IRON MOUNTAIN®

PRIVACY, SECURITY & REGULATORY CONCERNS:

RAPIDLY CHANGING TECHNOLOGY FOOTPRINT IN THE LEGAL INDUSTRY

2020 LAW FIRM INFORMATION GOVERNANCE SYMPOSIUM

CONTENTS

AUTHORS:

AUSTIN ANDERSON
Information Governance Senior Coordinator
Latham & Watkins LLP

MAUREEN A. BABCOCK
Information Protection and Privacy Officer
Snell & Wilmer L.L.P.

GALINA DATSKOVSKY, PH.D., CRM, FAI
CEO
Vaporstream Inc.

MICHELE GOSSMEYER
Global Director, Information
Governance, Risk & Compliance
Dentons

SHARON K. KECK
Paralegal
Rouse Frets White Goss Gentile Rhodes, P.C.

JESSICA MARLETTE, ESQ., CIP
Information Governance Counsel
White & Case LLP

ROBERT WEAVER
Chief Risk & Security Officer
Blank Rome LLP

INTRODUCTION

Mid-March 2020 is when many of us in the legal industry were told to pack up what we needed and start working from home. This included not just attorneys and administrative staff of law firms, but also judges, clerks, bailiffs and others who work in the legal eco-system. Some were more prepared than others for this sudden change. The preparation, as well as our firms' responses to it, impact the risk environment in which we are all working, This paper outlines the privacy, security and regulatory concerns associated with COVID-19, including new threats, vulnerabilities, technology challenges and information governance complexities. We review several of the risks facing courts and law firms and provide recommendations to help address them. We take a deeper dive into contact tracing and provide a checklist of considerations for lawyers to apply when representing clients participating in contact tracing, as well as for law firms considering use of contact tracing apps in their return to office plans.

COURTS

The courts remained (largely) closed for some time as a result of stay-at-home orders tied to the pandemic, though eventually began to conduct business using technology to facilitate virtual hearings without all of the normally required participants being physically present in one location (judge, bailiff, attorneys, parties, etc.). Courts are accustomed to having the final say when making decisions based on facts and precedents, but now must also deal with protecting the integrity of the evidence, proceedings, parties and more in an incredibly fluid and somewhat unpredictable environment. As such, courts have been forced to become creative in their efforts, while ensuring a fair and safe symposium for not only the attendees but for each stage of the trial from voir dire questionnaires/updated jury selections to the verdict.

Implementing new logistics for holding trials virtually has proven effective, though more courts are beginning to hold open jury trials as stay-at-home orders are lifted. Courts have been able to reconfigure existing courtrooms and jury deliberation spaces to assure appropriate social distancing, and the addition of Plexiglas barriers and consistent sanitizing of locations are becoming more standard. As courts continue to mitigate the ongoing risks associated with public gatherings, jury trials are being relocated to locations with lower COVID-19 positive numbers, in addition to utilizing hotels, churches, armories and school gymnasiums.

How courts are handling the new norm also seems to raise new questions about fairness, safety and due process. Judges and court staff are responding to new physical requirements that mandate all participants are masked and requisite headsets worn by lawyers make them look like air traffic controllers. Jury chairs are no longer side-by-side, but six feet apart, and spread across the back or taking up one side of the courtroom. In parallel, they are being forced to acquire knowledge of virtual solutions while protecting the integrity of a hearing. Prior to the pandemic, some would consider troubleshooting information technology outside their job description. Today, that logic no longer applies as judges, clerks and bailiffs are required to resolve issues and become IT techs.

As courts re-open, they are adopting technology solutions to replace in-person proceedings. Video conferencing platforms selected by the courts introduced new security concerns prompting many questions. Are they secure from uninvited guests? How are attendees authenticated? How are oaths administered? How are exhibits presented? What guidelines are needed to identify the acknowledgments of recording the hearings or the retention period required to preserve the recordings and evidence presented during the hearings?

Right now, the nation's courts are weighing constitutional rights with the need for public safety. It is mandatory to utilize a virtual bailiff and designate a staff/technology person to be "on call" for technology issues, in addition to a person assigned to check-in parties as they log on, and monitor issues with the technology.

ADDITIONAL COURTROOM LOGISTICAL CONSIDERATIONS:

- Attorneys are accustomed to entering the bench and huddling with the judge to be outside the "ears" of the juror. This is becoming an issue, as due to the pandemic, huddling is not permitted. Going forward, are the jurors going to have to step out of the room?

- Attorneys depend on the effective process of confrontation with their witnesses, yet masks currently prohibit this. Could this become another violation of our constitutional right? And on the flip side, there is the concept of tampering with a witness in a virtual proceeding using Instant Messaging tools and other electronic communications which are not possible/ permissible during in-person trials.

- Everyone has a constitutional right to a fair jury of their peers. Once civilians start back to work, how can we guarantee the jurors will be a "jury of your peers" with the pandemic and hardship exceptions added to the voir dire questionnaire and process? Who is going to want to miss work once they have finally found a job/employment, and attend a jury trial potentially without compensation? Will the updated process take away our guarantee to a "fair trial"?

- Currently products liability defect defense cases (car seats, etc.) often require jurors to handle and watch functionality of objects and tangible evidence, take field trips to manufacturing plants, and more. Do the modifications we are implementing in our courts violate the principles and associated procedures our country was founded upon?

LAW FIRMS

In addition to courts needing to make creative transitions to keep the wheels of justice turning, law firms around the world were deemed as essential services and had to quickly adjust to find ways to continue to deliver client service. Lawyers are ethically required to be prompt in representing their clients; to continue high levels of service, the adjustments some law firms had to make to leverage new technologies proved trickier than for other firms. Maybe your firm issued laptops with a robust security regimen because you were already mobile-ready. Changing to remote working may not have impacted security all that much. But perhaps your firm did not have secure mobility deployed – or maybe it was deployed to attorneys but not staff. What do they do when told to work from home? The potential for use of technology not controlled by the firm presents a number of security challenges, not the least of which is the duty of preservation of confidentiality and attorney-client privilege. Additionally, in several instances, these drastic changes pushed the limits of the duty of technological competency.

PERSONAL DEVICES AND ACCOUNTS

Users may now be working and storing client files on a personal computer. Does that computer have appropriate, up-to-date anti-virus/anti-malware protections? Or perhaps they are connecting into firm systems via less secure methods such as unprotected RDP (remote desktop protocol) or without consistent levels of multi-factor authentication. Perhaps lawyers or staff use personal email accounts to facilitate some of their work due to convenience, requirements to meet tight deadlines or simply due to lack of technical knowledge. Personal email accounts might be shared with family members, have less secure passwords and/or be more susceptible to compromise by hackers in a phishing attack. Not to mention the manner in which free email services handle data access and content usage for analytics, marketing and service delivery (see Terms of Service/Use below).

Personal mobile devices may not have proper security controls such as screen locks, remote wipe capabilities, containerization and more. In some cases, due to the way messages display on these smaller devices, it can be difficult to identify the markers of a malicious message, such as spoofed email addresses and fraudulent email domains.

What about consumer-grade tools such as WeChat or Dropbox with settings less focused on secure access or privacy protections (again, see usage policies below to better understand what data can be shared and how)?

Additional risks for firms include a personal computer getting a virus and exposing or losing data. Is it better or worse if someone is backing up firm files on home computers to additional locations (e.g., external drives, the cloud)? Apps on uncontrolled mobile devices may access data from mail programs (firm or personal) because users do not fully understand how various apps access other resources on the device. And what rights do users give to these apps (knowingly or unknowingly)? Some apps capture copy and paste clipboard data, browsing and search history, content of messages exchanged in other apps, personal data, contacts, photos and more. It is helpful to provide guidance to your user community and reminders of how to limit data sharing, particularly when firm data is involved.

There is a great deal of media coverage on apps such as TikTok, Facebook or Instagram; use these opportunities to gather key pieces of information and help educate your users around the risks and requirements of proper firm/client data handling involving such apps. And oftentimes, when you share risk tips that help your users not only protect firm data, but also better secure their own personal computing experiences, the information resonates better.

POLICIES AND PROCEDURES

How do these use cases impact client information confidentiality? Privilege? Litigation holds/e-discovery efforts? How do they match up to client outside counsel guidelines or client audit/assessment requirements? If you are not already doing so, it is a good idea to loop in your General Counsel or privacy/risk lawyers to get their views and assistance. It's a good time to review and possibly revise your guidelines and policies.

In remote working scenarios, likely every support department in your firm is trying to get important messages, procedures and updates to your users. Therefore, it can be a difficult balance to effectively communicate security and governance messages to your user community. Plan carefully to provide information in multiple formats such as email, web pages, video snip-its and other methods. You should also work with your support teams (e.g., helpdesks, trainers) to ensure they know where these helpful references can be found; they can be great advocates for directing people to the information at the most valuable times.

THE ENVIRONMENT: DEEPER DIVES ON VARIOUS TYPES OF ATTACKS

Malicious actors know that this sudden move to remote work increases opportunities for them. Many firms provide well-protected capabilities for attorneys to work remotely without compromising security, but many do not. The bad guys expect people to be lax with the rules while they have been working in shorts and slippers for months. Criminals are working hard to test our defenses every day. The industry has seen a rise in phishing and other types of attacks to prey on a perceived likelihood of reduced controls in remote environments. The attacks we are seeing are not necessarily new, but can be more successful with the targeted victims working remotely. Here are the most common attacks:

- *Phishing* is an attack using fake emails that look legitimate in an effort to convince the recipient to click a link leading to a malicious website or launch a malicious attachment.
- Business Email Compromise (BEC) uses similar techniques to phishers in an effort to trick the recipient into doing what the bad actors want. In this case, they simply ask the recipient to do something that the user might usually do as part of their job, rather than clicking on something malicious. This might involve wiring money to an alleged client or vendor. Sometimes an invoice or wire instructions are modified to redirect funds to the criminals.
- Technical Support Scam targets receive a pop-up on the screen, an email, or a phone call in an effort to convince the user there is something wrong with their computer, and they need to allow the technician to access their computer to fix it. If the user is on a corporate computer, hopefully they know not to allow someone outside their IT department to connect. If the user is using a personal computer, they may fall victim, allowing the fraudulent technician to access their computer. If they've used this computer for client work, the client content is now at risk of compromise.

WHY IS THERE MORE RISK DURING REMOTE WORK?

These attacks have been around for a long time. Why is there more risk during remote work? The bad guys are aware of the lifestyle changes that come with remote work, and they tailor their phishing emails to increase their effectiveness.

- Remote work has caused a significant increase in the use of *electronic signature capabilities*, so phishing emails often look like an invitation to sign an important document. Due to increased volumes, people may be less careful about examining a request for validity and fall for a phishing email that they would have questioned before the pandemic.
- The increased amount of *online shopping* while working remotely means increased shipping, which also means increased shipping notice emails. This is a common theme of phishing attacks, and generally increases around various holidays. Again with increased volumes, people may become less diligent about examining each notice.

- Use of home networks and maybe even personal computers while working remotely decrease the likelihood of protections and monitoring that may be on firm-issued computers. If users are on a firm-issued computer connecting to the firm network via VPN, their network traffic is tunneled through the firm infrastructure, where tighter security practices are likely in place. Firm networks often include software and/or devices that monitor traffic and detect what appears to be malicious traffic such as the use of suspicious protocols or users navigating to known malicious sites. If the user on the firm infrastructure gets malicious software on their computer, and this malware is crafty enough to avoid detection by anti-malware on the computer, it will attempt to traverse the network, or reach out to its controller to get further instructions. The network monitoring capabilities in the firm infrastructure can typically detect this activity and sound the alarm. However, if a user is working on their home network only, that network monitoring capability likely does not exist, and the same malicious software may go undetected and be able to cause more damage before it is detected.

- Users on home networks are also subject to the security (or lack) of the other computers on that home network that may not be as secure as firm computers. A user on their home computer may have that computer configured to communicate with other home computers on their home network, such as a computer used by a spouse or child. What if a family member works for another law firm, a client or another organization with conflicting interests to your firm? Additionally, other family members may be more easily duped into clicking on malicious links and getting malicious software on their computer, which can then traverse the unprotected home network to access the user's computer.

- Many people working from home do not have dedicated office space. Their working area might be on the couch, or at the kitchen table while helping a child with school. In these open areas, many homes have home automation tools, such as smart assistant devices, that are always listening for audio commands (e.g., Alexa, Siri). Reports vary on how much of the listening is sent to the cloud and how much might end up being listened to by an employee of the cloud company. Imagine an attorney has a sensitive call with a client while Alexa listens in. Since there is an unanswered question of how this might impact confidentiality and privilege, firms should consider policies that restrict such devices in the remote workspace.

- *Confidential phone calls* at home are a risk from a number of scenarios. Others within listening range (e.g. family, friends, neighbors) are not authorized to hear a client phone call.

Many of the risks we have reviewed are often fraud designed to steal money, rather than specifically looking to obtain confidential information from a firm. However, many types of malware, such as ransomware, imply that information was exposed. These events challenge law firms to consider data breach reporting in the context of legal ethics opinions, data breach laws, regulations and requirements outlined in client outside counsel guidelines.

WHAT TO DO

Here are some key considerations for your risk mitigation plan:

1. Implement multi-factor authentication (MFA).

   With MFA, even if a user's username and password are stolen by phishing, they cannot be used to access email or the firm network because they require something else, such as a hardware token or one-time-password sent to or generated on the user's mobile phone.

2. Keep systems up to date.

   Malicious software relies on taking advantage of vulnerabilities in the software on the computer. Have a process to install software manufacturer updates promptly so that malware written to exploit discovered vulnerabilities is less likely to be successful.

3. Implement network activity detection.

   Firm networks should employ technology that can detect and block potentially malicious network activity such as scanning, lateral movement and contact with malicious sites. There are a number of technologies that can be used in these efforts, such as intrusion detection, intrusion prevention, endpoint detection and response, web security filters and other emerging capabilities. Many of these tools can be configured to detect risks from personal as well as firm-issued devices.

4. Train employees to recognize and avoid scams.

   Many of the attacks noted earlier have tell-tale characteristics. Teach users to recognize traits such as messages:

   - with doctored display names or copy-cat email domains
   - that create a false sense of urgency, compelling the recipient to do something quickly
   - with poor language, typos, or unexpected/mis-matched styles and fonts

   Instill in users that when they receive an email, they ask themselves two questions: 1) do I know this person, and 2) did I expect this person to send me this message with this intent? If the answer to either question is no, they should not open the message. For example, if a client sends Word attachments all the time, but one comes out of the blue urging a rapid response unwarranted by the work, be suspicious. It is helpful to have a resource that users can send suspicious emails to for review as well as tools to safely review.

A LAYERED DEFENSE PLAN, INCLUDING ACTIONS BY YOUR FIRM'S IT/SECURITY TEAM AS WELL AS YOUR END USERS, CAN SIGNIFICANTLY REDUCE THE RISK OF REMOTE WORKING.

5. Ensure procedures are in place for financial transactions.

   Whether executing the transaction or advising one of the parties in a transaction, inform everyone to confirm funds transfer instructions before pulling the trigger, by calling the other party on a known, legitimate phone number.

6. Conduct phishing exercises.

   Even if you inform users how to detect these scams, there is nothing like real life experience to enforce it. Send users phishing emails that you design and follow up with those who click.

7. Encourage and educate employees to maintain their home computers and networks.

   Now that we are working from home, the firm-issued computer is on that home network among personal devices that have various degrees of security. Provide users with information about how to obtain resources that will help them secure their home environments and update their personal computers.

8. Encourage employees to educate their family members about scams.

   Even if users secure their home computers, the biggest vulnerability is the person using the computer. As we mentioned, children can be especially vulnerable, but so can the elderly, and those who aren't tech savvy. Encourage your users to talk to family members about these types of attacks.

9. Share information with other organizations.

   We may be competing with other law firms, but we are also subject to the same global online environment. One person getting scammed provides funding to the criminals that might be scamming you next. Talk with your peers. Share experiences. Provide intel to service providers. Participate in professional information sharing events. We are all in this together!

CONTACT TRACING

Due to global concerns about public health and in an attempt to curb the spread, many countries have seen the introduction of contact tracing apps which alert those who have come into close proximity with someone who has tested positive for COVID-19 that they may have also been infected. There are many privacy implications to such tracing, including maintaining compliance with various state, federal and international privacy laws, ensuring appropriate controls are placed on the collection, secure storage and disposal of the sensitive personal information and the location and movement patterns of the app users. This is truly the age of "big brother watching."

The apps that have been implemented in various jurisdictions differ in how they store information, whether the data collected is being used for other purposes and in how they are designed. While some comply with privacy by design principles, others may infringe on individual privacy rights. As privacy laws and regulations vary by jurisdiction, each state and country has a different tolerance threshold for these contact tracing initiatives including whether consent is required and if data mining is permissible.

There are a plethora of data privacy laws and regulations that must be considered during the pandemic. The EU's General Data Protection Regulation (GDPR) may be one of the most discussed, but many countries and states have implemented or are considering their own data protection laws, such as (California Consumer Privacy Act (CCPA), New York's Stop Hacks and Improve Electronic Data Security (SHIELD) Act, the LGPD in Brazil, Thailand's Personal Data Protection Act (PDPA) and Japan's Act on the Protection of Personal Information (APPI).

Although there is no current comprehensive US federal privacy law comparable to GDPR, employers need to consider potential legal obligations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Americans with Disabilities Act (ADA), Equal Employment Opportunity Commission (EEOC) guidance, the Occupational Safety and Health Administration (OSHA) standards and guidance from the Centers for Disease Control and Prevention (CDC), as well as any relevant state laws. Several data privacy laws have been proposed at the federal level, the most recent of which is the Setting an American Framework to Ensure Data Access, Transparency and Accountability (SAFE DATA) Act, so it is likely only a matter of time before the US has its own national privacy law.

Contact tracing apps are a method that many employers are using, or considering using, to help combat the spread of COVID-19. OSHA's Guidance on Returning to Work states that "where there is no OSHA standard specific to SARSCoV-2, employers have the responsibility to provide a safe and healthful workplace that is free from serious recognized hazards under the General Duty Clause, Section 5(a)(1) of the Occupational Safety and Health (OSH) Act of 1970." Employers exploring the use of contact tracing apps should ensure that the app does not infringe on individual privacy rights; some best practices for contact tracing apps include:

- Follow privacy by design principles
- Obtain consent from the individual for whom the data is being collected
- Minimize the data collected
- Be clear as to the reasons for data collection
- Acknowledge the privacy concerns of the individuals providing the personal information
- Be as transparent as possible as to how that information will be used, the length of time it will be stored and the methods by which it will be secured
- Only use the data for the purpose for which it was collected
- Store the data in a decentralized manner
- Use proximity data rather than geo-location data (e.g. GPS, cellular location) due to the sensitivity of providing exact location or movement
- Ensure proper information security protocols are in place (e.g., encryption)

Use of such apps create many important legal considerations due to the personal nature and sensitivity of the information collected. Even if an employer is not subject to HIPAA rules, any information obtained about an employee's symptoms would need to comply with the ADA by retaining it as a confidential medical record, separate from the personnel file. In New York, the legislature approved Senate Bill S8450C to address data protection for contact tracing. This bill, if signed by the Governor, would require a 30 day retention period after which the data must be expunged or de-identified under §2181(7)(B).

The extent to which employers must protect employees from COVID-19 varies state-to-state and is an ongoing debate, as is the question of whether an individual can prove how they contracted the virus. As such, employers using contact tracing apps need to carefully review and stay up-to-date on OSHA guidance and state laws such as workers' compensation. If there is potential employer liability, the data collected from a contact tracing app may be useful to defend a potential claim, which will create significant challenges for the employer to balance protecting itself while also complying with employees' data privacy rights and retention requirements.

SECURITY

Under normal conditions, applying strong security controls to maintain the privacy and confidentiality of the information gathered during contact tracing would be considered a critical component before application development and not after. With the speed at which the pandemic was spreading and the potentially fatal consequences of infection, functionality necessarily won out over security and privacy concerns. Protecting the collected information is becoming a priority now that the means to collect and interpret contact tracing data has advanced.

The nature of the highly sensitive information being collected and the risks to maintaining its confidentiality call for strong data security standards and frameworks such as those promoted by the International Organization for Standardization ("ISO") or by the National Institute of Standards and Technology ("NIST").

Verifiable data security controls must also be placed within the app's development process and throughout the lifecycle of the collected information. This would also include data calculated or extracted from the combined information provided by the app users, if that information can be attributed to the individual user in any way.

With no consensus to date among employers or agencies as to which app is best, app security protections may not meet the requirements to protect personal information specified under US state, federal or within international privacy laws. In addition to employing the ISO or NIST security standards, organizations with offices in multiple countries should consider benchmarking their privacy controls with the regulations in jurisdictions that have set higher bars for privacy compliance, such as Germany (for EU), China or South Korea (for Asia) or California (for the US). In the US, compliance with HIPAA's security requirements remains an obligation for covered entity employers and their business associates collecting PHI for contact tracing purposes.

As some employers may choose to bypass an app and collect information such as temperature scan or health questionnaire results directly or use a combination of both methods, the same security criteria for storage and retention criteria apply.

With the proliferation of employees working from home, security measures for both physical and electronic data needs to be emphasized with anyone who is processing contact tracing information outside the office. The CDC recommends that "approaches to ensuring confidentiality and data security should also be included in training of staff." This should include maintaining data security in a home environment where communication is taking place while other people and devices may be listening or recording.

DATA MINIMIZATION & ANONYMIZATION

Data minimization refers to the principle of limiting the collection and retention of information to that which is directly relevant and necessary for a specified purpose. For example, contact tracing applications that continue to collect and retain user's data for purposes unrelated to the underlying contact tracing feature would conflict with such data minimization principles. Moreover, much of the success of any contact tracing app relies solely on user adoption. In fact, a study by Oxford University claims that for any contact tracing application to be effective, at least half the total population of the country must use it. As such, any application requesting permission to more data than necessary, such as in the example above, will likely deter users from using the application, mitigating any chance of possible success.

In analyzing how governments and technology organizations have developed existing contact tracing apps, there are a number of key takeaways to ensure the application complies with data minimization core principles, the first of which is transparency. When it comes to the processing of personal data of users, organizations should only process personal data that is needed for specified and explicit purposes outlined in the organization's privacy policy. Additionally, there should be clear notice at time of collection to individuals with respect to the purposes of processing and the retention period for collected data.

SENSITIVE INFORMATION PROVIDED DURING THE CONTACT TRACING PROCESS MUST HAVE THE SAME SECURE COLLECTION, TRANSMISSION, STORAGE AND DESTRUCTION PROTECTIONS AFFORDED ANY PERSONAL INFORMATION THAT CAN BE CONNECTED WITH AN INDIVIDUAL.

Organizations should detail the security and privacy measures they are leveraging in the application's privacy policy in order to ensure their users' data is secure, the purposes for which the data being collected is narrowly tailored, whether they are leveraging anonymization or pseudonymization (enhances privacy by replacing most identifying fields within a data record by one or more artificial identifiers, or pseudonyms) practices to further protect user data and finally the retention period of the data. It is critical that the functions of the application are consistent with the data minimization principles laid out in the organization's privacy policy.

To ensure compliance with data minimization principles, a number of international regulators have released data minimization guidance for organizations looking to develop contact tracing apps. For example, the European Commission published a "toolbox" for organizations in the region developing contact tracing applications in response to COVID-19. In particular, the Commission expressly states that organizations "should process personal data only where adequate, relevant and limited to what is necessary, and should apply appropriate safeguards such as pseudonymization, aggregation, encryption and decentralization." Moreover, the Commission emphasized that while such data collection practices (such as geolocation tracking) are necessary to combatting the COVID-19 crisis, "any such restrictions should, in particular, be temporary, in that they remain strictly limited to what is necessary to combat the crisis and do not continue to exist, without an adequate justification, after the crisis has passed."

In Singapore, the Personal Data Protection Commission released similar guidance for organizations looking to employ a contact tracing application for use in their offices for returning employees. Listed as the first requirement, the Commission emphasizes the importance of ensuring that data minimization is properly employed saying, "personal data that is collected for COVID-19 response measures should not be used or disclosed for any other purposes, unless consent is obtained or it is authorized under the law. In general, organizations should expunge the data when it is no longer needed for the purpose it was collected or any legal or business purposes."

In Germany, the Conference of German Data Protection Authorities ("DSK") which is the body of federal and state Data Protection Authorities ("DPAs") issued a joint recommendation regarding employers' processing of employee personal data in the context of the COVID-19 pandemic. The DSK makes it clear that the pandemic should not infringe on the data minimization rights afforded under the GDPR, saying "the data must be treated confidentially and used exclusively for a specific purpose. After the respective purpose of processing no longer applies (usually at the latest at the end of the pandemic), the data collected must be deleted immediately." Additionally, the DSK states that "consent of data subjects can only be considered as a legal basis for COVID-19 measures if the data subjects are informed about the data processing and can provide consent about the measures voluntarily," further highlighting the importance of providing proper notice to the organization's employees or risk of running afoul with the GDPR.

Finally, the Federal Trade Commission ("FTC") recently released guidance for organizations in the United States looking to collect consumer data related to COVID-19 pandemic. In particular, the FTC addressed the importance of leveraging data minimization principles when collecting such data, stating that organizations that fail to adhere to such principles, such as failing to delete such data once the crisis is over, would likely run afoul of the FTC Act. The guidance further addresses the importance of using the collected data for emergency public health purposes only citing the 2019 Facebook complaint where the FTC brought an action against Facebook alleging the company claimed it "collected users' phone numbers for a consumer-protective security purpose, but used the information for advertising as well."

Collection and storage of information for secondary purposes has been going on for a very long time. As Douglas B. Laney states in his book *Infonomics*, "data monetization is a widespread practice in almost every industry." Law firms can greatly benefit from secondary usage of information as well (see the LFIGS paper on AI). From better pricing of matters, to the reuse of work product, to anticipating case outcomes, secondary use of data is highly important. Extremely large data sets may be analyzed computationally to reveal patterns, trends and associations. For every benefit that can be realized through data mining, there is, however, a pitfall.

For example, banks that track data on customers who change branches can offer other products such as a mortgage or home equity line or remind the customer to move their safety deposit box. Every retail organization, news outlet and social media site collects data and uses it for secondary purposes. To process these vast data collections, AI needs to be applied. Self-learning algorithms often draw conclusions that a human may not have been able to correlate from the data. Such algorithms are already in wide circulation:

- Used in diagnosis since vast collections of medical information can be analyzed
- Optimizing agricultural planting based on previous results in like conditions

However, privacy may be called into question when data is used for alternate reasons.

Since the pandemic began, much has been said and done about contact tracing. The big question is how is that data going to be used for secondary and tertiary purposes? For example, to simply contact trace, the data is only useful for about 2 weeks. So why store the data longer? One explanation can be to analyze the spread of the virus and transmission clusters later and it is scientifically useful to know this information and to learn more. However, a more sinister purpose can be to trace individuals' movements and personal contacts, as they have now opted in to be tracked and traced. It is easy to imagine that in a police state this can be quite dangerous. So again we are faced with the point that once data is collected, it can be mined for good, or not, and individuals may not realize what they opt in for.

All data that is collected must be secured and its privacy must be maintained. Security and privacy are certainly not synonymous. Securing the data means that you keep it safe from unauthorized access by either people or applications, and that the data is not stolen, leaked or otherwise disclosed. Privacy implies that the data is maintained such that it cannot be inadvertently or intentionally shared and disclosed, thus revealing private information. While closely aligned, security and privacy are different. Data can be secured by encryption, but sending an encrypted WhatsApp message to someone who in turn shares it on Facebook would violate privacy, not security. With health and movement-related information it is particularly concerning that information needs to be kept both secure and private.

Third parties who maintain data collection for others, such as cloud providers, are also responsible for data. There have been multiple cases of data breaches. For example, in United States v. Joseph Sullivan, Case No. 3-20-71168 JCS (N.D. Cal. 8/20/20), a criminal complaint was filed against the former Chief Security Officer of Uber Technologies, Inc. for failure to disclose a data breach and for the disclosure of tens of thousands of customer records, including riding patterns and therefore movement and location.

In a SAAS situation, Catchco Corporation signed a Master Service Agreement with Securico to provide a platform and data security services for Catchco. After Securico failed to update its platform, Catchco was hacked and its customer information released. Catchco sued Securico for breach as well as fraud in promising to keep the data secure. An example of recovery in excess of contractual limitation is Affy Tapple, LLC. v. ShopVisible, LLC, CVN18C07216MMJCCLD, 2019 WL 1324500 (Del. Super. Mar. 7, 2019). All of these cases point to the fact that if you collect data for any purpose and continue to store it for a period longer than necessary to the underlying purpose, you must consider security and privacy, system patching and security and access limitation to that data.

Likewise, keeping data for long periods of time may cause the data to be disclosed to, or subpoenaed by third parties. In a recent case, a criminal defendant issued a subpoena to Facebook seeking to disclose restricted posts and private messages of an alleged victim. While the Federal Stored Communications Act does not protect media entities from disclosing public communications, it does not address the protection of communications deemed private by the individual who has made them. The requesting party of course needs to show why it is entitled to the disclosure, but it is important to remember that information can be obtained if it is available. Facebook, Inc. v. Super. Ct. of San Diego County, 10 Cal. 5th 329 (2020).

Yet another consideration is retention. Records management wisdom dictates that data should be retained in accordance with a retention schedule and that it is best practice to dispose of the data once retention schedule requirements allow by getting rid of everything that you can legally get rid of. (Disposition may include destruction, return to client and archiving.) Data mining and secondary usage upends this notion, so once again, schedules need to be thoughtfully adjusted, taking into account all the criteria discussed above.

As regulations are getting tougher and clients are more concerned with privacy:

1. Understand fully all of your legal obligations both to maintain privacy and to secure the information collected
2. Understand the implications of an information request and have procedures in place in advance to comply
3. Be aware of the liability for a data breach in case of a failure to patch in a timely manner or failure to apply other security measures and implement prevention controls
4. Apply data deidentification where appropriate; anonymize data when possible
5. Adjust your data retention schedules

In conclusion, it is critical that organizations looking to leverage contact tracing applications have clear data minimization principles in place, including implementing retention limits, guardrails around public disclosure, and well thought-through anonymization protocols. In particular, for firms looking to develop such applications, it is critical to incorporate a privacy by design approach, particularly keeping data minimization principles at the core of the design. For organizations looking to leverage such applications, it is similarly critical to ensure that the data collected is narrowly tailored to the purposes and those purposes are clearly defined in their privacy policy. As noted above, failure to follow such principles run the risk of conflicting with applicable data protection laws and worse, result in losing the public's trust in such applications.

CONTACT TRACING CHECKLIST

1.		Adhere to the legal and ethical principles of handling personal information to ensure responsible data management and respect for privacy throughout the process.
2.		Safeguard the privacy and security of personal information in accordance with the legal requirements of the countries where the data is being collected.
3.		Assess the data security controls of the contact tracing app (even if occurs after its implementation).
4.		Decide on which personal data you will collect; minimize the data collected where possible.
5.		Determine how contact tracing data will flow into your organization (by app, email, text, etc.).
6.		Obtain verifiable consent from the individual for whom the data is being collected.
7.		Be clear as to the reasons for data collection.
8.		Acknowledge the privacy concerns of the individual providing the personal information.
9.		Be as transparent as possible as to how that information will be used, the length of time it will be stored and the methods by which it will be secured.
10.		Apply data deidentification where appropriate during the collection process; anonymize data when possible.
11.		Store collected data in decentralized repositories. Do not append to existing personnel records.
12.		Adjust data retention schedules.
13.		Use the data collected only for the purpose for which it was collected.
14.		Establish procedures to comply with individuals' information requests.
15.		Be prepared to respond to a breach of contact tracing information.

RESOURCES

INTRODUCTION

- COVID-19 Contact Tracing data protection expectations on app development. Information Commissioner's Office (ICO). https://ico.org.uk/media/for-organisations/documents/2617676/ico-contact-tracing-recommendations.pdf
- Guidance for COVID-19 Privacy Regulations. Iron Mountain. https://www.ironmountain.com/resources/infographics-and-tools/g/guidance-for-covid-19-data-processing-and-privacy
- Guidance on Returning to Work. Occupational Safety and Health Administration (OSHA). https://www.osha.gov/Publications/OSHA4045.pdf?deliveryName=USCDC_10_4-DM31187
- Guidelines for the Implementation and Use of Digital Tools to Augment Traditional Contact Tracing. Centers for Disease Control and Prevention. Updated 16 June 2020. https://www.cdc.gov/coronavirus/2019-ncov/downloads/php/guidelines-digital-tools-contact-tracing.pdf
- What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws. Us. Equal Employment Opportunity Commission. Last update 8 September 2020. https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws

SECURITY

- https://www.cdc.gov/coronavirus/2019-ncov/php/contact-tracing/contact-tracing-plan/Confidentiality-Consent.html
- https://www.cdc.gov/coronavirus/2019-ncov/php/contact-tracing/list-requirements-for-protecting-health-info.html

DATA MINIMIZATION & ANONYMIZATION

- University of Oxford, Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown, https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown, (last visited September 25, 2020).
- European Commission, Commission Recommendation of 8.4.2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymized mobility data, C(2020) 2296 final, https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf (last visited September 25, 2020).
- Personal Data Protection Commission Singapore, Advisories on Collection of Personal Data for COVID-19 Contact Tracing and Use of SafeEntry, https://www.pdpc.gov.sg/help-and-resources/2020/03/advisory-on-collection-of-personal-data-for-covid-19-contact-tracing#advisory3, (last visited September 25, 2020).

- German Federal Data Protection Commission, Information under data protection law on the processing of personal data by employers and employers in connection with the corona pandemic, https://www.bfdi.bund.de/DE/Datenschutz/Themen/Gesundheit_Soziales/GesundheitSozialesArtikel/Datenschutz-in-Corona-Pandemie.html?nn=5217154, (last visited September 25, 2020).
- Federal Trade Commission, Privacy during coronavirus, https://www.ftc.gov/news-events/blogs/business-blog/2020/06/privacy-during-coronavirus, (last visited October 1, 2020).

CONTACT TRACKING CHECKLIST

- https://www.who.int/publications/i/item/contact-tracing-in-the-context-of-covid-19
- https://www.cdc.gov/coronavirus/2019-ncov/php/contact-tracing/list-requirements-for-protecting-health-info.html

REFERENCE LINKS

TERMS OF SERVICE/USE:

- Gmail: https://policies.google.com/terms?hl=en-US#toc-permission
  - *Excerpt*: This license allows Google to: ...modify and create derivative works based on your content, such as reformatting or translating it"
- Dropbox: https://www.dropbox.com/privacy?trigger=_footer
  - *Excerpt*: To provide these and other features, Dropbox accesses, stores, and scans Your Stuff. You give us permission to do those things, and this permission extends to our affiliates and trusted third parties we work with.
- TikTok: https://www.tiktok.com/legal/terms-of-use?lang=en
  - *Excerpt*: "You also waive any and all rights of privacy, publicity, or any other rights of a similar nature in connection with your User Content, or any portion thereof."
- WeChat Terms of Service: https://www.wechat.com/en/service_terms.html
  - *Excerpt*: "we and our affiliate companies may, subject to the our WeChat Privacy Policy, copy, reproduce, host, store, process, adapt, modify, translate, perform, distribute and publish Your Content worldwide in all media and by all distribution methods, including those that are developed in the future;"

TO READ OTHER REPORTS WRITTEN BY THE LAW FIRM INFORMATION GOVERNANCE SYMPOSIUM, PLEASE VISIT:
SYMPOSIUM.IRONMOUNTAIN.COM

800.899.IRON | IRONMOUNTAIN.COM

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM) provides information management services that help organizations lower the costs, risks and inefficiencies of managing their physical and digital data. Founded in 1951, Iron Mountain manages billions of information assets, including backup and archival data, electronic records, document imaging, business records, secure shredding, and more, for organizations around the world. Visit the company website at www.ironmountain.com for more information.

USLGL-RPT-011420A