NYCJI
New York Civil Justice Institute

2020

The New York Civil Justice Institute

Authored by: Katherine Hobday

Data Privacy in the Age of COVID-19

Contents

EXECUTIVE SUMMARY

Over the past few years, a handful of states have passed data privacy legislation. Many of these new laws included a controversial private right of action which took the enforcement of data privacy out of the hand of elected officials and into the hands of private attorneys. Incentivized by multi-million-dollar payouts, several lawsuits were quickly filed. This study explores several topics, including:

- The structure data privacy legislation in several states and the fallout in those states which passed such legislation
- The questionable public value of data privacy class action lawsuits and corresponding public value of a private right of action
- The extraordinary risks to data privacy during the COVID-19 pandemic and how data privacy lawsuits are ill-equipped to address those risks
- How businesses and educational institutions can protect employee, student, and consumer data in our new work-from-home world

Most states considering data privacy legislation did so well before the onset of the COVID-19 pandemic. This study is the first known comprehensive review of the impact of COVID-19 on data privacy and data privacy legislation.

INTRODUCTION

Businesses and Consumers have become increasingly dependent on the internet in recent years, but the COVID-19 outbreak has changed our use of the internet forever. Businesses have closed their physical locations, students are now completing their courses online, and 62% of the workforce is working remotely as of April 2020.[i] Many analysts suspect this is a permanent change and that many business will continue to operate more remotely after the pandemic. According to a March 2020 survey of company CFO's, 74% believe that 5% of their employees that were previously office employees will permanently work from home even after COVID-19 restrictions are lifted.[ii]

A recent study by the Connected Commerce Council and Google found that nearly three–fourths of New York Small Businesses 71% increased their use of digital tools during COVID–19, and most 54% intend to increase their use of digital tools post–COVID–19.[iii]

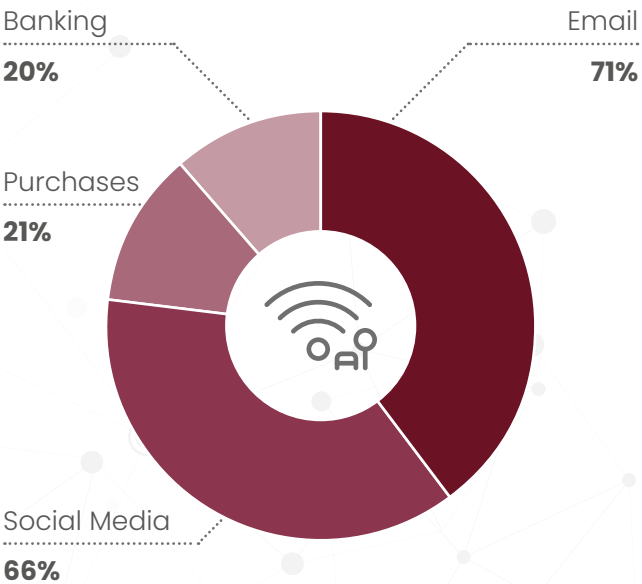
This new post-COVID-19 reality creates significant security challenges for businesses, non-profits, and public institutions. Most Americans do not have the security (firewalls, etc.) on their home computers to protect the information being sent back and forth. Communications between students and schools, employees to employers or consumers to businesses are far more vulnerable when those communications are sent from an unprotected home computer rather than via a professional network with firewalls, encryption, or other security protocols.[iv] These innumerable security challenges potentially create a similarly unknowable amount of liabilities. The available security solutions raise a whole new number of privacy concerns.

AMERICAN INTERNET USAGE

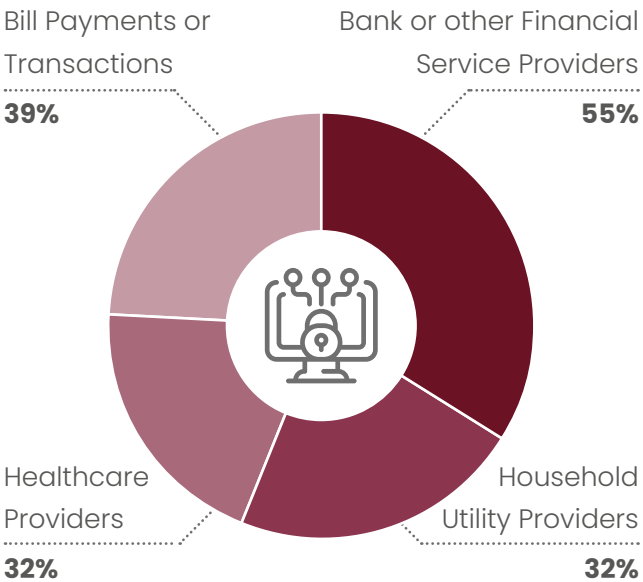
The number of Americans utilizing the internet has steadily increased in the last decade.[v] People use the internet in their homes, offices, classrooms, or in public spaces on public Wi-Fi systems. They use the internet for banking, shopping, research, social media, email communications, work, and school. With this usage comes the exchange of information across platforms and networks that may not be secure. This is especially an issue now that COVID-19 has forced so many people to work from home and take classes remotely. Kon Leong, CEO of ZL technologies warned at the onset of COVID-19, "companies must pay special attention to security. They must add extra protection above the network layer, particularly in the application to and content layers, to watch out for internal threats."[vi]

A study conducted by MariaDB found that 40% of companies were accelerating their adoption of a cloud-based network due to COVID-19. However, 73% of respondents told researchers that security was their biggest concern in adopting the cloud-based model.[vii]

54% of Internet Users Use Public Wi-Fi



American's with Online Accounts Containing Sensitive Data



DATA PRIVACY

For an individual, data privacy is primarily personal information like, your banking information or social security number.[viii]

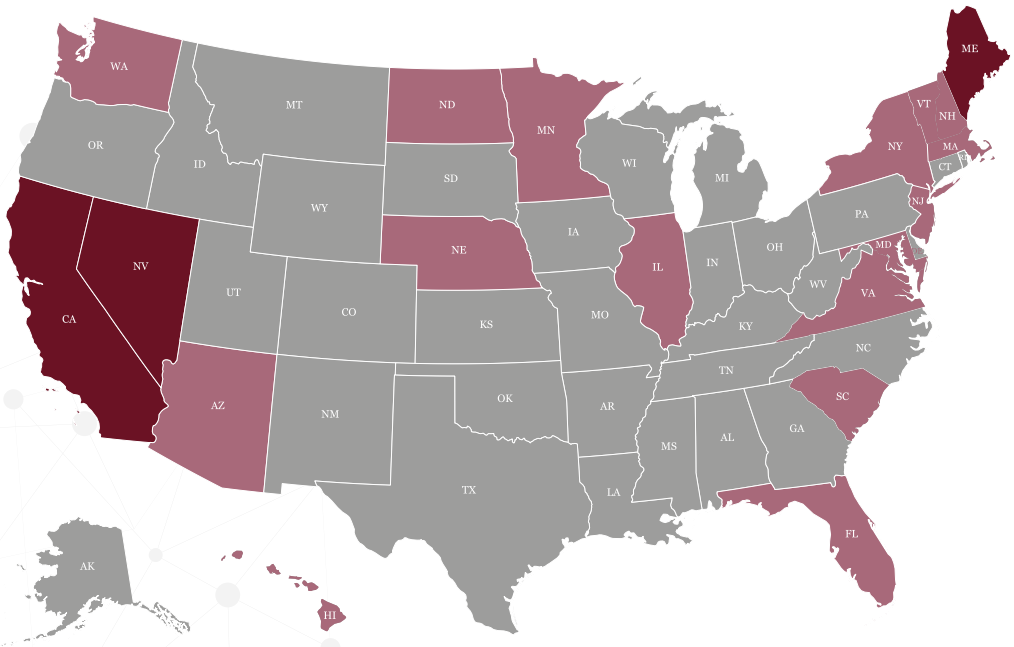
For businesses, data privacy is not only about protecting employees and consumers, but it also involves internal or proprietary information like financial reports, customer information, or research and development data.[ix] Many schools and businesses became instantly more vulnerable to data breaches because they did not have the same level of security on their employees' home computers than they had on the computers in the school or business.[x]

As employers start to catch up to this new reality, trying to keep data secure presents a whole new swath of ethical issues. How do they continue to monitor and oversee their employees without overstepping privacy boundaries? NPR reported that one New York-based E-commerce company asked their employees to download software on their home computers that would record all of their mouse-clicks and key strokes, as well as downloading an app for their phones that would monitor their locations during work hours. Employers argue that they are entitled to a way to monitor the work efforts of their employees in this unprecedented time. Their actions are not illegal but raise serious ethical concerns. [xi] Employers are being forced to balance the importance of privacy of their customers versus their employees.

US States with Introduced / Passed Data Privacy Legislation as of April 2020

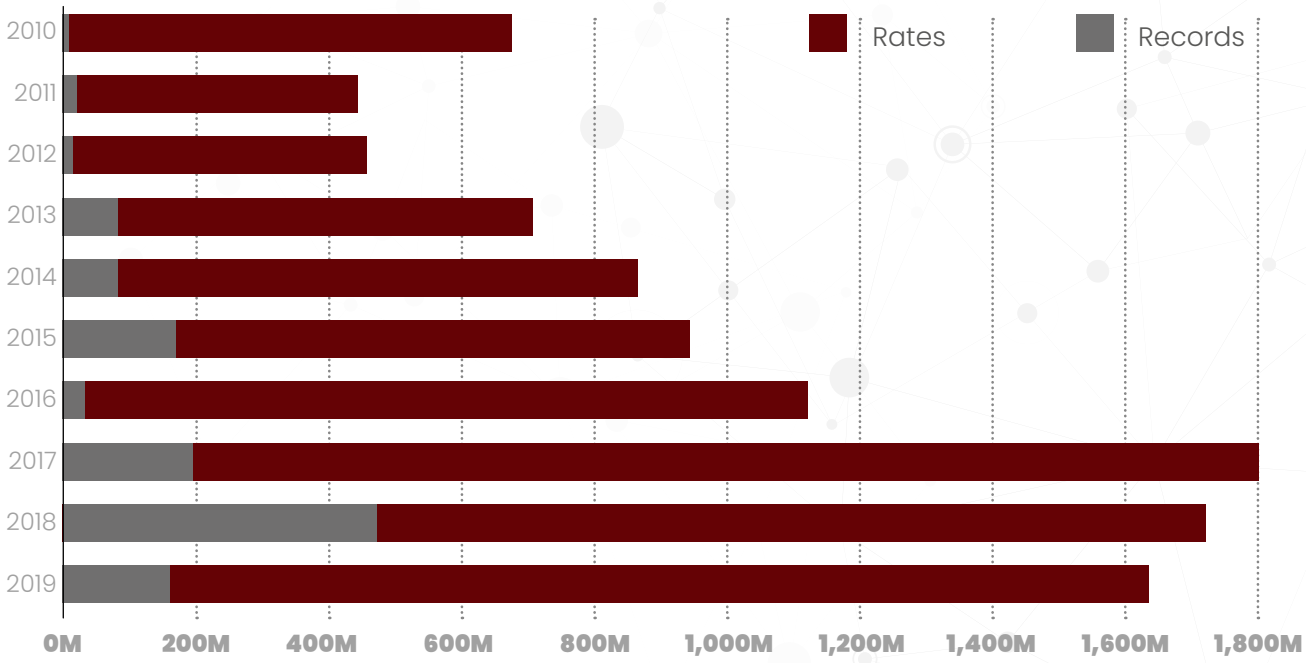
Passed

Introduced



Data Privacy Breaches in the United States

Data Privacy Breach Rates/Records Accessed in Millions



Data breaches occur when a cybercriminal infiltrates, or "hacks," an information system, and steals confidential information. People often imagine that data breaches are perpetrated by a hacker accessing a computer or network to steal local files or by bypassing network security remotely. The reality is often more mundane: many data breaches are the result of human error or intentional corruption.[xii] According to a recent Deloitte Consumer data privacy study, one in three people polled has had their data compromised. [xiii] The most common types of data breaches include:

- **Malware** – a virus used to interrupt, or gain access to unauthorized servers, computers, or network.
- **Phishing emails**- these emails are targeted to entice an individual to click an unsecure link, making their personal information vulnerable. Google's Threat Analysis team recently reported that they have discovered 18 million malware and phishing Gmail messages per day related to COVID-19.[xiv] New phishing attacks have been uncovered across many communication platforms since the onset of COVID-19: Skype, Zoom, WhatsApp, Google Hangouts, and Google Classroom. [xv]

The **COVID-19 pandemic** has left employers with **few ways to monitor** or oversee their employee's actions

- **Password attacks** – a hacker will use multiple attempts to gain access to personal information by trying passwords to a network based on public information.[xvi]
- **Ransomware** – used by cybercriminals, or 'hackers' to gain access to a network. Once the hackers have gained access to the network, they take control over it and lock it from use by its owners.
- **Employee error** – an employee may make an unintentional error such as sending a bulk email that was not intended to be a bulk email, sending information to people who should not have access to it.
- **Malicious employee** – an employee may also intentionally steal private data for revenge purposes or for financial gain.[xvii] COVID-19 has made the malicious employee a growing problem.

Nearly all the above types of data breaches are more likely with employees working from home. The COVID-19 pandemic has left employers with few ways to monitor or oversee their employee's actions.[xviii] Further, the employees themselves may be more at risk of inadvertently causing a data breach as phishing scams and malware are more likely to penetrate a home network.

Working remotely from home computers also presents a breach timing issue. William Denny, Data Privacy and Security Partner for Potter Anderson & Corron, warns that "If you are relying on an employee to detect a breach, rather than network monitoring systems it may take longer to discover a breach. It may impact the compliance with data breach disclosure laws because some of those laws require notification to regulators within a very short time frame."[xix]

Timing is also an issue when an employee is unwilling to provide access to their personal computer and the data contained within it. Daniel Pepper, Partner at Baker & Hostetler pointed to the fact that this is a new problem that lawyers are facing in the face of COVID-19 data breach lawsuits. "Previously, you limit your investigation to within the business premises versus now having to look at the systems or other setups employees may have in their homes".[xx]

PRIVATE RIGHTS OF ACTION

Most states put the enforcement of data privacy in the hands of the Attorney General, as is the case with New York's Stop Hacks and Improve Electronic Data Security Act, otherwise known as the SHIELD Act of 2019. The data privacy laws in California and Illinois differ, in that they provide individual consumers with the ability to sue organizations for violating a law, a concept known as a "private right of action." Under the California Consumer Protection Act, hereinafter CCPA, the private right of action is limited.

Private Rights of Action

ILR. July 2019. Ill Suited: Private Rights of Action and Privacy Claims. Institute for Legal Reform.

Even before the pandemic, private rights of action were controversial. Critics argue that they do not enhance consumer privacy and impose costs on businesses that are not proportionate to harm. It is undeniable that private rights of action will open businesses to more class-action lawsuits for major breaches as well as minor offenses. Policymakers are right to question the value of this additional litigation.[xxi] [xxii]

DO NOT enhance consumer privacy

As New York looked to impose a private right of action for data breaches, Tom Stebbins, Executive Director for The Lawsuit Reform Alliance of New York stated in his testimony to the Senate Standing Committee on Consumer Protection and Internet and Technology, "Data privacy is a critical issue facing New York consumers, however, the current proposal under consideration, and specifically the private right of action, which in effect deputizes private attorneys to act as government enforcers, outlined in S5642, would potentially cause more problems than it will solve."[xxiii]

DO NOT impose costs to businesses that are proportional to harms

James Copeland, Director of Legal Policy for the Manhattan Institute reiterated concerns over private rights of action in his testimony, "I would like to advise the committee and the broader New York state legislature against creating a "private right of action" enforcement mechanism. Rather, any legislation with operative force should limit enforcement to the state attorney general's office and other appropriate executive branch and administrative actors. In general, and particularly in this field, private rights of action have shown a high propensity for abuse—largely functioning to enrich plaintiffs' lawyers and to give little to no compensation to plaintiffs alleging harms from privacy breaches."[xxiv]

DO NOT target the true bad actors

To fully explore the effects of Private rights of action, we will review policy efforts in three states: Illinois, California, and New York State.

ILLINOIS

Patel v. Facebook: **$550M Settlement**

The Illinois Biometric Information Privacy Act ("BIPA") provides a private right of action for statutory violations, including violations of procedural provisions that do not result in any harm. The private rights of action included in this legislation $100-$750 per incident. This has resulted in an influx of lawsuits under the act.[xxv]

Patel v. Facebook was a class-action suit alleging that Facebook's facial recognition technology violates the Illinois Biometric Information Privacy Act ("BIPA"), 740 Ill. Comp.Stat. 14/5(e).[xxvi] In this case, the Plaintiffs' complaint alleged that Facebook subjected them to facial-recognition technology without complying with the Illinois Biometric Information Privacy Act.[xxvii] Each of the Plaintiffs in this case had joined Facebook and uploaded photos of themselves, which Facebook then stored, using facial recognition technology. Facebook then moved to dismiss the case based on a lack of 'concrete injury'. The court ruled in favor of the Plaintiff's for $550M[xxviii] Because the case was settled before judgment, we do not know how courts would count alleged violations. But with BIPA's mandate of payment of up to $5,000 per privacy violation and Facebook's massive user base, a judgment potentially could have ended in the billions of dollars.[xxix]

Rosenbach v. Six Flags Entertainment Corp.: The Court ruled that a plaintiff does not need to allege an **"actual injury or adverse effect"**

In the Illinois Supreme Court case, Rosenbach v. Six Flags Entertainment Corp. Plaintiff Stacy Rosenbach filed a lawsuit against defendant Six Flags, alleging that it violated BIPA's requirements under Section 15(b) when Six Flags took her son's fingerprint as part of his purchase of a season pass to the amusement park.[xxx] The court ruled that a plaintiff does not need to allege an "actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an aggrieved person" entitled to seek injunctive relief and liquidated damages of up to $5,000 per alleged violation of the statute. Again, evidence that the private right of action proves problematic.[xxxi] According to Lawyers employed by the Paul Hastings Law firm, "It is conceivable that the Plaintiffs' bar will be emboldened by Rosenbach to file new class action lawsuits in state courts in Illinois based on mere allegations of technical or facial violations of the statute."[xxxii]

In Dinerstein v. Google. LLC., University of Chicago, University of Chicago Medical Campus, the complaint accused the university of consumer fraud and fraudulent business practices because it never received express consent from patients to disclose medical records to Google. It disclosed information that was used to develop artificial intelligence rather than for research, therefore the complaint also accused Google of unjust enrichment. In a privacy agreement, the university said it would keep medical information confidential and comply with HIPPA regulations. The Plaintiff, Matt Dinerstein believes that he is owed damages by Google in the amount that they would have paid him for the information had they been acting in good faith[xxxiii] Google and the medical center have already made several attempts to dismiss the class action, and have most recently alleged that the plaintiffs' attorney has a conflict of interest as an investor in a competing analytics company[xxxiv] The lawsuit is still pending.

CALIFORNIA

The **CCPA's private right of action** and related **statutory damages provisions** should be taken **seriously** and present many of the same challenge's critics say arise from **traditional private rights of action**

California has had data privacy laws on the record since 2018. One major change in 2020 version of the California Consumer Protection Act (CCPA) is the establishment of a limited but potentially significant private right of action. The term limited is used frequently about the CCPA's private right of action because the original proposed bill contained a "'sweeping' and 'unrestricted' private rights of action, authorizing lawsuits for any potential noncompliance."[xxxv] The Attorney General and a limited group may sue for statutory damages, and will begin enforcing this law on July 1, 2020. Section 1798.150(a)(1) of the CCPA provides that "[a]ny consumer whose nonencrypted and nonredacted personal information . . . is subject to unauthorized access and exfiltration, theft, or disclosure" due to a business's failure to "implement and maintain reasonable security procedures" may commence a civil action to recover either: 1) actual damages; or 2) statutory damages between $100 and $750 per consumer per incident (whichever is greater). The CCPA's private right of action and related statutory damages provisions should be taken seriously and present many of the same challenge's critics say arise from traditional private rights of action. While California's data breach law already provided a private right of action to recover damages, *id.* § 1798.84(b), the CCPA's addition of statutory damages puts companies at risk of more Plaintiffs lawsuits, lawsuits that do not require a showing of actual harm.[xxxvi] The damages Attorney General can recover under the CCPA is a maximum of $7,500 for ill intended breaches and $2,500 for those found lacking in intent.[xxxvii] Since the onset of the COVID-19 outbreak, there has been support of making the CCPA more stringent with regards to private rights of action, restoring the more expansive version contained in the originally proposed 2019 bill..[xxxviii] A proposal to strengthen the CCPA, called the California Privacy Rights Act (CPRA), has qualified to appear on the California ballot in November. "If passed, the CPRA would, among other things, eliminate the 30-day cure period prior to a government enforcement action, create a new California Privacy Protection Agency to enforce the CCPA and CPRA, and provide consumers with additional rights to restrict businesses' use of their sensitive personal information (SPI). SPI would specifically include information germane to COVID-19 mitigation efforts—like precise geolocation and biometric and health information."[xxxix]

Grant Fritchey, a product advocate for Redgate Software stated, "Already dubbed 'CCPA 2.0', the California Privacy Rights Act is being championed by the same campaigning group that forced the introduction of the CCPA and demands a lot more than the CCPA in terms of protecting consumer privacy."[xl]

Largest US Data Breach Settlments

$575 Million
Equifax 2017

$148 Million
Uber 2016

$85 Million
Yahoo 2013

$18.5 Million
Target 2017

$16 Million
Anthem 2016

Since the passage of the CCPA in 2020, there have emerged two types of lawsuits with regards to private rights of action: those that seek damages under the CCPA's limited private rights of action for personal data breaches and those that test the bar that the CCPA has imposed on private rights of action.

Barnes v. Hanna Andersson, LLC, is an example of a case seeking damages under the CCPA's limited private rights of action for personal data breaches. The case is very first data breach class action ever filed with alleged violations of the California Consumer Privacy Act ("CCPA") and was filed in the Northern District of California on February 3, 2020. The allegations in the Barnes complaint relate to a data breach involving consumer data.[xli] Retailer Hanna Andersson's website was hacked, and customers personal data was stolen. Salesforce, the company who hosts Hanna Andersson's website is also named as a Defendant, on the grounds that their software did not do enough to protect consumers personal information. According to Natalie Prescott of the National Law Review, "The *Barnes* complaint, however, does not allege an express cause of action for a violation of the CCPA. Rather the *Barnes* plaintiffs predicate their UCL § 17200 causes of action, in part, on alleged violations of the CCPA. This is a creative procedural mechanism that allows plaintiffs to buttress their privacy claims, as well as to rebut any challenges with respect to standing, namely, that they did not suffer an injury-in-fact that is "concrete and particularized"—as required by the U.S. Supreme Court in *Spokeo, Inc. v. Robins*, 578 U.S. ___ (2016)."[xlii] This case is ongoing.

The Burke v. Clearview AI, Inc., on the other hand, demonstrates the latter type of litigation, by testing the bar that the CCPA has imposed on private rights of action. The case was filed in the Southern District of California on February 27, 2020. The complaint alleges that the CCPA was violated when Clearview collected and sold consumers' personal information without first notifying consumers or obtaining their consent. The Plaintiff's claim that the company illegally stole more than 3 billion images from websites such as Facebook, Twitter, and Google without the consent of users, and then sold the images to third parties.[xliii] On April 15, 2020 this case was transferred to District of Southern District of New York, and remains ongoing. The reason for the transfer of venue was explained in a Motion filed on April 14, 2020, "While Plaintiffs assert specific personal jurisdiction and venue is proper in this Court, pursuant to 28 U.S.C. §1404(b), Plaintiffs do not oppose transfer to the SDNY to serve the interest of justice and the convenience of the courts and the parties. Clearview is headquartered in New York and the individual defendants, Ton-That and Richard Schwartz, reside in New York. Similarly, a substantial amount of conduct giving rise to the alleged unlawful activity in Plaintiffs' FAC emanated from New York." The court ruled in favor of the transfer.[xliv]

NEW YORK

The **Act** amended the state's **data breach notification law**, broadened the information that is subject to **breach notification**, and even **expanded** the very **definition** of **what is considered a breach**

In New York, the Stop Hacks and Improve Electronic Data Security Act, aka the SHIELD Act, was signed into law in July 2019, but went officially into effect in March 2020. The Act amended the state's data breach notification law, broadened the information that is subject to breach notification, and even expanded the very definition of what is considered a breach.[xlv] The new guidelines for what is considered a breach include: financial account information, such as credit card numbers, usernames and emails, biometric information, and protected health information.[xlvi] The SHIELD Act applies to all companies that gather data on New York State residents, not just those conducting business within the state.[xlvii]

The SHIELD Act does not create a private right of action, instead, the "Attorney General may bring an action to enjoin violations of the law and obtain civil penalties".[xlviii]. Damages are based upon whether an infraction is malicious and avoidable or unintended. Unintentional violations are capped at $5,000 whereas violations that are found to be malicious or avoidable start at $5,000 and are capped at $250,000.

In January, a data privacy bill was re-introduced, called the New York Privacy Act which is currently in the Consumer Protections Committee. New York Privacy Act would give New Yorkers the right to sue companies directly over privacy violations, a private right of action. Instead of leaving the authority with the Attorney General. Whereas the, the CCPA has limited the law to companies who gross more than $25 million annually.[xlix] New York Privacy Act has no such limitation. Data privacy is a critical issue facing New York consumers, however, the New York Data Privacy Act, and specifically the private right of action, which in effect deputizes private attorneys to act as government enforcers, would potentially cause more problems than it will solve as we have seen in Illinois and California. Companies, like Facebook have come forth publicly to voice their opinions on the proposed bill. A Facebook Spokesperson said in an interview, "Facebook does have concerns about the New York bill. The company objects to the inclusion of a private right of action, as well as what it says is some overly broad language in the bill regarding data fiduciaries."[l]

COVID-19

With the rapid spread of COVID-19, businesses and educational institutions have been forced to have employees work remotely and students learn from home. Many businesses and schools did not have the luxury of time to address whether or not their data privacy standards were up to speed, especially considering the fact that in many states, these laws have just gone into effect or will be in the near future. The new laws, coupled with the new data challenges of the COVID-19 pandemic, have greatly increased the chance of COVID-related data breach litigation.[li]

Internet based **video calling** or **conferencing** service **increases** since 1/01/2020

32%
Ages 18-29

33%
Ages 30-49

According to the Federal Trade Commission, COVID-19 related data fraud has cost Americans a cumulative $13.4 million dollars, due to the rise in the number of people online at once and distraction from regular routines.[lii]

A report published by Avira states "Cybercriminals took advantage of the vulnerable populations searching for information about the virus; according to a report by Interpol, by the end of March 2020, more than 40,000 high-risk domains with the key words 'COVID' or 'corona' were registered."[liii]

Cyber security expert and CyberScout founder Adam Levin. "People are trying to juggle working from home, homeschooling, applying for unemployment, looking for their stimulus checks. You have enormous vulnerability. Scammers now know that they can use all of these different avenues."[liv]

In California, trade groups and businesses wrote a letter to the Attorney General, Xavier Becerra urging him to delay the enforcement beyond the grace period of July 1, 2020 of the CCPA due to COVID-19. The Attorney General declined, resulting in several lawsuits being filed against popular 'web-based meeting rooms', Zoom and Hangout.[lv]

In the Zoom complaint, filed in federal court in California by a Zoom user, the company is accused of failing to safeguard the personal information of its users. Plaintiff's claim that Zoom disclosed personal user information without adequate notice or authorization to Facebook and possibly other third parties, a violation of the CCPA.

Microsoft reports that it's **group chat** and **collaboration software** use has **spiked** since 1/01/2020

500%

Under the terms of the CCPA, if every one of the 300 million daily active participants on Zoom were to file a class action lawsuit against the platform, Zoom could potentially be held liable for $2.25 trillion dollars in damages.[lvi] Zoom Video Communications net worth as of June 23, 2020 is only $71.32 billion dollars.[lvii]

As a result of this lawsuit, New York Attorney General, Leticia James, wrote a letter to Zoom asking them to inform her, in writing, of their security policies. As of April 2020, the parties had reached an agreement about Zoom's security practices.[lviii] A statement from Attorney General James's website states, "This agreement puts protections in place so that Zoom users have control over their privacy and security, and so that workplaces, schools, religious institutions, and consumers don't have to worry while participating in a video call. As the coronavirus continues to spread across New York State and this nation and we come more accustomed to our new normal, my office will continue to do everything in its power to help our state's residents and give them every tool to continue living their lives."[lix]

In the case against the Houseparty app, *Sweeney v. Life on Air, Inc. Et al,* filed in April 2020, the Plaintiff alleges that the app provided her personal data to third parties without her consent. Like the Zoom lawsuit, this complaint alleges that Facebook was notified whenever a user opened the Houseparty app.[lx]

CONTACT TRACING

Contact tracing, where patients are interviewed about where they have been and who they have seen, recently has been used by public health officials since at least the 1920s. Over the decades, it has been relied upon to help control outbreaks from the flu to Ebola. In response to the COVID-19 pandemic, health officials have utilized modern technology rather than relying solely on in person interviews to stem the spread of this terrible illness.[lxi]

Employers who maintain or have access to **data collected** by contact tracing applications may also be subject to the **increasing data security regulation** at the state level

Contract tracing is now being used throughout the country in an attempt to slow and track COVID-19. This effort has presented its own set of data privacy concerns.[lxii] When getting a call from a contact tracer, employers must find a balance between protecting their work environment from COVID-19 and maintaining data privacy standards set forth by their state. For example, it may be within an employers' rights to request that employees use contract tracing devices on employer-owned phones but not on the personal device of an employee. Further, all contracting tracing requests must be *job related* and a *business necessity* to be admissible, as stated by the Americans With Disabilities Act (ADA) and the Equal Employment Opportunity Commission (EEOC).[lxiii]

According to experts, "Employers who maintain or have access to data collected by contact tracing applications may also be subject to the increasing data security regulation at the state level. For example, under New York's SHIELD Act, certain companies who possess personal information about New York residents are required to develop, implement, and maintain "reasonable safeguards" to protect the "security, confidentiality and integrity" of the collected data."[lxiv]

Senator Kevin Thomas introduced a bill in June of this year "to create ethical guidelines for entities using technology to track, screen, monitor, contact trace, mitigate or respond to the C0VID-19 health emergency." The bill would place strict limits on how health and personal data used in collecting COVID-19 data can be used, how long it can be stored, and who it can be shared with. Unfortunately, the bill also includes a provision that gives the Attorney General the right to "The attorney general may bring an action in the name of the state, or as *parens patriae* on behalf of persons residing in the state, to enforce the provisions of this act. In an action brought by the attorney general, the court may award injunctive relief, including preliminary injunctions, to prevent further violations of and compel compliance with this act; civil penalties up to twenty-five thousand dollars per violation or up to four percent of annual revenue; other

appropriate relief, including restitution, to redress harms to individuals or to mitigate all substantial risk of harm; and any other relief the court determines." lxiii. The bill has passed the Senate and is pending the Governor's action.

According to a report published by Avira, 71% of those surveyed said that would not use contact tracing apps due to digital privacy concerns and 75% reported that they feared that their personal data would not be secure if stored on apps that the government or authorities have access to.[lxv]

With a lack of Federal guidelines in place, the responsibility for contact tracing falls on the states. Many are slow to start, putting together tasks forces to review apps and technology before making decisions to protect the privacy of their constituents. Arkansas, for example, has put together a panel that includes the states Chief Information officer. In Kansas, the state legislature passed emergency legislation prohibiting contact tracing that uses cellphone location data to identify or track individuals.

Personally identifiable information will be **collected** in other ways due to the COVID-19 crisis; virus **testing**, **temperature** taking, video **monitoring** for ensuring **social distancing** and the utilization of **masks**

The Better Business Bureau has suggested that employers who will implement contact tracing technologies prepare responses for questions that their employees may have, including:

- What information do employees receive at the onset about tracking or contact tracing?
- What information do employees receive if there is a suspected case of COVID-19 in the workplace?
- How is the data stored and for how long?
- Who has access to the collected data?
- How is the data being collected used to inform community health decisions?

Julie Brill and Peter Lee, vice-president for research and incubation for Microsoft said in a joint statement, "An updated legal framework placing obligations on businesses that collect and use personal data would help provide the necessary guardrails for companies to know how to protect and respect personal data as they create tools and technologies to address urgent societal needs. Privacy and ethical concerns must be considered as we move forward to use data responsibly to defeat the pandemic," [lxvi]

In a recent survey conducted by W20, a health intelligence data firm, regarding the sharing of their personal health data, "Control over and understanding of those data was highly valued among the respondents. The ability to opt out of data sharing (44%) as well as the receipt of details of how the data is being used (41%) were both highly cited as factors that would increase respondents' personal comfort with tech company-healthcare organization partnerships."[lxvii]

In addition to contact tracing, personally identifiable information will be collected in other ways due to the COVID-19 crisis; virus testing, temperature taking, video monitoring for ensuring social distancing and the utilization of masks.[lxviii]

FEDERAL RESPONSE

Three privacy bills have been introduced at the Federal level as of July 2020 to address COVID-19 and data privacy concerns:

- **The Exposure Notification Privacy Act (ENPA) –** introduced by Senator Maria Cantwell (D), Senator Amy Klobuchar (D) and Senator Bill Cassidy (R).
- **The COIVD-19 Consumer Data Protection Act of 2020 (CCDPA)-** introduced by Senator Roger Wicker (R)
- **The Public Health Emergency Privacy Act (PHEPA)–** introduced by Senator Richard Blumenthal (D) and Senator Mark Warner (D)

All **three** of the **proposed bills** would **regulate collection** and **use** of personal health, geolocation and proxmity for **contact tracing** by requiring employers, educators and other administrators of the tests **receive express consent** from those being tested.

All three of the proposed bills would regulate collection and use of personal health, geolocation and proxmity for contact tracing by requiring employers, educators and other administrators of the tests receive express consent from those being tested. They would also minimize the information being collected and establish privacy policies.

Where they differ most significantly is in their enforcement and preemption provisions. The ENPA is enforced by the Federal Trade Commission, the State Attorney General and existing private rights of actions, whereas the PHEPA is enforced by the Federal Trade Commission, the State Attorney General and a *new* private right of action. The CCDPA is enforced only by the Federal Trade Commission and the State Attorney General.

The ENPA does not "preempt, displace or supplant" state laws whereas the PHEPA adopts reasonable safeguards to "prevent unlawful discrimination on the basis of emergency health data" but does not "preemept or superceded" other federal or state laws. In contrast, the CCDPA "preemepts state laws and regulations".[lxix]

In addition to the bills proposed above, the Senate Committee of Appropriations introduced an Emergency Cornonavirus Stimulus Package in late July. This package would direct $53 million of the new $306 million package to the Department of Homeland Seciruty Cybersecurity asnd Infrastructure Security Agency for the protection of COVID-19 data and research. The Public Health Emergency Privacy Act (PHEPA) may be included in this package. If included, PHEPA would be a temporary measure, ending once COIVID-19 was no longer considered a public emergency.[lxx]

Employers and Educational institutes would have to educate themselves on these new guidelines, should any of them pass

RECOMMENDATIONS

Employers who maintain or have access to **data collected** by contact tracing applications may also be subject to the **increasing data security regulation** at the state level

There is no doubt that the COVID 19 outbreak has changed the landscape of our use of the internet forever. Businesses have been forced to close their physical locations, students are now completing their courses online, and much of the workforce is now working remotely from home. Legislative solutions and guidelines must be put in place to address this changing landscape.

Current data privacy legislation has left businesses open and vulnerable to lawsuits due to private rights of action and the lack of reasonable damage caps, while doing nothing to improve the safety of consumer privacy. Businesses and schools should implement clear guidelines that help protect their employees and students. New York State needs to look to the adverse experiences of both California and Illinois with regards to private rights of action before considering new legislation that would allow for the provision.

Zoom's agreement with New York Attorney General Letitia James is a good example of how a videoconferencing or social media company can protect their users and themselves from data breach violations. In the agreement Zoom will now:

- **Be more secure** – Zoom will implement a new data security plan, conduct risk assessments and software reviews. Zoom will also enhance its encryption protocols.
- **Enhanced privacy controls** – Zoom will enhance privacy controls for free accounts as well as kindergarten – through 12th grade education accounts.
- **Protect users from abuse** – Zoom will maintain reasonable procedures to enable users to report abuse and update its policies to include abuse based on race, religion, ethnicity national origin, gender, or sexual orientation.[lxxi]

Companies and **businesses** large or small should also **set systems in place** to **protect consumer data** as well as inhouse data.

Consumers, employees, and students can also do more to protect themselves and their employers and institutions by:

- **Being wary of scams** – the COVID-19 crisis led to a quick shift in working from home which cybercriminals or hackers see as an opportunity to steal vulnerable information.
- **Using stronger passwords** – make sure passwords are strong and use different passwords
- **Multifactor authentication** – one of the most effective controls. Using multiple layered authentications may seem tedious but it makes it much harder to access private data.
- **Updating devices and software** – updates are often developed for security reasons or to repair security glitches
- **Using trusted wi-fi** – do not conduct work, school health or financial related business on public networks.
- **Securing your devices** – do not allow others unnecessary access to your devices[lxxii]

Companies and businesses large or small should also set systems in place to protect consumer data as well as inhouse data. They can implement several measures to attain a higher level of data safety:

- **Establishing a data privacy and security person or team** – this person can be hired, or in-house to implement and maintain a plan of action regarding data security and privacy. Provide regular training for this individual as cybersecurity is an issue that is always changing. Communication is essential between this team or individual and employers.
- **Assess the new work environment** – Are employees using personal devices to perform work duties? Put multifactor authentication into place, provide employees with security training and current anti-virus protection.
- **Adjust policies and procedures** – create new procedures or strategies to address and discovered or perceived risks. Use the NIST Cybersecurity Framework: Identify, Protect, Detect, Respond framework.
- **Research** - The Cybersecurity and Infrastructure Security Agency, which is part of the Department of Homeland Security also has detailed advice available on their website: https://www.cisa.gov/

CONCLUSION

Based on the experiences of states with Data Privacy legislation, as well as a review of all the data privacy lawsuits that legislation unleashed, several key takeaways become clear:

1. Private rights of action are very profitable for lawyers but offer little value to either plaintiffs or the public. Not only do plaintiffs generally secure little to no money, but the cases often center around no-injury violations with limited public benefit. Indeed, a proliferation of hundred-million-dollar class action lawsuits against in-state businesses for statutory violations, rather than actual damages or harm, could have a detrimental effect.

2. The COVID-19 pandemic has dramatically increased the number of students and employees working from home, and therefore massively increased the risks to data privacy as more communication happens over unsecured networks. Most data privacy legislation was not equipped to handle this new reality.

3. States looking to pass data privacy legislation must look to tailor their legislation to ensure that violations focus on actual harm. Legislation focused on stringent or prescriptive statutes, rather than the effect on consumers, can lead to unnecessary sanctions, and in the states' where there is a private right of action, opportunistic lawsuits.

The New York Civil Justice Institute is a non-partisan nonprofit research organization committed to providing objective analysis and solutions to issues affecting the integrity, equality, and fundamental fairness of New York's Civil Justice System.

NYCJI's mission is to advance understanding of civil justice issues. This is achieved by partnering with academic institutions to produce objective, empirical research. Our primary focus is on areas in which current academic research is limited or nonexistent.

The New York civil justice Institute is a privately funded 501(c)(3) nonprofit organization and is not affiliated with any academic or educational institution.

CLOSING NOTES

i Hickman, Adam, PhD. Saad, Lydia. May 2020. *Reviewing Remote Work in the U.S. Under COVID-19*. Gallup. Available at: https://news.gallup.com/poll/311375/reviewing-remote-work-covid.aspx

ii Kovar. Joseph. April 2020. *Some May Work from Home Permanently After COVID-19: Gartner*. CRN. Available at: https://www.crn.com/news/running-your-business/some-may-work-from-home-permanently-after-covid-19-gartner

iii Connected Commerce Council & Google. September 2020. *U.S. Small Businesses Find a Digital Security Net During COVID-19. Digitally Driven.* Available at: https://connectedcouncil.org/wp-content/uploads/2020/09/Digitally-Driven-Report.pdf

iv IBM Staff. June 2020. *IBM Security Study Finds Employees New to Working from Home Pose Security Risk*. Cision PR Newswire. Available at: https://www.prnewswire.com/news-releases/ibm-security-study-finds-employees-new-to-working-from-home-pose-security-risk-301080534.html

v Pew Staff. June 2019. *Internet/ Broadband Fact Sheet*. Pew Research Center: Internet and Technology. Available at: https://www.pewresearch.org/internet/fact-sheet/internet-broadband/

vi Stone, Henry. Tribune Byte. May 2020. *The COVID-19 Pandemic may have Accelerated Cloud Adoption*. Available at: https://www.tribunebyte.com/the-covid-19-pandemic-may-have-accelerated-cloud-adoption/

vii Johnson, Shane. MariaDB. June 2020. *Survey Reveals COVID-19 Driving Cloud Adoption*. Available at: https://mariadb.com/resources/blog/survey-reveals-covid-19-driving-cloud-adoption/

viii *What is Data Privacy and Why is it Important?* Written for NortonLifeLock. Available at: https://www.lifelock.com/learn-identity-theft-resources-what-is-data-privacy-and-why-is-it-important.html

ix *What is Data Privacy and Why is it Important?* Written for NortonLifeLock. Available at: https://www.lifelock.com/learn-identity-theft-resources-what-is-data-privacy-and-why-is-it-important.html

x IBM Staff. June 2020. *IBM Security Study Finds Employees New to Working from Home Pose Security Risk*. Cision PR Newswire. Available at: https://www.prnewswire.com/news-releases/ibm-security-study-finds-employees-new-to-working-from-home-pose-security-risk-301080534.html

xi Allyn, Bobby. May 2020. *Your Boss is Watching You: Work-From-Home Boom Leads to More Surveillance*. NPR. Available at: https://www.npr.org/2020/05/13/854014403/your-boss-is-watching-you-work-from-home-boom-leads-to-more-surveillance

xii *Data Breaches 101: How They Happen, What Gets Stolen, and Where It All Goes?* August 2018. Trend Micro. Available at: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101

xiii Abssy, Mark. Hawskins, Lenore Elle. Versace, Chris. August 2020. *Cybersecurity and Privacy Concerns Fuel Raft of New Regulations*. Nasdaq, Cybersecurity. Available at: https://www.nasdaq.com/articles/cybersecurity-and-privacy-concerns-fuel-raft-of-new-regulations-2020-08-11

xiv Huntley, Shane. April 2020. *Findings on COVID-19 and Online Security Threats*. Google Threat Analysis. Available at: https://www.blog.google/technology/safety-security/threat-analysis-group/findings-covid-19-and-online-security-threats/

xv Stevens, Gary. Street Fight. May 2020. *Using Zoom During COVID-19 Lockdown Exposes Users to New Data and Privacy Cyberattacks.* Available at: https://gritdaily.com/using-zoom-during-covid-19-lockdown-exposes-users-to-new-data-and-privacy-cyberattacks/

xvi *Data Breaches and Types of Data Breaches*. January 2019. Infoguard Cyber Security. Available at: https://www.infoguardsecurity.com/data-breaches-and-types-of-data-breaches/

xvii Irwin, Luke. June 2019. How Do Data Breaches Happen? Understanding Your Organization's Biggest Threats. IT Governance. Available at: https://www.itgovernance.co.uk/blog/understanding-the-different-types-of-data-breaches

xviii April 2020. *Risk Management, Insider Threats and Security Leaders in the Age of COVID-19*. Security Magazine. Available at: https://www.securitymagazine.com/articles/92194-risk-management-insider-threats-and-security-leaders-in-the-age-of-covid-19

xix Hudgins, Victoria. August 2020. *Prepare for Slower Data Breach Detection, Higher Costs with Remote Workforce*. Legal Tech News. Available at: https://www.law.com/legaltechnews/2020/08/10/prepare-for-slower-data-breach-detection-higher-costs-with-remote-workforce/

xx Hudgins, Victoria. August 2020. *Prepare for Slower Data Breach Detection, Higher Costs with Remote Workforce*. Legal Tech News. Available at: https://www.law.com/legaltechnews/2020/08/10/prepare-for-slower-data-breach-detection-higher-costs-with-remote-workforce/

xxi *See Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, ¶¶ 20–22, 40.

xxii *See Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, ¶¶ 20–22, 40.

xxiii Available at: https://lrany.org/wp-content/uploads/2019/11/3.pdf

xxiv Available at: https://lrany.org/wp-content/uploads/2019/11/3.pdf

xxv *See Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, ¶¶ 20–22, 40.

xxvi Pester, Rachel. February 2020. *Patel v. Facebook: Facebook Settles Illinois Biometric Information Privacy Act ("BIPA") Violation Suit. Jolt Digest. Available at:* https://jolt.law.harvard.edu/digest/patel-v-facebook-facebook-settles-illinois-biometric-information-privacy-act-bipa-violation-suit

xxvii Patel v. Facebook, Inc., No. 18-15982 (9th Cir. 2019)

xxviii Huddleston, Jennifer. *Three Lessons from BIPA for Data Privacy Legislation*. February 02, 2020. The Hill. Available at: https://thehill.com/opinion/cybersecurity/481709-three-lessons-from-bipa-for-data-privacy-legislation

xxix Pester, Rachel. February 2020. *Patel v. Facebook: Facebook Settles Illinois Biometric Information Privacy Act ("BIPA") Violation Suit. Jolt Digest. Available at:* https://jolt.law.harvard.edu/digest/patel-v-facebook-facebook-settles-illinois-biometric-information-privacy-act-bipa-violation-suit

xxx Kim, Tae. *Rosenbach v. Six Flags: Illinois Supreme Court Interprets Illinois Biometric Privacy Law.* February 2019. Jolt Digest. Available at: https://jolt.law.harvard.edu/digest/rosenbach-v-six-flags-illinois-supreme-court-interprets-illinois-biometric-privacy-law

xxxi Hayes, Michael D., Mayette, Anne M., Tomaso, Robert J. Overview of Recent Decisions Interpreting the Illinois Biometric Information Privacy Act. October 12, 2019. Husch Blackwell, LLP. Available at: https://www.huschblackwell.com/newsandinsights/overview-of-recent-decisions-interpreting-the-illinois-biometric-information-privacy-act

xxxii Dayanim, Behn. Et al. February 2019. Rosenbach v. Six Flags Entertainment Corporation: The Illinois Supreme Court Clarifies BIPA's "Aggrieved" Pleading Requirement. Paul Hastings. Available at: https://www.paulhastings.com/publication-items/details/?id=3b81716c-2334-6428-811c-ff00004cbded

xxxiii Wakabayashi, Daisuke. Google and the University of Chicago Are Sued Over Data Sharing. June 26, 2019. The New York Times. Available at: https://www.nytimes.com/2019/06/26/technology/google-university-chicago-data-sharing-lawsuit.html

xxxiv Daniel R. Stoller. November 2019. *U of Chicago Seeks Health Suit End on Alleged Attorney Conflict*, Bloomberg Law. Available at: https://news.bloomberglaw.com/privacy-and-data-security/u-of-chicago-seeks-health-suit-end-on- alleged-attorney-conflict.

xxxv 2019/2020. Judicial Hellholes Report. American Tort Reform Association. Available at: https://www.judicialhellholes.org/wp-content/uploads/2019/12/ATRA_JH19_layout_FINAL.pdf

xxxvi Schenker, Jonathan. Et al. August 2019. *A Closer Look at the CCPA's Private Right of Action and Statutory Damages.* Patterson Belknap Law Blog. Available at: https://www.pbwt.com/data-security-law-blog/a-closer-look-at-the-ccpas-private-right-of-action-and-statutory-damages

xxxvii Furneaux, Alison. *What is the CCPA and Who Must Comply? The California Consumer Privacy Act Explained.* August 2019. Security boulevard. Available at: https://securityboulevard.com/2019/08/what-is-the-ccpa-and-who-must-comply-the-california-consumer-privacy-act-explained/

xxxviii April 2020. *Cornoavirus and CCPA Compliance*. Justia. Available at: https://www.justia.com/covid-19/business-assistance-during-the-coronavirus-pandemic/coronavirus-and-ccpa-compliance/

xxxix Polidora, Roxane A. Et al. July 2020. *New Privacy Laws in California and New York are on a Collision Course with the COVID-19 Technology Boom*. Available at: https://www.pillsburylaw.com/en/news-and-insights/ccpa-ny-shield-privacy-covid-19.html

xl Bennett, Rory. Information Age. March 2020. What to Expect if the New York Privacy Act is Enacted, Following the Privacy Regulation Boom of GDPR and CCPA. Available at: https://www.information-age.com/what-to-expect-new-york-privacy-act-enacted-123488202/

xli Copeland, Jessica. Redmond, Hannah. *Let the Litigation Begin! California Residents Already Filing Enforcement Actions Under the CCPA*. March 20, 2020. Bons, Schoeneck & King, PLLC. Available at: https://www.jdsupra.com/legalnews/let-the-litigation-begin-california-35462/

xlii Prescott, Natalie, A. February 2020. *The First Wave of CCPA Allegations Makes Its Way Into a New Data Breach Class Action Against Salesforce and Hanna Andersson.* Mintz Privacy and Cybersecurity Viewpoints. Available at: https://www.natlawreview.com/article/first-wave-ccpa-allegations-makes-its-way-new-data-breach-class-action-against

xliii Copeland, Jessica. Redmond, Hannah. *Let the Litigation Begin! California Residents Already Filing Enforcement Actions Under the CCPA*. March 20, 2020. Bons, Schoeneck & King, PLLC. Available at: https://www.jdsupra.com/legalnews/let-the-litigation-begin-california-35462/

xliv Burke *v.* Clearview AI, Inc. (3:20-cv-00370). District Court, S.D. California. JOINT MOTION TO TRANSFER VENUE PURSUANT TO 28 U.S.C. §1404(a). Document 10 Filed 04/14/20 PageID.139 Page 1 of 5. Available at: https://ecf.casd.uscourts.gov/doc1/037115746172 (Paywall)

xlv Brumfield, Cynthia. *New York's SHIELD Act Could Change Companies' Security Practices Nationwide*. March 2020. CSO. Available at: https://www.csoonline.com/article/3533455/new-yorks-shield-act-could-change-companies-security-practices-nationwide.html

xlvi *The SHIELD Act Aims to Improve Data Security in New York*. Schlanger Law Group, LLP. Bolg. Available at: https://consumerprotection.net/blog/shield-act-aims-improve-data-security/

xlvii Ashkenazi, Asaf. August 2020. Forbes Technology Council. *Four Tips for Protecting Apps and Complying with Online Privacy Laws*. Available at: https://www.forbes.com/sites/forbestechcouncil/2020/08/17/four-tips-for-protecting-apps-and-complying-with-online-privacy-laws/#681003f05524

xlviii Lazzarotti, Joseph J. July 2020. *New York SHIELD Act Facts*. The New York Law Review. Volume X, Number 203. Available at: https://www.natlawreview.com/print/article/new-york-shield-act-faqs

xlix Lapowsky, Issie. *New York's Privacy Bill Is Even Bolder Than California's.* June 4, 2019. Wired. Available at: https://www.wired.com/story/new-york-privacy-act-bolder/

l Lapowsky, Issie. *New York's Privacy Bill Is Even Bolder Than California's.* June 4, 2019. Wired. Available at: https://www.wired.com/story/new-york-privacy-act-bolder/

li Meyer, Catherine. Toto, Carolyn. April 2020. *COVID-19, COPPA and the CCPA: Educators Face Privacy Questions as Students Move to Remote Learning.*. JDSupra. Available at: https://www.jdsupra.com/legalnews/covid-19-coppa-and-the-ccpa-educators-42118/

lii Solomon, Katherine. July 2020. Yahoo Life. *How Online Shoppers Have Lost Millions to Fraud During the Pandemic: You Have Enormous Vulnerability*. Available at: https://www.yahoo.com/lifestyle/online-shopping-cyber-security-tools-190000460.html

liii Avira. June 2020. *Majority of Americans Say They Won't Use COVID Contact Tracing Apps*. Avira. Available at: https://www.avira.com/en/covid-contact-tracing-app-report

liv Solomon, Katherine.Yahoo Life. July 2020. *How Online Shoppers Have Lost Millions to Fraud During the Pandemic: You Have Enormous Vulnerability*. Available at: https://www.yahoo.com/lifestyle/online-shopping-cyber-security-tools-190000460.html

lv Casale, Elizabeth. Shreve, James. Sosnicki, Luke. *In Wake of COVID-19, California AG Asked to Delay Enforcement of CCPA*. March 2020. Thompson Coburn, LLP.

lvi Fernandez, Ryan. April 2020. *How Many Users Does Zoom Have Exactly? Well, it is Complicated*. Silicon Valley Business Journals. Available at: https://www.bizjournals.com/sanjose/news/2020/04/30/zoom-user-numbers-zm.html. $7,500 damage cap included in the CCPA multiplied by 300 million daily active Zoom participants.

lvii Zacks Investment Research. June 2020. *Zoom Video Communications Net Worth 2019-2020 | ZM.* Macrotrends. Available at: https://www.macrotrends.net/stocks/charts/ZM/zoom-video-communications/net-worth

lviii Wise, Justin. *Zoom Accused in Lawsuit of Improperly Sharing User Data with Facebook*. The Hill. March 31, 2020. Available at: https://thehill.com/policy/technology/490513-zoom-accused-in-lawsuit-of-improperly-sharing-user-data-with-facebook

lix New York State Attorney General's Office. May 2020. *Attorney General James Secures New Protections, Security Safeguards for All Zoom Users.* Available at: https://ag.ny.gov/press-release/2020/attorney-general-james-secures-new-protections-security-safeguards-all-zoom-users#:~:text=Attorney%20General%20James%20Secures%20New%20Protections%2C%20Security%20Safeguards%20for%20All%20Zoom%20Users,Agreement%20Will%20Enhance&text=NEW%20YORK%20%E2%80%93%20New%20York%20Attorney,meeting%20participants%20on%20the%20platform.

lx *S.D. County Woman Sues Video Chat App for Alleged Privacy Breach. April 21, 2020. The Village. Available at:* https://www.villagenews.com/story/2020/04/16/regional/sd-county-woman-sues-video-chat-app-for-alleged-privacy-breach/60406.html

lxi StateScoop. July 2020. *Privacy Concerns Have States Taking it Slow on Contact Tracing Apps.* StateScoop. Available at: https://statescoop.com/contact-tracing-apps-states-privacy/

lxii Brossman, Mark, E., Et al. *Banking Law News. July 2020. Insight: Contact Tracing Apps Can Trigger Workplace, Privacy Concerns.*Available at: https://news.bloomberglaw.com/banking-law/insight-contact-tracing-apps-can-trigger-workplace-privacy-concerns

lxiii Brossman, Mark, E., Et al. *Banking Law News. July 2020. Insight: Contact Tracing Apps Can Trigger Workplace, Privacy Concerns.*Available at: https://news.bloomberglaw.com/banking-law/insight-contact-tracing-apps-can-trigger-workplace-privacy-concerns

lxiv Plutis, Diana. June 2020. *In Their Own Words: American Opinions on COVID-19 Contact-Tracing Apps and Digital Privacy*. Avira. Available at: https://www.avira.com/en/blog/in-their-own-words-american-opinions-on-covid-19-contact-tracing-apps-and-digital-privacy

lxv Avira. June 2020. *The Majority of Americans Say They Won't Use COVID-19 Contact Tracing Apps.* Avira. Available at: https://www.avira.com/en/covid-contact-tracing-app-report

lxvi Roy, Shriya. July 2020. *Work from Home: Cyber Security, Contact-Tracing Apps are Serious Threats. What's the way Forward?* Financial Express. Available at: https://www.financialexpress.com/industry/technology/work-from-home-cyber-security-contact-tracing-apps-are-serious-threats-whats-the-way-forward/2028260/lite/

lxvii Muoio, Dave. August 2020. Mobi Health News. *Privacy-minded Consumers More Likely to Share Health Data if Transparency and Altruistic Use are Guaranteed.* Available at: https://www.mobihealthnews.com/news/privacy-minded-consumers-more-likely-share-health-data-if-transparency-altruistic-use

lxviii Polidora, Roxane A. Et al. July 2020. *New Privacy Laws in California and New York are on a Collision Course with the COVID-19 Technology Boom*. Available at: https://www.pillsburylaw.com/en/news-and-insights/ccpa-ny-shield-privacy-covid-19.html

lxix Gaffney, Jonathan, M. CRS Legal Sidebar. June 2020. *"Tracing Papers": A Comparison of COVID-19 Data Privacy Bills*. Available at: https://crsreports.congress.gov/product/pdf/LSB/LSB10501

lxx Atrakchi, Maya. Lazzarotti, Joseph. August 2020. JD Supra. *Will the Public Health Emergency Privacy Act Make it Into the Next Stimulus Package?* Available at: https://www.jdsupra.com/legalnews/will-the-public-health-emergency-48389/

lxxi New York State Attorney General's Office. May 2020. *Attorney General James Secures New Protections, Security Safeguards for All Zoom Users.* Available at: https://ag.ny.gov/press-release/2020/attorney-general-james-secures-new-protections-security-safeguards-all-zoom-users#:~:text=Attorney%20General%20James%20Secures%20New%20Protections%2C%20Security%20Safeguards%20for%20All%20Zoom%20Users,Agreement%20Will%20Enhance&text=NEW%20YORK%20%E2%80%93%20New%20York%20Attorney,meeting%20participants%20on%20the%20platform

lxxii Australian Cyber Security Center. April 2020. *COVID-19: Cyber Security Tips When Working from Home.* Australian Government. Available at: https://www.cyber.gov.au/acsc/view-all-content/advisories/covid-19-cyber-security-tips-when-working-home#:~:text=Do%20not%20leave%20your%20device,your%20work%20profile%20or%20account.

NYCJI

New York Civil Justice Institute

New York Civil Justice Institute

19 Dove St., Suite 201

Albany, NY 12210

www.nycji.org

khobday@lrany.org

518-512-5265

518-512-5267