Bloomberg BNA

Privacy & Security Law Report®

VOL. 14, NO. 15 APRIL 13, 2015

Privacy Policies

Views on Privacy, Security Challenges for Startups From Fernando A. Bohorquez Jr. of BakerHostetler

Technology startups are often involved in projects that are based on, or at least make use of, personal information. But with sometimes tight budgets and pressure to achieve financial viability, these companies may be hard-pressed to incorporate privacy and security into their operations.

Bloomberg BNA Privacy & Security Law Report Senior Legal Editor Donald G. Aplin posed a series of questions to Fernando A. Bohorquez Jr., a partner at BakerHostetler in New York, about privacy and security issues startups should consider.

BLOOMBERG BNA: What do you think are the most challenging initial privacy and data security issues that startup companies and their counsel face with the sometimes limited resources and focus on bottom line viability as an overarching goal?

Bohorquez: The first initial challenge is one of mindset. Privacy and data security is simply not top of mind for many if not most startups. Remember that it was not too long ago that it was a challenge to get the C-suites in many Fortune 500 companies to focus on privacy and data security. That of course has changed dramatically in the post-big data and data breach corporate world. But if it took a sea change for well financed and profitable Fortune 500 companies to recognize the value in robust privacy and data security practices, then it should be no surprise that privacy is an afterthought to the average startup founder who barely has enough runway to raise funding, develop and cultivate customers and establish a minimum viable product or service.

This mindset is starting to change. On the one hand, the Federal Trade Commission is sending more and more messages to the startup community to take privacy seriously. The regulator has issued a series of reports on mobile privacy and data security (12 PVLR 166, 2/4/13), as well as ramped up its enforcement against startups like Snapchat Inc. (14 PVLR 69, 1/12/15)and Goldenshores Technologies LLC (Brightest Flashlight app) (12 PVLR 2027, 12/9/13) that fall short on their privacy practices and promises. And on the other end within the startup community itself, privacy and data security are becoming increasingly high profile topics. There is also a growing acknowledgement by tech leaders from Apple Inc. to Intel Corp. to Microsoft Corp. that privacy is a business value in and of itself, not just a hoop to jump through to release a product.

Another initial privacy challenge for startups is what to prioritize on a very limited budget. Startups—especially seed-stage companies—have very limited funds for all legal and compliance. Given this financial reality, even the most well-informed and well-intentioned startup can only do so much at the outset when it comes to privacy and data security because every dollar that goes to the initial legal spend does not go to forming and running the business. But privacy is part of any credible business in the digital economy, so it is incredibly important for startups to work creatively with counsel to prioritize baseline privacy and security policies and practices that fit the profile of the early-stage company and can then be updated with minimal cost and expense as the startup scales.

This budget challenge is a different calculus with emerging companies in the health-care or financial industries, or those in the business of providing services to children. These startups have to fully understand and comply with the regulatory regimes and requirements of the Health Insurance Portability and Accountability Act/Health Information Technology for Economic and Clinical Health (HITECH) Act, the Gramm-Leach-Bliley Act and the Children's Online Privacy Protection Act, respectively. For emerging companies in any of these spaces, significant investment early on in legal and regulatory compliance is not an option; it is a necessity because their very business model depends on it.

Getting a handle on data flow, data practices and intended use cases should be seen more as a good business practice than a regulatory hurdle, especially for startups that rely on data in their business model.

BLOOMBERG BNA: What advice do you give to startups about moving from no or only a basic grasp of information governance issues toward mature privacy and data security policies and procedures?

Bohorquez: Start with your data. A startup cannot design and implement a privacy plan without first getting a handle on its data flow, data practices and intended use cases. Again, frankly this should be seen more as a good business practice than a regulatory hurdle, especially for startups that rely on data in their business model. Specifically, the startup needs to ask the following: What data are the startup collecting? How and for what purpose? Where are the data stored and how are the data protected? Who is the information shared with and why? How aggressive or how cautious does the startup want to be in its use of consumer information collected? The answers to all these questions are not only essential to a sound privacy plan but also integral to understanding how to better run the business and leverage the data to market to potential investors, business partners and consumers.

With an understanding of the data inventory, a startup should work with counsel to classify the data according to the level of sensitivity and assess the applicable laws, regulations and contractual obligations that govern the company's collection or use of certain information. I would also add that this goes beyond just consumer information. Startups should also be mindful during this process to identify sensitive internal corporate information such as trade secrets and employee information. In a very practical way, this data inventory and classification process will help the startup identify at a root level what reasonable and proportionate data security measures it should consider internally, e.g., encryption, and/or outsource, e.g., engaging a credible third-party vendor for payment processing or cloud storage.

The next step is to create an internal privacy policy that addresses how the company handles personal information so everyone is on the same page and held accountable. This is not a legal document in the sense that it should be chock full of ''wherefore'' and ''whereas.'' Rather it is a plain English mission statement on how the company handles customer information and addresses:

- accountability (who is responsible for what);
- notice to consumers and transparency;
- consumer choice and consent;
- data collection (and limits on unnecessary or sensitive personal information);
- data use cases and retention;
- disclosure to third parties;
- data security (reasonable and appropriate controls to protect personal information in its possession); and
- data accuracy and consumer access.

Where a startup may not have the wherewithal to create both an internal privacy and external privacy notice, it should always have the latter (which is typically what startups do). And similar to the internal privacy policy, an external privacy notice or policy should hit most if not all of the foregoing Fair Information Practice Principles (FIPPs) and be just as transparent and easy to read and understand.

There is, of course, the challenge of not only communicating the privacy policy to employees but monitoring and training startup employees on privacy. Given the fast pace and budget limitations of startup life, monitoring and training may be easier said than done, especially for seed-stage companies. That said, there are a few hacks a startup could use until it is big enough for a formal training program, such as prioritizing training of key employees, including a streamlined training as part of the annual performance review, or have counsel provide annual privacy training lunch and learns.

When moving to a mature privacy and data security program, startups also need to consider vendor management. Startups—like other companies—are responsible for the data they collect and share even when the data are processed by a third party. It is obviously important to deal with credible and vetted vendors, especially when handling your customers' personal information. Along those lines, a startup should also develop requirements for its vendors that will have access to users' personal information and ensure that they are meeting, or will meet, its privacy and data security policies. On the other side of the coin, where startups themselves are the vendor to a credible business partner, many times the established partner will ask for verification of basic privacy and data security practices and policies. Insurance companies also may require the same from startups before issuing cyber coverage.

Finally, as a startup scales it is important to ensure consideration of, and ultimately compliance with, the company's privacy policies through the life cycle of products and services. As is common for many startups, the original product or service typically undergoes a series of iterations. As the startup grows, the amount and type of data collected may vary. It is therefore very important to revisit existing data privacy and security policies whenever there is a significant shift in a startup's business model. Snapchat mentioned above failed to do exactly that. Early on in Snapchat's development, it did not track users' geolocation information, and its privacy policy affirmatively informed consumers that such data would not be collected. As the company evolved, it began tracking geolocation data without making changes to its privacy policy or notifying consumers. This resulted in an FTC enforcement action and then settlement requiring Snapchat to implement a comprehensive data privacy program, monitored by an independent privacy professional for the next 20 years.

It is important to remember that even for established companies the development of good privacy practices is an iterative process that does not happen overnight.

Another classic example of growing too fast without considering the privacy implications of the changes in data uses is Uber. Last fall, Uber was taken to task by what seemed like the entire Internet—as well as a U.S. senator—for its employees' alleged use of, among other things, its ''God View'' tool to spy on customers and reporters alike. Uber has since learned the error of its ways and brought on an experienced legal counsel and data security team to reboot its privacy program (14 PVLR 245, 2/9/15), but Uber easily could have avoided the public relations debacle by keeping its privacy practices up to speed with its data use cases.

It is important to remember that even for established companies the development of good privacy practices is an iterative process that does not happen overnight. Startups should not only revisit their policies when making any significant changes to data collection and use but as they grow get in the habit of conducting annual data privacy risk assessments to identify and address any holes in their security or privacy practices.

BLOOMBERG BNA: Are there general best practices and other guidance that startups across the board can make use of to inform their privacy and security, or is industry-specific guidance—such as the privacy principles for mobile applications developers created by the FTC, California Office of Attorney General (12 PVLR 80, 1/14/13) and Digital Advertising Alliance (12 PVLR 1316, 7/29/13)—more helpful?

Bohorquez: Over the last two years, the FTC and California attorney general have been very active on privacy and data security in general, and in mobile specifically, releasing various reports and guidelines on the topics. On the self-regulatory front, the Digital Advertising Alliance, among others, has released several self-regulatory principles on privacy and interest-based advertising and mobile.

But startup founders have even less free time than lawyers. On the assumption that they probably do not have time to read these somewhat lengthy regulator guidelines, here are a few best practices for startups gleaned from these reports:

> **Be transparent about your data practices:** Explain what information you collect from users or their devices and what you do with their data. If you share information with another company, tell your users and give them information about that company's data practices. On mobile, make sure the language is clear and easy to read on a small screen, and create just-in time disclosures and obtain affirmative consent when accessing sensitive information like geolocation, contacts, calendar or photos.
>
> **Honor your privacy promises:** Remember that your privacy policy is itself a promise to consumers that you will actually guard their personal information to the extent you so state. Ensure that all employees know and understand your policies, are trained and are putting into practice the promises you make to your users.
>
> **Set reasonable collection limits and keep user data secure:** Collect only the data you need that are consistent with the context of the transaction or relationship to the consumer; secure the data you keep by taking reasonable precautions against well-known security risks; limit access to data on a need-to-know basis; and safely dispose of data you no longer need.
>
> **Update your policies and procedures:** Revisit data privacy and security policies and procedures whenever a major change to the business model is made. Clearly inform users of any changes and update relevant personnel whenever changes are made.

BLOOMBERG BNA: Is trying to instill privacy by design and/or privacy by engineering principles a viable approach when it comes to startups?

Bohorquez: Yes. In the long run it is better to instill a privacy by design approach sooner rather than later. The only issues are how much you invest in privacy and security and when.

Privacy by design may at first sound like a bureaucratic fiat to certain startups, but the concept is at its core a business value—treat your customer's privacy and information with respect. I don't know any company—startup or otherwise—that wouldn't agree with that principle. All privacy by design does is provide a road map for best practices to honor that core business value. Getting up to speed on the FIPPs that underline privacy by design will make it easier for the startup to understand not only what should be done, but the reasoning behind why it should do it.

It is not only better for business from a reputational and regulatory perspective to be privacy and data security cognizant, but it also saves money on fixing your product down the line.

I have found that it is much easier—and cost effective—for startups to be able to instruct their engineers and coders on the way they want consumer data collected and stored from the start, rather than to go through the (often expensive) trouble of changing it down the line to comply with privacy issues they hadn't considered earlier. But it also takes flexibility on the lawyer's part.

We have worked with startups where we were engaged as counsel after the engineers were done, and it was simply too late and expensive to pay the coders to redo the work. In those situations, which are typically a low risk profile, we make a note with the startup to revisit the issue the next time the engineer works on that code and we incorporate the compliance steps then.

BLOOMBERG BNA: Is a startup with an advanced privacy and security infrastructure in a better position to earn the trust of venture capital (VC) investors?

Bohorquez: All other things being equal, yes. VC investors are looking at not only the business and the team but how competitive and crowded the space is.

In the health-care and financial technology industries in particular, a robust privacy and security program is a must, and many VCs may likely see a lack of discipline on this front as a red flag. And even in nonindustry regulated spaces like social media, a respectable privacy and security program demonstrates maturity and foresight, and one less risk that the VC has to worry about or spend its capital on. Robust privacy and data security can also be a powerful marketing tool. Wickr Inc., for instance, has gained tremendous traction with investors and consumers because of its strong security measures. For startups handing customers' personal information, reputable privacy and security infrastructure cannot only be a value add to their business model, but also a differentiator for VCs and other investors.

BLOOMBERG BNA: Do you agree that because a goal for many startups is to be acquired by a larger enterprise, having a handle on data security and privacy compliance issues would ease the mergers and acquisitions due diligence review process for potential purchasers and contribute to a higher valuation?

Bohorquez: Yes. Similar to making a startup more attractive to VCs, solid privacy and data security practices and reputation can positively contribute to a valuation and make a startup a more attractive acquisition target. For the acquiring company, strong privacy and data security policies and practices likely mean less litigation risk and less additional expenditures post-acquisition.

Solid privacy and data security practices and reputation can positively contribute to a valuation and make a startup a more attractive acquisition target.

It could also mean higher valuation driven by consumer goodwill. Recent research suggests that eight in 10 consumers are more likely to buy from companies that they believe protect their personal information. Nearly three out of four consumers agree that easy-to-understand privacy policies would increase their trust in these companies. Purchase prices of Internet and electronic commerce companies tend to over-index in their allocation of goodwill to the bottom-line. While most industries typically allocate more than 50 percent of a purchase price to goodwill, Internet and e-commerce companies reflect the highest allocation at 70 percent. All these trends suggest that a tech startup's goodwill and value is increasingly affected by how consumers perceive how a startup handles personal information and privacy.

In a world where everyone is collecting data, maybe it's better to be ahead of the pack on privacy instead of second-to-last. In other words, startups that affirmatively place themselves at the front of the privacy and security curve—instead of at the end of it or worse—will be better-positioned to compete for and secure an asset that may in the long run be worth even more than the data collected—consumer trust.