Audience Questions from the Data Privacy in the Digital World Panel Discussion

September 24, 2019

1. **Can the human mind be GDPR compliant?**

Denny: GDPR applies to individuals as well as legal entities, so long as they meet the other criteria, *i.e.*, being established in the EU or targeting EU residents with their goods or services. GDPR, however, does not apply to purely personal or household activities.

Arena: Interesting thought. Are your inner thoughts protected as personally identifiable information? This may not be something we necessarily need to worry about today, but the futurist in me says that maybe this becomes a topic of conversation in the future.

Adler: GDPR is a regulation in EU law on data protection and privacy for individual citizens of the European Union and the European Economic Area. It centers around how organizations process and protect such information. Humans who process the data must be trained in the principles. However, human minds can not be considered 'GDPR Compliant'.

2. **How should incident response teams approach ownership and management of breaches with security and privacy impacts?**

Denny: If a potential data breach involves data that the business owns, then it is responsible for providing notice to the affected data subjects. If the business is processing data for its customer, then it is responsible for notifying the customer as soon as possible so the customer can determine its obligation to notify data subjects. Regardless of ownership, any business that suffers a breach will want to stop the breach, investigate what happened and remediate the breach to minimize risk to the business. That includes identifying and fixing any security holes.

Arena: Most newer data privacy laws are requiring disclosure during a certain time period (eg: GDPR is 72 hours from identification.) It is essential to document the procedures a team must follow when presented with an incident and who the decision makers are for each major decision so that they have something tangible and definitive to guide them. When teams are left to their own decisions, especially in times of stress, a lack of practiced procedure can put the business in greater risk.

Adler: An incident is a compromise of the confidentiality, integrity, or availability of an information asset. A breach is a confirmed disclosure of personal data to an unauthorized party. While all breaches are incidents, the reverse is not true. Handling incidents and breaches in an appropriate manner requires a coordinated effort across IT Security Teams, the Privacy Office, and Legal.

3. **Can you further explain if PII has different levels of security requirements?**

Denny: Under GDPR, there are stricter rules for special categories of personal data, which are defined as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data, biometric data for the purpose of identification of a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Under certain sectorial laws in the U.S., financial information, health information, and information about children have special security requirements.

Arena: In addition to Bill's comments, most businesses should do more to improve the classification of their data so the importance of the data in question, PII or not, is adequately protected.

Adler: Yes, certain laws call out special requirements, such as encryption or transfer/processing restrictions for specific types of data. For example, Article 9 of the GDPR has processing restrictions for 'special categories of personal data' that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data or a natural person's sex life or sexual orientation.

4. **For CCPA and other similar regulations, would it be better to apply the controls over all records as opposed to identifying residence?**

Denny: Because it is so difficult in many cases to identify the place of residence of all data subjects, many companies are opting to apply CCPA-like controls to all of their personal information without regard to location. However, it's important to know whether there are special rules in any of the jurisdictions in which you are doing business that impose different requirements as, for example, the biometric privacy law in Illinois or the data security regulations in Massachusetts.

Arena: While it may seem tempting to apply the most stringent data protections uniformly across all data, that ultimately is a costly endeavor. Identifying what data holds importance / is required to be protected by the respective jurisdictions is a smarter choice and forces you to understand the location, age and significance of all of your data.

Adler: Each company has a unique risk profile, product offerings, and other factors that impact the optimal approach.

5. **Is there expected conflict across states that will make implementation difficult to impossible/impractical (cheaper to pay the fine)?**

Denny: It is impractical to comply with all applicable laws, so businesses need to do a risk assessment based on what laws apply and then try to construct a program that addresses the most significant compliance risks.

Arena: I feel that a federal privacy law is necessary for the benefit of our citizenry and to show the world that the US takes the privacy of the individual seriously. While that day seems way off into the future, as the number of breaches and other security incidents increase and gain in complexity, I feel such a law is inevitable.

Adler: Given the complexity of privacy and security regulations, it is almost impossible for a global corporation to fully comply with every law. However, it is a strategic imperative for <most> companies to make a good faith effort to build comprehensive security and privacy programs that meet the spirit of the regulations, via a risk-based approach. Companies that can demonstrate their 'good faith efforts' towards compliance reduce the risk of security breaches, large fines, and other enforcement actions.

6. **Does population of a country play a big role on data privacy? For example, Estonia with very fewer population has a big cybersecurity posture that with fewer instance of breach.**

Denny: The strictness of the data privacy laws is not necessarily proportional to the population of the respective jurisdictions. Different countries have different cultures of compliance, and different countries put different degrees of effort into cyber defense and education. Estonia has a strong culture of compliance and a very technologically sophisticated government.

Arena: Generally speaking, countries like Canada are very sensitive to the location of their data, and have little interest in keeping their data in US datacenters due to a perceived risk of government accessibility. In countries like Australia, there are requirements to keep the data housed in country. You will notice that many of the third-party cloud providers have set up datacenters in nations with these requirements to assure their residents of their data's protection under their laws.

Adler: It is unclear how population influences the laws and culture of a country. The US is a more 'open', innovative, and capitalistic society than some other countries. 'Big Tech' is largely a US phenomenon. Our business friendly laws helped to share the industry – and can contribute to some of the weaknesses in privacy & security of personal data.

7. **How do extreme large population in the North America especially, the USA maintains a balance on how much population influences privacy? Or does it mean large population experiences large exponent of big data and smaller population do less of big data?**

Denny: I don't think the size of the population is directly relevant to the laws governing privacy and security. Many tech companies operate across national borders and so deal with data from many jurisdictions. National borders are becoming less relevant as laws increasingly have extraterritorial reach.

Arena: Unfortunately, the vast majority of the US population is agnostic towards data privacy. Other nations, like China culturally put very little emphasis on privacy. Both the US and China are very populated regions so I am not sure population is directly correlated to how much privacy laws are developed. However, California, as 12% of the US population and (apart from all other states) is 5th in global GDP, is effectively forcing the hand of the US to enact greater privacy laws & expectations. As California goes, so goes the country.

8. **What changes are being considered or implemented to elementary the dependency on SSN as means to authenticate a persons identity?**

Denny: There are various projects to develop national standards for authentication of identity, and private industry is working on standards for what they call "federated identity management." There are also experimental blockchain solutions to identity management that are not close to implementation. In the U.S., we are moving toward more secure driver's licenses (a TSA requirement), and many financial institutions identify their customers in ways other than by social security number. Once a relationship is established with a business, they often have their own credentials (hopefully two-factor) for authentication.

Arena: When social security numbers began to be issued people were apprehensive that it would be used as a unique identifier by the government. Unfortunately, it has turned into just that. Regardless of the number being used, whether it is an SSN, drivers id, health id, EDIPI or another record of choice, it is a unique identifier that will be used in the same manner, so the same protections need to be followed for them as all of them are PII based on newer legal definitions. That being said, each organization should have its own unique identifier key in which to base their dealings with, rather than leveraging a social security number.

9. **Large organizations such as Target, Equifax, etc have had major breaches. Presumably they had the money and resources to address security and privacy and they still had a breach. How does a small organization with far less resources address privacy and security successfully?**

Denny: The cost of privacy and security is a huge burden for small organizations. They should address it by following FTC guidance for small businesses. This includes addressing the easy issues first that have the biggest impact. For example, patching software, having firewalls in place and training users not to click on unknown links will stop the vast majority of all breaches. After that, security compliance begins to get more expensive. As for privacy, all businesses of any size need to inventory what data they have, where they keep it, how they process it and who has access to it. Then they need to assess what laws apply and develop a plan to move toward compliance. This has to be done in a reasonable way that

takes cost into account. What might be demanded from Amazon or Microsoft might be unreasonable when applied to a small business.

Arena: Reduce your attack surface by doing the basics. Understand where your data lives, encrypt it, patch the servers they live on, scan for vulnerabilities regularly, use two-factor authentication, & keep good and frequent backups of your data. Do vendor risk assessments, and if you are the vendor offer to have one performed as a sign of goodwill and confidence in your data protection and security. Get ample cyber insurance to cover the difference.

Adler: It is a strategic imperative for <most> companies to make a good faith effort to build comprehensive security and privacy programs that meet the spirit of the regulations, via a risk-based approach. Companies that can demonstrate their 'good faith efforts' towards compliance reduce the risk of security breaches, large fines, and other enforcement actions. The cost and effort of a smaller company should be proportionally less than what is required of a large, more complex company.

10. **Much of the dialogue has been about what companies and organizations should do to protect data (sort of an inside out view), what advice would you give to citizens (Dos or Don'ts) to help protect themselves?**

Denny: Use strong passwords at all of the sites where you have accounts, and use a password manager so you never use the same password at two or more sites. Make sure you have downloaded and installed the latest patches to your computer. Don't click on the links in any unsolicited email or in any unusual email. Make sure you have an anti-virus program installed. Be extremely careful in using public wi-fi unless you are also using a VPN for accessing data.

Arena: Everything Bill mentioned is spot on. Additionally, Aesop's fables taught me at a young age to not believe everything you see. This advice should also be adhered to in the cyber world. Be a 'cyber cynic.' Be ever vigilant for the signs of fraudulent activity, and if you don't know what that email is, don't open it!

Adler: Individuals need to educate themselves in best practices and tools to protect their passwords, identities, and devices. People should limit their use of IOT devices & Apps (where possible). For example, the convenience of using Siri or Alexa may not outweigh the privacy risks of having a microphone record your private conversations.

11. **What are your thoughts in regards to data privacy and security with the trend of vendors leveraging global cloud data centers? Vendors are promoting the redundancy as a business**

advantage but my organization requires all data and connections to remain in the continental USA

Denny: The larger cloud providers understand the importance of data localization so they are offering services, typically at higher prices, under which you can specify the jurisdictions where your data will be located.

Arena: The cloud is not a magical place that makes all of your privacy, security or even resiliency requirements disappear. It is not a place to simply transfer risk. Think of the cloud as a Tesla and your legacy infrastructure as a Chevy. They both do the same thing, but both do it in a different way. Regardless of which cloud you are using, you must understand that business' role in the shared responsibility model as well as your own. For IaaS providers like AWS, the cloud provider's responsibility usually ends at the hypervisor (the layer above the virtual machine.) For SaaS providers, that line of demarcation may be closer to your application. The best rule of thumb to follow is any steps you would need to take to protect your data inside your four walls should be equally matched in a cloud provider.

Alder: Some global providers are reputable and provide services with robust security protections, when implemented appropriately. Strong vendor due diligence is an important element of a comprehensive privacy and security program.

12. **How do we increase corporate liability if the cost of a breach, such as non-compliance fines, insurance claims, class action suits, etc does not exceed the cost of reducing the data privacy risks?**

Denny: The costs companies incur as a result of data breach are huge as well as unpredictable, and they dribble in for years. The trend of these costs is only going up. Regulatory actions in addition impose onerous regimes where companies are required to take certain specific actions and certify compliance annually for up to 20 years. In my experience, the cost of breach is typically much higher than the cost of implementing reasonable privacy and security.

Arena: An ounce of prevention is worth a pound of cure. Do your risk assessment, remediate the greatest risks, continually test and enact monitoring to identify active threats. If you do all these things, your risk will go down. There is no silver bullet however, so insurance needs to be part of the preparation strategy.

13. **What is the purpose of the breached company insurance to the affected consumer? (they should be eligible for lifetime monitoring services)**

Denny: Some laws require that a company that has suffered a data breach that includes social security numbers or other sensitive information provide 1 or 2 years of credit monitoring or identity theft protection. Historically, very few individuals whose data has been breached ever suffers identity theft. For those who do, they have a damages claim against the company responsible for the breach. Identity theft protect can be very expensive, so it's a cost applied to a lot of people, most of whom will not need it. I have not seen any data indicating that identity theft is happening multiple years after the data has been lost in a breach.

Arena: Consumers are receiving notice after notice of their data being compromised. Identify theft monitoring services can assist in detecting breached information so you can react accordingly; and companies should offer it when they identify their data has been breached, but consumers should be cautious of the data they are often so willing to provide. Consumers should also educate themselves further to understand when their data is being collected. Data is the 21st century gold rush. Every little bit helps paint a picture of your buying habits, political affiliations and more. With the enhancements of algorithms that predict your behaviors with concerning accuracy, the smaller your cyber footprint, the better.

For additional questions, feel free to contact:

William R. Denny | Partner
Potter Anderson & Corroon LLP | 1313 N. Market Street, 6th Floor | Wilmington, DE 19801-6108
T 302.984.6039 | F 302.658.1192
wdenny@potteranderson.com | potteranderson.com

Jonathan Arena, CISSP, ITIL, CSM
Managing Director
Phone: 302-722-7362
Email: jon@protectpath.com | Web: ProtectPath.com
LinkedIn: https://www.linkedin.com/in/jfarena

Bonnie M Adler, CIPP/US, HCISPP, CISA

Managing Member & Principal Consultant

PSR&C Solutions LLC

badler@psrcsolutions.com

linkedin.com/in/bonnieadler