VIGILANT PSA

The New *Free* OLENDERFELDMAN Privacy E-Newsletter

Edition 1

Welcome

Welcome to the first edition of the **VIGILANT PSA** e-newsletter. The **VIGILANT PSA** e-newsletter is designed and dedicated to enable you to stay at the forefront of the latest advances in all about providing updates, information and practical advice/tips about Protecting, Securing and Advancing your and your clients' and customers' privacy, data and security in today's modern Cyber world. Maybe we will even have some fun along the way. As a reader of the **VIGILANT PSA** e-newsletter, we invite you to contact Michael J. Feldman, Esq., CIPP/US at mfeldman@olenderfeldman.com if you have any questions, are interested in hearing about any particular topics, or have a suggestion for who should be interviewed for future editions of the **VIGILANT PSA** e-newsletter. Thanks for tuning in, sharing around, and hopefully enjoying the read!

Legal Notice

Since the **VIGILANT PSA** e-newsletter is written by lawyers, it is only appropriate that it also contain a legal notice. **The VIGILANT PSA e-newsletter is not intended to provide legal advice and is not intended to issue any legal opinion, nor determine whether or not any specific legal action is legally required.** Rather, the VIGILANT PSA e-newsletter is what it is says it is: updates, information and practical advice/tips about **P**rotecting, **S**ecuring and **A**dvancing your and your clients' and customers' privacy, data and security in today's modern Cyber world, all hopefully in a practical, enjoyable and easy to follow manner.

In This Issue

In The News

▸ **More privacy law mishmash.** Though Congress keeps threatening to get into the privacy law game, so far, it has done little. As a result, more states continue to take privacy law into their own hands. The California Consumer Privacy Act, the first comprehensive privacy law in the US, has already been expanded through the recently voter-passed California Privacy Rights Act (to take effect January 2023). Next in line is the recently passed Virginia Consumer Data Protection Act (also effective as of January 2023). Nevada and Maine have passed less comprehensive data privacy laws, while at least 10 other states have bills bouncing around.

▸ **Have you been taking care of your face during your COVID quarantine?** Facial recognition technology is expected to be a $7 billion market by 2024 according to MarketsandMarkets. Places like Disney's Magic Kingdom and several airports are expected to start using facial recognition technology for various purposes this year. While some studies have suggested that some facial recognition technology may have different error rates depending on your race (and I do not mean the marathon versus the 100m dash), technology companies are working hard to fix these problems, as well as adapt to our new mask-wearing trend. Get ready for the brave new world out there.

▸ **The breach has more reach.** With all 50 states already having breach notification laws, not to mention sector-specific laws such as HIPAA, the Federal Government is working hard to get into the game after the infamous SolarWinds hack. More to come here.

▸ **No Cyber Czar sure is bizarre.** With cyber attacks by China, Russia, North Korea, Iran all in the news, and the White House considering various Executive Orders to address these issues, the Biden Administration has still failed to fill the post of National Cyber Director. The post was created by Congress towards the end of the Trump Administration (over President Trump's veto) and has yet to be filled by either President. According to Politico and other sources, believe it or not, political infighting has stalled the appointment.

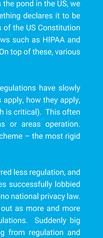
▸ **What else is new?** Believe it or not, ransomware attacks continue to flourish as many businesses continue to keep their heads in the sand, or believe that the defenses they put in place 2 years will still help. According to HealthItSecurity, the Avaddon ransomware baddies recently published 2.09 GB of data allegedly stolen from New Jersey-based Bridgeway Senior Healthcare. Of course, this is merely a fraction of a fraction of the data which has been stolen around the country (not to mention the world) that also often finds its way to the dark web and elsewhere. Law firms are also subject to these breaches, with 1 in 4 being victims themselves.

▸ **GDPR being used to make personal data more vulnerable?** You betcha! According to The Daily Swig, full-time bug bounty hunter HxO1 (yes, there is an entire industry of bug bounty hunters), was able to gain access to individuals' personal information by exploiting weaknesses in organizations' DSAR portals. DSAR portals are mechanisms whereby individuals are allowed to access their own personal data to change and update same as required under GDPR. Unfortunately, not all of these DSAR portals took sufficient action to authenticate the identity of the purported individual seeking access to his or her personal data, thus allowing third parties to improperly access an individual's personal data held by the organization. Yes, bad guys are bad, and some of them are pretty smart too. Are you and your organization striving to be even more smart?

▸ **AWS is safe, but is it too safe?** According to DataBreaches.net, SalusCare, a substance and abuse mental health services provider, has sued Amazon after Amazon refused to provide SalusCare with Amazon's audit logs as part of SalusCare's investigation into how hackers gained access to its data hosted on AWS. Basically, SalusCare wants to make sure that the stolen data is frozen (a step Amazon supposedly has taken), stays frozen, and they want to know what data was actually taken. It's this last part to which Amazon apparently objects since SalusCare does not own the "bucket" in which this allegedly stolen data now resides. Wow!

▸ **Health Passports the new rave, or required to get into the rave?** As more people receive one of the various COVID vaccines, our government officials and businesses are working hard to figure out how these vaccinations can work together with opening businesses and maybe even getting back to "normal." New York Governor Andrew Cuomo has recently spoken of a "health passport" that people could use to gain access to certain events and activities. On the other end of the spectrum, Florida looks to prohibit any businesses from requiring a COVID vaccine passport. What will other states do? What position will the Federal government take? Will this create a new black market for passports? Do the passports this violate the ADA or any other laws? And of course, how will this play out in the world of privacy laws and concerns? Time will tell.

▸ **The Empire (State) Strikes Back.** The NY Department of Financial Services ("DFS") fined Residential Mortgage Services, Inc. ("RMS") $1.5 million as a penalty for violating Cybersecurity Regulation, Part 500 of Title 23 of the NY Codes, Rules and Regulations. RMS, a licensed mortgage banker which collects personal data in connection with closing on mortgage loans, failed to report to DFS a cyber breach to which it was subject in 2019. RMS also failed to conduct an internal investigation into the breach and the scope of consumer data which was exposed until told to do so by DFS. In addition to the penalty, RMS will be required to improve its cybersecurity program.



Mike's Mind

We Need A Comprehensive National Data Privacy Protection Law

As a general matter, European nations start with the proposition that all personal data is private and worthy of protection unless there is a law that says otherwise. Across the pond in the US, we start with the proposition that nothing is private unless someone or something declares it to be private. These declarations can be found everywhere from the penumbras of the US Constitution with the "right to privacy", various state constitutions, countless sector laws such as HIPAA and Gramm-Leach-Bliley, as well as even more countless state and local laws. On top of these, various industries have started voluntary privacy guidelines.

As a result of the convoluted manner in which privacy laws, rules and regulations have slowly evolved in the US, it often takes a team of lawyers to figure out what laws apply, how they apply, and how to integrate compliance with a successful business venture (which is critical). This often means having multiple operational schemes over multiple jurisdictions or areas operation. Alternatively, some businesses simply voluntarily impose one regulatory scheme – the most rigid – across the board.

Initially, big business was against a national privacy law. Businesses preferred less regulation, and a national privacy law certainly was not less regulation. These businesses successfully lobbied Congress and the political parties sufficiently to assure that there would be no national privacy law. As is often the case, the law of unintended consequences slowly played out as more and more states and industries started imposing their own privacy rules and regulations. Suddenly big business (and others) recognized their short-sighted thinking in running from regulation and figured out that a national privacy law combined with the Supremacy Clause could make their lives far more simple if there was a single regulatory scheme to follow.
Putting aside what should be in such a national privacy law (i.e., should it be like GDPR, or the CCPA, or some soft regulatory scheme simply to cancel out laws like the CCPA, etc.?), it is clear that it is time for the US to join the growing worldwide trend at national privacy laws. Reasons for having a national privacy law include:

- Having a more uniform standard for businesses to follow;
- Providing more protection to the privacy of our residents and citizens in a world where cybercrime is ever on the rise;
- Setting uniform privacy expectations of businesses and individuals alike;
- Minimizing confusion in the marketplace;
- Maximizing technological growth with a uniform regulatory scheme; and
- While we are a nation of states, data and technology know no borders, so the law that protects and regulates same also should know no borders.

Of course, there are lots of reasons to not have a national privacy law:

- We just like to be different;
- We like to hire more lawyers and pay them more money (my door is always open);
- We should not do anything they do in Europe;
- It's easier for businesses to wing it and cross their fingers that they are in compliance with everything; and
- People in California really like the CCPA.

It is clear that the time to do so has come. An appropriate national privacy law would benefit all and bring this country's data position into the modern world. Unfortunately, we are faced with a reality which is even more certain than the need for a national privacy law – a dysfunctional Congress which seems largely incapable of bipartisan thinking on critical issues. Notwithstanding, the time has come for big business, small business, the technology world, the mom and pops and families and everyone else to come together and demand that our Federal government do its job on this one. I'll save my opinion on what should be in such a national privacy law for another edition.

What are your thoughts? Feel free to send them to me at mfeldman@olenderfeldman.com.

Useful Tips – Information Security Policies

While many businesses believe that they have adequate procedures in place to protect their own confidential information or that of their clients/customers, most do not. Rather, they merely have a section in their Employee Handbook on confidentiality, and maybe require their employees to sign confidentiality or non-disclosure agreements. Don't get me wrong, you definitely want to have such documents in place. However, generally such provisions are not sufficient to protect a company's confidential and proprietary information, nor to effectively minimize the chances of a data breach. Indeed, there is little contained in such documents which actually address how to preserve and protect such confidential information from inadvertent or malicious disclosure. Further, without a proper policy and training, compliance is less likely. This is where an Information Security (or "InfoSec") Policy comes into play.

Purposes and Areas Addressed by an InfoSec Policy

The purpose of an InfoSec Policy is to outline your company's position on corporate information security and establish general rules for its personnel to follow, which will ensure the confidentiality, integrity, and availability of information and protect your company's own information technology assets from unauthorized access, use and/or modification and damage or destruction.

The InfoSec Policy establishes certain roles and responsibilities for information security within the company, as well as a framework with which those individuals can perform these obligations.

InfoSec Policies typically address computer systems, smartphones and the like, network operations, and all company/client information, as well as the individuals who work with or have access to same. The concept is to create standard operating procedures to address information security requirements related to:

- General security controls
- Computer acceptable use
- Passwords
- Internet use
- E-mail/instant messaging
- Virus and other infection prevention
- Communication devices
- Remote network access
- Wireless networking
- Information protection
- Physical access security
- Software installation
- Clean desk
- Technology equipment disposal
- Pandemic response
- Security incident response
- Policy maintenance

Implementation of an InfoSec Policy

An InfoSec Policy must be more than a resource for employees, contractors, etc., to access and review when they have questions. It must also be understood by the company and its personnel so its policies can be implemented and followed on a daily basis. Therefore, once an InfoSec Policy is prepared and finalized, all personnel must be appropriately trained, and such training should be repeated at least annually.

Getting Started

If you follow the news, or read the **VIGILANT PSA** e-newsletter, you know that ransomware attacks continue to increase. While a good InfoSec Policy and training, together with strong technical security, can do much to minimize the chances that you fall victim to ransomware, there are things you can also do to minimize any potential harm should be victimized, including:

Useful Tips – Minimize Potential Harm From Ransomware

If you follow the news, or read the **VIGILANT PSA** e-newsletter, you know that ransomware attacks continue to increase almost daily. While a good InfoSec Policy and personnel training, together with strong technical security, can do much to minimize the chances that you fall victim to ransomware, there are things you can also do to minimize any potential harm should be victimized, including:

- Back-up all critical data as frequently as practically possible, but no less frequently than daily. Such back-ups should be on a separate server (or cloud server) or device so the backups cannot be corrupted by your active server.

- Train, train, train all personnel to never open an attachment or email they are not expecting. If in doubt, call or e-mail the source directly to inquire as to the attachment – but obtain the contact information directly and NOT from the e-mail itself (i.e., from your separate contacts, or directly from the company's website, etc., as the potentially spoofed or fraudulent e-mail is likely to contain incorrect information).

- If it looks suspicious, treat it that way.

- Have a written plan in place to deal with a ransomware attack AND make sure that all participants in this plan know exactly what to do and when to do it.

- Disconnect all computers and devices from your network as soon as you know there has been an attack.

- Know if you have insurance to cover a ransomware attack, and/or consider obtaining appropriate Cyber insurance (though rates are increasing rapidly).

- Contact your local police and the FBI promptly.

- Seek professional help. While trying to understand more through searching online, NEVER rely on such online advice or download any proposed solution as these may not work and are sometimes from the bad guys themselves.

Useful Tips – Cheap Insurance

Ok, this is not about Cyber insurance (which is a good idea, though its cost is increasing). This is about limiting your potential liability through action. Imagine you owned a few million dollars of jewelry. Some of it gets worn daily, some of it gets worn only for special events, and some of it almost never sees the light of day. Would you leave all of this expensive jewelry sitting out on your dining room table? What if you were sure that someone was eventually going to break into your house, then would you leave it out? Surely not. You would likely keep the jewelry that gets worn on a regular basis in your house, maybe in a safe. You might keep the rest in a safety deposit box outside the house or in a more secure vault.

Treat your sensitive data the same way you would your expensive jewelry. You should assume that you will be the victim of a data breach at some point. Just like with your jewelry, you should minimize the risk of loss, and if there is a loss, minimizing the size of that loss. After all, if you only had 10% of your jewelry in your house at the time someone breaks in, that is the most you could lose. How do you apply this logic to your data?

- Only obtain the data that you need.
- Only keep the data as long as you need it, and only keep what you need to keep.
- Know what data you have.
- Know where your data is.
- Protect your data with physical/logical/technical security and minimize who has access.
- Have a document retention and destruction policy and follow it.
- Assess all of the above at least on an annual basis.

Industry Interview

Wouldn't you love to know what those big companies imposing detailed privacy and security requirements on your business really think about; what they really want; what they really care about; and how they handle their own data? If you asked, would they ever tell you? Surely not. I was fortunate enough to find an insider who agreed to tell the truth. Specifically, I spoke with an in-house privacy attorney (separate from compliance) who provides advice and support on a global basis to a Fortune 50 global financial services company. The answers to my questions were quite interesting, but perhaps not truly surprising given my experiences. I believe you will be happy if you read on. For obvious reasons, I am not identifying the individual or the company, and any responses not in quotes represent my summary of the actual response.

Q: What are the primary internal or company driving forces in making decisions concerning data privacy and security?

A: It's legal and regulatory requirements as well as client-led requirements. We are a service provider to a lot of other companies and the requirements from them [our clients] are getting more and more onerous.

Q: Are these requirements being brought to you by business people or lawyers?

A: I would say it's coming mostly from the lawyers – even though the business or other corporate functions should understand what their legal and regulatory requirements are, it is unfortunately not the case." Sometimes the business people, who do not really understand the legal implications, will take the side of the other party to the transaction just to get the deal done without much concern for those legal implications. "It's the opposite of privacy by design.

Q: What are the primary impediments to implement data privacy and security programs/processes you wish were in place or could be implemented?

A: Money and time. Also, the tone from the top is focused on cutting costs and making money, and unfortunately, privacy is seen as a hindrance." The result is often incomplete programs, policies and procedures due to lack of serious investing in privacy and security.

Q: What are the real concerns of your stakeholders/bosses/executives when entering into the various privacy-related agreements?

A: It all depends on the business group involved. If the business group is more familiar with technology and the company's obligations to protect data when sharing with a third party, the obligations are taken more seriously. If it is coming from a business group not so familiar with these requirements, the agreements are more frequently viewed as simply checking a box that the agreement was signed. Of course, the more sensitive the data at issue, the more likely we are to care about robust requirements.

Q: How frequently does your company conduct data privacy/security audits on your vendors?

A: [This answer required me, the author, to read between the lines of the attorney's response] There is not much auditing done here, and when it is done, there are lots of loopholes. From a privacy attorney's view, there is not nearly enough done to audit the vendors, thus making the contractual requirements more of a box-check exercise or a fallback position in the event something catastrophic happens. This position seems to correspond to the concerns about expenses for a robust data privacy/security program.

Q: From a privacy/data security viewpoint, what do you look for in your vendors and what does not matter so much?

A: I actually get concerned when they wholesale agree to our terms because it usually signals to me that they are not as mature as they should be. I like to have a vendor who can talk the talk, etc., when we're hashing out terms around security incident notification, for example.

Q: Do the business people really understand and/or care about data privacy and security when it comes to entering into business contracts?

A: Most do not care.

Q: What's your best advice for prospective vendors with respect to data privacy and security issues if they want to engage in business with your company?

A: This is a tough one. I would say that when you have a prospective customer that is in an industry that is highly regulated (like pharma or financial services), knowing that the customers are required by their regulators to ensure that third party service providers meet certain minimum requirements and have minimum contractual terms in place – especially when that third party is going to be processing certain information on the customer's behalf." Vendors should be aware of the company's basic regulator requirements and recognize when there may be some CYA in not wanting to hire an unknown or untested business for an important job.

Q: Does your company expect more of its vendors and business partners than your company itself when it comes to data privacy and security compliance, policies and procedures.

A: Yes. Do as I say, not as I do!

Strictly Personal But Certainly Not Confidential

Not everything here is about Protecting, Securing and Advancing your and your clients' and customers' privacy, data and security in today's modern Cyber world. Apart from being a lawyer, I am also a volunteer high school distance running coach. Perhaps to no surprise, I have learned a lot about myself as a running coach which has also helped me as a professional. Since I am far too old to run as fast as the fastest kids I coach, I had to find other ways to lead by example – a/k/a problem solving. Last month I decided to try the Goggins 4x4x48 challenge. It sounded pretty simple. Run 4 miles every 4 hours for 48 hours. The total distance was long, but not too long. To make a long story short, this thing was hard. My legs got stiff, my body and mind started to hate me, and I could never eat as much as I wanted. In the end, I completed the challenge no worse for the wear. It turns out, this was really just a mental challenge. More problem solving. It was about keeping my mind focused on what needed to be done when there were tremendous distractions pulling me in all different directions, including to a warm bed!

At the end of the day, or the two days, this challenge was not that different than what we all face at work. We face challenges and problems, and despite all the distractions around us, we need to focus on the job at hand. Sometimes that is easy. I had no problem running in the sun during the day when I knew hot food was waiting at the end. Sometimes, the challenge is, well, challenging – like getting out of bed to run in the dark and cold. When used properly, our minds can be quite amazing. When analyzing your own daily challenges, whether it be personal or how to handle the next data privacy and security problem or roadblock, stay vigilant, use your mind, and get the job done. You will be happy you did.

For more on the unbreakable former Navy SEAL and current everything, check out https://davidgoggins.com/. For some advice on how to handle the Goggins 4x4x48 challenge next year, check out https://marathonhandbook.com/4x4x48-challenge/. And if you try it next year, please train more than I did!