IAPP, San Francisco KnowledgeNet (Wednesday, April 18, 2018)

Operationalizing the General Data Protection Regulation (GDPR): How Silicon Valley Tech Titans Balance Innovation with Compliance

Reported by: Tay Nguyen

"What does the first Star Wars film and the GDPR have in common?" Rafae Bhatti, CIPP/US, CIPM, Head of Security and Privacy at HealthTap and current SCU Law student, opened Wednesday evening's KnowledgeNet with a lighthearted joke during a time when stress levels around the GDPR are particularly high. The answer (of course) was a May 25th release date. Taking over for Rafae at the podium, SCU Law's Dean Lisa Kloppenberg stressed the theme of the night's event as balancing innovation with GDPR compliance. The panelists picked up on this theme, successfully providing the "actionable advice" attendees were looking for to meet their compliance needs.

The panel consisted of privacy professionals on both the legal and compliance teams of major Silicon Valley companies, including:

- Stu Eaton, CIPP/US, Director, Legal, Uber
- Amanda Katzenstein, CIPP/US, Product and Privacy Counsel, Salesforce.org
- Andrew Rausa, Senior Product and Privacy Counsel, Facebook
- Tolga Erbay, CIPP/US, Head of Risk and Compliance, Dropbox

The following provides an overview of the topics covered in the panel (note that questions and answers may be paraphrased or condensed):

Q: What are key priorities, challenges, and solutions to preparing for GDPR compliance?

Stu: My top five things to know when creating a DPIA process is: (1) know that the DPIA is part of a larger lifecycle of tracking products that requires, among other things, a detailed collection of information for product and business cases; (2) use short trigger questions in privacy questionnaires; (3) establish a process for review; (4) get buy in from the top and build privacy champions; and (5) think about the structuring of your DPIA.

Amanda: You should remember that there are also internal issues with GDPR compliance. Think about employee data and finding a basis other than consent for processing employee data. Obtaining bank information to pay employees is a processing required for performance of the employee contract or obtaining background checks is compelled by a legitimate interest of the employer. In regard to vendors, build into the contract GDPR requirements like reporting obligations relating to breach or subprocessor responsibilities, and organize your vendors according to different review processes taking into consdieration whether that vendor only processes in the U.S. or whether that vendor contract ends before May.

Andrew: Lean in on practical guidance in approaching data collection and processing and use product counsel as an intermediary between GDPR experts and the business to determine how to implement compliance. Not everyone has to be GDPR experts; instead, follow the herd mentality because DPAs will be focused on big companies and blatant infringers come May 25th. It is also important to know your data flows – this isn't just a GDPR thing, but about understanding your business – and don't over-pivot. For example, it's not a great idea to get consent for everything, because data subjects must also have the ability to withdraw consent and its not great for business having to figure out how to keep your processes going when data subjects withdraw their consent. Finally, collaborate with your competitors; share processes to help each other with compliance.

Tolga: To meet compliance, actual business processes need to change. DPIAs are prescriptive and most small or medium businesses probably haven't done them before. Operationalizing the DPIA is where you have a shift from legal to business: companies need to know who will implement a privacy program and how to prioritize. DPIAs are not a one-time thing – it'll have to be done before May 25th – but should be done before the launch of a new product as well as for core processing activities because product features and uses are fluid. One easy way to get in trouble with the GDPR relates to data subject access requests because of the 30-day requirement to respond under the GDPR. Companies hoping to be in compliance with this should look to automate general requests and responses and then go after specific requests manually.

Q: How do you recommend getting up to speed before May 25th?

Amanda: The IAPP/E book connects the dots for understanding the GDPR.

Stu: The best way to learn about the GDPR is to read the GDPR, but Article 29 Working Party opinions are a great place to learn about concepts and how things will be implemented. OneTrust and other vendors also put out great summaries.

Tolga: Read the GDPR.

Andrew: It only takes a couple of hours to read the GDPR, so read the summaries vendors put out, and then go back and read the GDPR to see how it applies to your company specifically.

Q: Do you have any anecdotes about balancing innovation and compliance?

Andrew: Broadly speaking, design is paramount. Make it user-friendly and layering is good – create the big points and allow "click to expand".

Stu: We are in this together with the regulators, so it is important, as was said before, to no over-pivot. The scary things about the GDPR will probably end up being things that business can work with.

Tolga: Compliance is about mitigating risks over merely checking off boxes, so innovate in ways to mitigate risks for data subjects. Innovation and compliance are not necessarily opposing things.

Amanda: Look at country-specific laws too. Not all countries have their laws [update to GDPR requirements] out yet, but they're not as bad as you think.

Andrew: Don't forget other laws too, like laws regulating cookies.

Q: What is the most challenging thing about GDPR compliance for small and medium-size businesses?

Tolga: Data subject access requests are not the model in Silicon Valley business, where requests are usually automated.

Andrew: Erasure will be more difficult thanks to access, so know your data flows.

Amanda: 30 days to respond to data subject access requests is not a lot.

Stu: Data subject access rights imply that companies have people to handle those requests but not all companies do. Consent can be withdrawn, so companies should not use it as the primary basis for processing data – it should be one of the last bases for processing.

***

Following this initial panel segment, Rafae then opened up the KnowledgeNet for a brief word from the event sponsors, BigID and OneTrust, for a description of technologies and tools available to help companies handle compliance, as well as tips from each vendor for managing compliance.

BigID: Just awarded the most innovative startup at the 2018 RSA Conference, BigID recognizes that the biggest problem for most clients is that they don't know what data they have. BigID also recognizes that clients' biggest worry is about data subject access request. BigID's patent-pending technology helps resolve some of these concerns. It allows companies to correlate their data and take it to map back to identity. It also autogenerates and monitors business processes and data flows to meet Article 30 requirements and allows companies to generate reports for auditors. Another key feature of the BigID technology is consent tracking.

OneTrust: OneTrust is a holistic and global compliance tool. To help companies with GDPR compliance, OneTrust offers the following advice: clients tend to have a misunderstanding of when to use consent, so it is important to use other bases for processing; and do your data discovery because you can't start a data program without knowing what and where your data is. OneTrust also notes that cookie compliance and website scanning have been big in the last few months because more companies want to show transparency.

***

To end the evening, Rafae opened up the panel to questions submitted by attendees.

Q: What are your thoughts on GDPR compliance for companies without an EU presence yet?

Stu: Think about whether you're collecting data about EU data subjects and at what volume. Talk to your legal counsel regarding the risk of enforcement for your current state.

Andrew: Presence is not just physical location. Think about things like whether you receive IP hits in Europe.

Q: What is the interplay between accuracy of data and the right to be forgotten?

Amanda: They both have a 30-day response requirement.

Andrew: They're not mutually exclusive.

Q: How granular are you defining process for Article 30 (records of processing activities)?

Andrew: Companies with less than 250 employees don't need to follow the Article 30 requirement for records of processing.

Tolga: That's up to you. The goal of records is to index your processes – it depends on how you logically groups things.

Stu: Records of processing depends on your construct of how you process. Compare it to a product. There is no real guidance on what they should look like.

Tolga: The ICO and others have examples but do what makes sense for your business.

Andrew: Article 35 requires a DPIA to be conducted when there is a high risk to people. Take a practical approach.

Q: How do you validate subprocessor compliance obligations?

Amanda: Build it into the contract and update consistently or regularly. Include auditing rights in the contract, confirm if vendors are Privacy Shield certified, and check their websites.

Stu: All you can do is your due diligence on the front end, but it is hard to prove compliance according to contracts.

Tolga: If the subprocessor is of a certain size, then it is on them to provide independent audit reports.

Stu: Often, the only time you use the audit provision in the contract is when something goes wrong.

Tolga: Vendor security questionnaires are useful because of their granularity and is still a useful tool for small vendors.

Andrew: Vendor security questionnaires are useful also because if vendors complete it, it should how good that vendor is. A vendor's reputation is also important to consider.

Q: How do small businesses demonstrate they are compliance ready?

Andrew: Do it now. Also, remember that users are more responsive when companies are not blocking access to their products for lack of consent.

Amanda: Put it on your website by doing things like publishing white papers.

Q: Is a follow-up on data subject access requests allowed 30 new days?

Amanda: That is fact specific.

Andrew: That may depend on whether the original response showed bona fide efforts.

Q: Do you advocate for companies getting acknowledgment of new privacy notices?

Andrew: That depends on what the company's basis of processing is. If their basis is consent, then yes.

Amanda: I'd recommend also updating information and giving notice to users of when it takes effect. LinkedIn just did this -- give users time to decide if they want to continue using the product when the new privacy policy goes into effect.

Q: What are your thoughts on having user data on mobile devices for employees?

Tolga: Try not to have user data on mobile devices.

Amanda: It depends on the business purpose, but give users notice.

Stu: There are issues with "bring your own device" (BYOD) that should be considered. A higher level of consent is required if the BYOD policy include an erasure program. The big question is around balancing the protection of business information against the device owner's rights.

Q: How do we handle data residency requirements?

Tolga: There is a misconception that data must be stored in Europe. The GDPR only says that there needs to be a data transfer mechanism. The focus is less on data residency and more on transfer mechanism and protection. In most cases, there is no data residency requirement.

Q: When a vendor purchases data from another company and misuses it, what is the best way to handle the situation if there is no indemnification clause in their contract?

Andrew: The GDPR makes this situation easier by requiring processing language in agreements. The E.U. and U.S. differ on data rights in the resale of data. There needs to be careful reflection of data practices.

Stu: The U.S. has sectoral laws that address that.