Privacy 101 for SMEs: The Best Defense is a Good Offense

By Omer Tene and Marc Groman, CIPP/US

Imagine you are a major retailer and have to disclose a few days before Christmas that hackers stole credit card details and personal data on about –oh, 110 million shoppers – from your secure safe. Or that just as your app is experiencing hockey stick growth, leading tech blogs and media blast you for uploading users' contact lists to your servers without permission.

Hearing news like this, you probably cringe at the thought that this might happen to you. But, of course, you are not a major retailer or global corporation, or even an app with tens of millions of users commanding media attention; you are a small or medium enterprise (SME), so you don't have to worry, right? Wrong! Privacy and data security must be strategic considerations for every business, including garage entrepreneurs developing cool apps or analytics companies with half a dozen employees.

If you touch data –and who doesn't these days? –you need to think about responsible information management from cradle to grave. The risks include not just security breaches but also a variety of privacy glitches, such as FTC enforcement actions alleging insufficient or inaccurate notice in a privacy policy, violation of user expectations or architectural design flaws in hardware or apps. The consequences can be grave, including enforcement actions by regulators, class-action lawsuits or worst of all, reputational injury just as you are trying to grow your business and seek funding from investors. Given the high-profile privacy issues over the past several months, you can expect angel investors and strategic partners to seek confirmation that you are privacy-savvy from the start.

Last week, marketing technologist and Ion Interactive CTO Scott Brinker released version 3.0 of his "marketing technology landscape supergraphic." Nearly a thousand companies, many of them SMEs, were categorized into 43 sectors of an increasingly

elaborate market awash with data. And as Brinker writes, "this graphic is not comprehensive … There are many more companies—indeed, entire categories — that were not included merely due to the constraints of time and space. And by the time you read this, it will inevitably be out-of-date due to new launches, re-launches, expansions, exits and mergers. The pace of change in this field is breathtaking."

Do all of these players have their houses in order? What should you do as an SME to help manage privacy and data security risks?

Employing expensive consultants and law firms may not be an option right out of the gate. To get it right, remember that the best defense is a good offense. Attack the problem early; be proactive; prepare in advance; implement Privacy by Design; follow industry best practices. Most important, you need to have rudimentary issue-spotting skills. Half a day of privacy training can do wonders and should be seen as a critical investment for any start-up.

Here are some down-and-dirty tips to help you safeguard your data, build trust and avoid boosting newspaper sales with sensationalist business titles:

First, simply recognize that privacy and data security are not to be ignored and appoint a person responsible for both. It doesn't necessarily need to be an IT person or a lawyer but rather somebody in the organization has to own the issue. In privacy-lingo, we call it "accountability."

Second, understand your business model, and know what data you are collecting. Don't settle for open-ended or vague responses like "nothing sensitive" or "no personal data." Someone needs to understand exactly what data is being collected and why. The distinction between "PII" and "non-PII" can be very fine and highly technical. Don't use intuition. It doesn't work here. As an example, if you are collecting consumers' birthdates, examine what data you need and for what purpose—is year sufficient, or month and year or do you require an exact date? As with most data elements, the less data you collect and store, the lower the risk of identity theft or other harm in the event of a breach. And knowing the exact age of a consumer may create other risks of liability for your entity.

Third, sensitize your entire staff to the issue. It's not that your employees need to

become privacy professionals who "live and breathe" privacy, but they need to know why it's important, what they can do about it and whom they should address with questions or concerns. You want to flag the topic and encourage issue-spotting by your staff. It's about the bottom line and reputation—a hard-core business issue not an arcane compliance matter. Give examples—nothing works better than a few examples of a privacy disaster or data security incident to wake people up.

Fourth, find out if your business model touches any areas with sensitive data that may be subject to specific laws. Are you dealing with health data, financial data or children's data? Are you moving data around between the U.S. and Europe? If so, it may be time to call counsel.

Fifth, look for self-regulatory associations in your industry and check what they require. Consider joining, but if it isn't feasible in the early stages of your business, you can benchmark your practices against the requirements of the self-regulatory framework. Strive for more but make sure that you at least comply with industry best practices.

Sixth, take this test: Do I want my company's name to appear in *The Wall Street Journal* next to this business practice? Does this line of business generate enough revenue to justify the risk? If you pause, think again.

Let's get a bit more specific.

» Be careful about just cutting and pasting a privacy policy from a similar business model. To be sure, it's very common for small businesses to do so. But it's also a good way to get in trouble. No case is easier for regulators or individual litigants to prove than one based on inaccurate or deceptive promises in a privacy policy. Make absolutely sure the representations accurately reflect your business practices. Don't over promise in your privacy policy. It's a legal document, which creates liability. Avoid terms like "never" unless you are 100-percent certain you will "never" do that.

» Have a data retention policy? Don't just keep data because it's there. And that includes e-mail, documents, etc. You can't lose what you don't have. And yes, we know you are all high-tech, but don't forget about paper. Get a shredder

and use it to grind employee files, confidential data from audits, anything sensitive. Regulators have brought enforcement actions against companies for data breaches based on the failure to properly dispose of paper records.

» In the marketing business? Do some due diligence on your data sources. The NAI code, for example, has a "reliable sources" requirement that directs companies to do basic homework on business partners and sources of data. When examining a business partner, companies should look for membership in a self-regulatory association or seek a representation that the data provider has the necessary authority or permission to share the information.

» If you offer any type of choice mechanism—for e-mail, catalogues, interest-based ads, telephone calls, data sharing—make sure that it works. Again, don't over promise here.

» Most SMEs today have a website. Do you know what data is collected across your site? How? If you have forms or a shopping cart on your site, are they secure?

For more useful resources and in-depth analysis, we suggest you use the business resources page on the FTC website. It's a great place to start with some very sound basic tips regardless of your business model or the size of your company. And of course, go to the IAPP's Resource Center, which has practical tools, checklists, templates and more in-depth research from the Westin Research Center.

For more useful resources and in-depth analysis, we suggest you use the business resources page on the FTC website. It's a great place to start with some very sound basic tips regardless of your business model or the size of your company. And of course, go to the IAPP's Resource Center, which has practical tools, checklists, templates and more in-depth research from the Westin Research Center.

About the Authors

Omer Tene is Vice President of Research and Education at the IAPP where he administers the Westin Fellowship program and fosters ties between the industry and academia. He is also Vice Dean of the College of Management School of Law, Rishon Le Zion, Israel; an Affiliate Scholar at the Stanford Center for Internet and Society; and a Senior Fellow at the Future of Privacy Forum. He has published extensively in US and European law reviews about big data, online tracking, and international privacy law.

Marc Groman, CIPP/US, is the President and CEO of the Network Advertising Initiative. He leads the organization's growth and ongoing efforts to develop and maintain high standards for Interest-Based Advertising. Prior to joining the NAI, Marc served as the FTC's first chief privacy officer, where he built an award-winning privacy program from the ground up. In 2009 and 2010, he served as counsel on the Energy and Commerce Committee in the U.S. House of Representatives. While on the Committee, Marc drafted a significant consumer privacy bill and shepherded data security and breach notification bills through passage in the House.