event were to happen in this new environment.

- ***For public companies, revisit the public disclosure on cybersecurity measures***. Public companies should ensure that any disclosure of the company's cybersecurity measures and internal control practices still accurately reflects the actual operation; and if not, consider whether there is a need to update or amend the disclosure.

- ***Documentation***. Finally, businesses should keep detailed documentation of all the steps taken to ensure that they are maintaining a secure environment and adapting to novel challenges being presented by remote employees and COVID-19 related attacks. In the event that a cyber breach occurs and results in regulatory scrutiny or civil litigation, the ability to document all reasonable security enhancement measures will be important.

In addition to the above, below are some practical tips that businesses can consider circulating to employees who have remote access.

- ***Start with cybersecurity basics.*** Use passwords on all your devices and make sure the passwords are long, strong, and unique. Make sure your devices have installed and maintained anti-virus software, firewalls, and email filters. Secure your home network by turning up encryption (WAP2 or WAP3).
- ***Be vigilant about suspicious emails***. Always be suspicious when receiving emails with obvious grammatical or spelling mistakes, especially when the emails have links or attachments. Better yet, always think twice about clicking on links in any email.
- ***Be alert when someone asks for personal or confidential information***. Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about personal information or other internal company information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company. Take advantage of any anti-phishing features offered by the email software or web browser.
- ***Be careful about the authenticity and security of webpages***. Do not send sensitive information over the internet before checking a website's security. Pay attention to the website's Uniform Resource Locator (URL) and look for URLs that begin with "https"—an indication that sites are secure—rather than "http." Look for a closed padlock icon—a sign that information will be encrypted.
- ***Pay attention to the source of information***. Always rely on trusted sources of information for facts about COVID-19, like government or international sites (e.g., CDC, NHS, WHO, CISA, etc.).
- ***Always follow the company's security protocol***. Avoid downloading the company's information to personal devices, uploading the information to personal cloud accounts, or sending the information through personal email accounts. When in doubt or having technical issues, check the company's security protocol or contact the company's IT security team.

* * *

These are only some of the myriad cybersecurity issues potentially posed by the COVID-19 outbreak. If you have any questions about the issues addressed in this memorandum or otherwise, please do not hesitate to reach out to us.

---

[1] Brian Fung & Alex Marquartdt, *Millions of Americans are Suddenly Working from Home. That's a Huge Security Risk*, CNN (Mar. 20, 2020), *available at* https://www.cnn.com/2020/03/20/tech/telework-security/index.html; Maggie Miller, *Hackers Find New Target as Americans Work from Home During Outbreak*, The Hill (Mar. 14, 2020), *available at* https://thehill.com/policy/cybersecurity/487542-hackers-find-new-target-as-americans-work-from-home-during-outbreak.

[2] Reuters, *Elite Hackers Target WHO as Coronavirus Cyberattacks Spike* (Mar. 24, 2020), *available at* https://www.businessinsurance.com/article/20200324/NEWS06/912333684/Elite-hackers-target-WHO-as-coronavirus-cyberattacks-spike-World-Health-Organiza?utm_campaign=BI20200324BreakingNewsAlert&utm_medium=email&utm_source=ActiveCampaign&utm_campaign=BI20200324BreakingNewsAlert&utm_medium=email&utm_source=ActiveCampaign.

[3] *See, e.g.*, Cybersecurity and Infrastructure Security Agency, *Defending Against COVID-19 Cyber Scams* (Mar. 6, 2020), *available at* https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams.

[4] Craig Timberg and Tony Romm, *Hackers are Seizing on Coronavirus Fears to Steal Data, Researchers and U.S. Regulators Warn*, Wash. Post (Mar. 12, 2020), *available at* https://www.washingtonpost.com/technology/2020/03/12/hackers-are-using-coronavirus-fears-target-people-looking-information-infection-maps/.

[5] William Turton and Alyza Sebenius, *Hackers Posing as CDC, WHO using Coronavirus in Phishing Attacks*, Bloomberg (Mar. 12, 2020), *available at* https://www.bloomberg.com/news/articles/2020-03-12/hackers-posing-as-cdc-who-using-coronavirus-in-phishing-attacks.

[6] Krebs on Security, *Live Coronavirus Map Used to Spread Malware* (Mar. 20, 2020), *available at* https://krebsonsecurity.com/2020/03/live-coronavirus-map-used-to-spread-malware/.

[7] FEDERAL TRADE COMMISSION, START WITH SECURITY: A GUIDE FOR BUSINESS, *available at* **https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf**.

[8] Federal Trade Commission, *Cybersecurity for Small Business*, *available at* **https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/securing-remote-access-to-your-network**.

[9] Lisa Weintraub Schifferle, Federal Trade Commission, Division of Consumer & Business Education, *Online Security Tips for Working From Home* (Mar. 18, 2020), *available at* **https://www.consumer.ftc.gov/blog/2020/03/online-security-tips-working-home?utm_source=slider**.

[10] SECURITIES AND EXCHANGE COMMISSION, CYBERSECURITY AND RESILIENCY OBSERVATIONS, *available at* **https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf**.

[11] SECURITIES AND EXCHANGE COMMISSION, OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS, CYBERSECURITY AND RESILIENCY OBSERVATIONS (Jan. 2020), *available at* **https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf**.

[12] Cybersecurity and Infrastructure Security Agency, *CISA Insights, Risk Management for Novel Coronavirus (COVID-19)* (Mar. 6, 2020), *available at* **https://www.cisa.gov/sites/default/files/publications/20_0306_cisa_insights_risk_management_for_novel_coronavirus_0.pdf**.

[13] Cybersecurity and Infrastructure Security Agency, *Alerts*, **https://www.us-cert.gov/ncas/alerts**.

[14] Cybersecurity and Infrastructure Security Agency, *Alert (AA20-073A): Enterprise VPN Security* (Mar. 13, 2020), **https://www.us-cert.gov/ncas/alerts/aa20-073a**.

[15] National Institute of Standards and Technology, Information Technology Laboratory, *Security for Enterprise Telework Remote Access, and Bring Your Own Device (BYOD) Solutions* (Mar. 2020), *available at* **https://csrc.nist.gov/publications/detail/itl-bulletin/2020/03/security-for-enterprise-telework-remote-access-and-byod/final**.

[16] *Id.*

[17] Jeff Greene, National Institute of Standards and Technology, *Telework Security Basics* (Mar. 19, 2020), *available at* **https://www.nist.gov/blogs/cybersecurity-insights/telework-security-basics**.

[18] *See, e.g.*, CAL. CIV. CODE 1798.2; DEL. CODE Ann. tit. 6 § 12B-101*et seq.*; H.R.S. § 487N-1 *et seq.*; Idaho Code § 28-51-104 *et seq.*; LA. REV. STAT. § 51:3071 *et seq.*; MASS. GEN. LAWS 93H § *et seq.*; MICH. COMP. LAWS § 445.63, 72 *et seq.*; MINN. STAT. § 325E.61.

[19] CAL. CIV. CODE § 1798.140(o) (containing an expansive definition of "personal information"); § 1798.150(a)(1) (granting private cause of action for PII breach resulting from business's violation of the duty to implement and maintain reasonable security procedures and practices)

[20] S.5575B Reg. Sess. 2019-2020 (N.Y. May 7, 2019).

[21] *Id.*

[22] Cal. Dep't of Tech., Information Security – Resources, *available at* https://cdt.ca.gov/security/resources/#guidance; Procedures/Standards Updates, *available at* https://cdt.ca.gov/policy/announcements.

[23] CAL. DEP'T OF TECH., OFFICE OF INFO. SECURITY, TELEWORK AND REMOTE ACCESS SECURITY STANDARD (SIMM 5360-A) (Oct. 2018), *available at* https://cdt.ca.gov/wp-content/uploads/2018/01/SIMM-5360A_2018-1018.pdf.

[24] CAL. DEP'T OF TECH., OFFICE OF INFO. SECURITY, ENDPOINT PROTECTION STANDARD (SIMM 5355-A) (Jan. 2019), *available at* https://cdt.ca.gov/wp-content/uploads/2019/01/SIMM-5355-A.pdf.

[25] CAL. DEP'T OF TECH., OFFICE OF INFO. SECURITY, EMAIL THREAT PROTECTION STANDARD (SIMM 5315-A) (Oct. 2018), https://cdt.ca.gov/wp-content/uploads/2018/10/SIMM-5315A.pdf.

[26] N.Y. OFFICE OF INFO. TECH. SERVS., N.Y. STATE INFO. TECH. STANDARD, REMOTE ACCESS (NYS-S14-010) (Mar. 10, 2017), *available at* https://its.ny.gov/sites/default/files/documents/nys-s14-010_remote_access_1.pdf.

[27] N.Y. OFFICE OF INFO. TECH. SERVS., N.Y. STATE INFO. TECH. STANDARD, AUTHENTICATION TOKENS (NYS-S14-006) (Feb. 15, 2017), *available at* https://its.ny.gov/sites/default/files/documents/nys-s14-006_authentication_tokens_standard_3.pdf.

[28] N.Y. OFFICE OF INFO. TECH. SERVS., N.Y. STATE INFO. TECH. POLICY, IDENTITY ASSURANCE (NYS-P10-006) (Feb. 16, 2017), *available at* https://its.ny.gov/sites/default/files/documents/nys-p10-006_identity_assurance_policy.pdf.

[29] N.Y. OFFICE OF INFO. TECH. SERVS., N.Y. STATE INFO. TECH. STANDARD, IDENTITY ASSURANCE (NYS-S13-004) (Mar. 10, 2017), *available at* https://its.ny.gov/sites/default/files/documents/nys-s13-004_identity_assurance_standard.pdf

[30] N.Y. OFFICE OF INFO. TECH. SERVS., N.Y. STATE INFO. TECH. STANDARD, CYBER INCIDENT RESPONSE (NYS-S13-005) (Sept. 10, 2018), *available at* https://its.ny.gov/sites/default/files/documents/nys-s13-005_cyber_incident_response_2.pdf.

[31] *See, e.g.*, N.Y. Office of Info. Tech. Servs., *Awareness/Training/Events*, *available at* https://its.ny.gov/awarenesstrainingevents.

[32] Indeed, the Chair of the European Data Protection Board issued guidance on March 16, 2020, in which he stated that "Data protection rules (such as GDPR) do not hinder measures taken in the fight against the coronavirus pandemic. However, I would like to underline that, even in these exceptional times, the data controller must ensure the protection of the personal data of the data subjects. Therefore, a number of considerations should be taken into account to guarantee the lawful processing of personal data." European Data Protection Board, *Statement by the EDPB Chair on the Processing of Personal Data in the Context of the COVID-19 Outbreak* (Mar. 16, 2020), *available at* https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en.

[33] *See* Compl. for Permanent Injunction & Other Equitable Relief, *FTC v. LifeLock, Inc., et al.*, 2:10-cv-00530-JJT, (D. Ariz. Mar. 9, 2010).

[34] *LabMD, Inc. v. FTC*, 894 F.3d 1221, 1225 n.8 (11th Cir. 2018).

[35] *Id.*

[36] *Id.* at 1230, 1236-37.

[37] Andrew Smith, *New and Improved FTC Data Security Orders: Better Guidance for Companies, Better Protection for Consumers*, Federal Trade Commission (Jan. 6, 2020), *available at* https://www.ftc.gov/news-events/blogs/business-blog/2020/01/new-improved-ftc-data-security-orders-better-guidance.

[38] CAL. CIV. CODE § 1798.150(a)(1).

[39] *Id.*

[40] B. 134, Gen. Assemb., Feb. Sess. (Conn. 2020), § 12.

[41] S.B. 2330, 101st Gen. Assemb. (Ill. 2019 & 2020), §40(a).

[42] S.B. 120, 191st Sess. (Mass. 2019), § 9.

[43] H.B. 3096, 91st Leg. (Minn. 2019-2020), § 9.

[44] H.B. 1680-FN, Reg. Sess. (N.H. 2020), 359-R:11.

[45] S.B. 5642, Leg. Sess. (N.Y. 2019-2020), § 1109(3).

[46] H.B. 473, Gen. Assemb. (Va. 2020), § 59.1-579.

[47] *See e.g., Attias v. CareFirst*, 365 F. Supp. 3d 1 (D.D.C. 2019).

[48] *See e.g.*, *id.*; *In re Equifax,* 362 F. Supp. 3d 1295 (N.D. Ga. 2019); *Enslin v. Coca-Cola Co.*, 136 F. Supp. 3d 654 (E.D. Pa. 2015).

[49] *See, e.g., Attias*, 365 F. Supp. 3d 1 (dismissing breach of contract, negligence, negligence per se, fraud, constructive fraud, breach of duty of confidentiality, unjust enrichment claims, and various statutory claims based on inability to show injury); *Carlsen v. GameStop, Inc.*, 112 F. Supp. 3d 855 (D. Minn. 2015); *Storm v. Paytime, Inc.*, 90 F. Supp. 3d 359, 368 (M.D. Pa. 2015) ("Plaintiffs have not alleged that harm to their privacy interest is actual or imminent."); *In re Linkedin User Privacy Litig.*, 932 F. Supp. 2d 1089 (N.D. Cal. 2013) (dismissed due to lack of standing); *In re Barnes & Noble Pin Pad*, No. 12-cv-8617, 2013 U.S. Dist. LEXIS 125730 (N.D. Ill. Sep. 3, 2013) (same); *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046 (E.D. Mo. 2009) (same).

[50] *See In re Marriott Int'l, Inc.*, No. MDL No. 19-md-2879, 2020 U.S. Dist. LEXIS 30435, at *152 (D. Md. Feb. 21, 2020); *see also In re Target Corp. Customer Data Sec. Breach Litig.,* 66 F. Supp. 3d 1154, 1159 (D. Minn. 2014) ("Plaintiffs have alleged injury . . . including unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees.").

[51] *Marriott*, 2020 U.S. Dist. LEXIS 30435, at *45-46.

[52] *Id.* at *78-81.

[53] Complaint, *Delta Air Lines, Inc. v. [24]7.AI, Inc., et al.*, Civ. Action No. 1:19-cv-7430 (S.D.N.Y. Aug. 9, 2019).

[54] *See, e.g., Cmty. Bank of Trenton v. Schnuck Mkts. Inc.*, 887 F.3d 803 (7th Cir. 2018).

[55] *Id.* at 814.

[56] *Id.* (citing *Annett Holdings, Inc. v. Kum & Go, L.C.*, 801 N.W.2d 499, 504 (Iowa 2011)).

[57] *Equifax*, 362 F. Supp. 3d 1295.

[58] *Sgarlata v. PayPal Holdings, Inc.*, No. 17-cv-06956-EMC, 2018 U.S. Dist. LEXIS 210564 (N.D. Cal. Dec. 13, 2018).

[59] Complaint, *Shah*, *et al.* v. *Chegg*, *et al.*, Civ. Action No. 3:18-cv-05956 (N.D. Cal. Aug. 27, 2018).

[60] *Marriott*, 2020 U.S. Dist. LEXIS 30435.

[61] Securities and Exchange Commission, Press Release, *SEC Provides Conditional Regulatory Relief and Assistance for Companies Affected by the Coronavirus Disease 2019 (COVID-19)*, *available at* **https://www.sec.gov/news/press-release/2020-53**.

[62] *See* Andrea Arias, *The NIST Cybersecurity Framework and the FTC* (Aug. 31, 2016), *available at* **https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc**.

[63] *Patco Constr. Co. v. People's United Bank*, 684 F.3d 197, 212-13 (1st Cir. 2012); *cf. Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, 3:16-cv-00014-GPC-BLM, 2016 U.S. Dist. LEXIS 152838, at *32 (Nov. 3, 2016) (denying motion to dismiss in part on the grounds that plaintiff's pleaded sufficient facts by alleging that defendant "failed to 'appropriately encrypt customer' data in its possession'" and that defendant's "'security systems and protocols' should have been designed, implemented, maintained, and tested 'consistent with industry standards and requirements.'") (citing other cases).