iapp

The Top 45 Security and Privacy

# BLIND SPOTS

By Jeff Northrop, CIPP, CIPT, CISSP

# THE TOP 45 SECURITY AND PRIVACY BLIND SPOTS

By Jeff Northrop, CIPP, CIPT, CISSP

Consumers are increasingly concerned with protection and appropriate uses of their personal data. You can see evidence of this in the steady drumbeat of news from major outlets covering this issue; you can see it in the public uproar over each new corporate breach of public trust that comes to light, and you clearly saw it in the hypersensitive response to each Snowden revelation as that story unfolded.

The level of attention to—and the intensity of public consciousness over—data protection issues is unprecedented.

As we become more innovative with ways to collect personal data, uncover more uses for it and tie the success of our organizations ever more tightly to it, this consumer sensitivity is only likely to grow.

Politicians, regulators and markets are reacting to this growth of consumer sensitivity in significant ways. Reactions to the massive breach at Target, the celebrity photo leaks and the political turmoil resulting from Sony's breach demonstrate a trend. The demand for accountability in respect to privacy protection is growing, and security professionals are finding themselves in part responsible for this issue.

For decades, information security functions have fought for the responsibility to monitor the flow of information through the organization, in paper and digital formats, throughout its entire life cycle, and to determine the existence and accuracy of data classification. This effort has largely been successful. However, if all data flows through security's filters, it is incumbent upon them to implement the proper controls to ensure personal data is properly collected for its intended use, either to own that responsibility or, at a minimum, to flag potential issues for compliance, marketing and privacy functions.

These types of considerations are new to many in the security profession, and this situation is creating an environment rife with blind spots.

The challenge is twofold. First, it is important for security professionals to recognize the breadth and scope of these new responsibilities, and, second, those same professionals need to understand the context and risks inherent with them. Sometimes the mistakes made in these blind spots result in nothing more than a slap on the wrist; other times, they can utterly destroy a company.

To assist in addressing these challenges we have collected 45 lessons learned from common mistakes occurring in these blind spots. Each blind spot is accompanied by an example adding context and aiding the communication of the importance of this risk to organization executives.

## 1. Enforce Strong Password Policies

Possibly the most discussed breach of 2014 was not the JP Morgan breach, the breach at Home Depot or even Target; it was the publication of 500 private photos from more than a dozen celebrities. While Apple iCloud was the source of the photos, the service's security wasn't at fault. Rather, the breach resulted from targeted attacks against the celebrities' passwords.

The most robust security measures can easily be foiled by a weak password. Most systems have mechanisms for ensuring users create acceptably strong passwords; use those features.

## 2. Ensure Proper Procedures When Terminating Employment

On June 16, 2014, Joshua Howell downloaded patient information from DCH Regional Medical Center in Tuscaloosa, AL, onto his personal laptop, a violation of the center's policies and a potential Health Insurance Portability and Accountability Act violation. He did this on the same day he was terminated from the hospital.

When terminating an employee, it is important to prevent access to all systems, particularly those with sensitive information, prior or during termination notice to that employee.

## 3. Keep Your Data Accurate

In July of 2013, a jury awarded Julie Miller $18.6 million in punitive damages and $180,000 in compensatory damages after she spent two years unsuccessfully trying to get Equifax Information Services to fix major mistakes on her credit report. The errors included erroneous accounts, collection attempts and a wrong Social Security number and birthdate.

It is well understood that if you collect sensitive information you must protect it, but it is also important, particularly if decisions are based off this information, that the information be up-to-date and accurate.

## 4. Collecting Information Without Asking

Aaron's, Inc., a national franchise of rent-to-own stores, allowed franchisees to install software on the computers they rented that permitted the store owner to surreptitiously track consumers' locations, capture images through the computers' webcams and activate key-loggers that captured users' login credentials for email accounts and financial and social media sites. The Federal Trade Commission (FTC) sued Aaron's, stating, "By enabling their franchisees to use this invasive software, Aaron's facilitated a violation of many consumers' privacy."

You shouldn't collect personal information without proper consent from the person of interest.

## 5. Pay Close Attention to Your Alert Systems

Possibly the most reported business news in 2014 was the hack and subsequent breach in late 2013 at Target resulting in the theft of millions of credit card numbers. Unfortunately, while Target's security systems had alerted administrators to the malware that led to the breach, those alerts where ignored.

Security teams are often overwhelmed by the torrent of information coming from noisy alert systems, threat intelligence feeds and other sources. Finding a process for properly assigning risk to that information so proper prioritization can occur is paramount.

## 6. Logging IP Addresses May Violate Privacy Policies

In late 2007 Peter Scharr, Germany's data protection commissioner, argued that Internet Protocol (IP) addresses should be considered personal information, but a court ruling in Washington state in 2009 decided it wasn't. Which is it, then? As a general rule of thumb, if you can combine an IP address with other information to identify an individual, it should be considered personal information. In either case, only collect IP addresses when there is a specific purpose for that information.

Many organizations make public promises that they don't capture any personally identifying information. Yet just about every website or web-based application keeps a log of visitors to their sites, most of which capture IP addresses.

## 7. Shared Servers May Be Confiscated by Authorities

Liquid Motors provides inventory management and marketing services to national automobile dealers. It was one of 50 companies whose servers were seized by the Federal Bureau of Investigation in an unrelated matter. As a result, the company was put out of business.

If you are running critical business processes on servers that are shared with other enterprises, you need to plan for the risk of confiscation and the immediate and unplanned shutdown of those servers.

## 8. Track Your Unstructured Data

In April of 2012, Memorial Sloan-Kettering Cancer Center in New York discovered that PowerPoint presentation files posted on two websites exposed the personal information of 880 patients. The information behind the charts contained in these presentations included patient names, clinical information and, in some cases, Social Security numbers.

Tracking and securing unstructured sensitive data, residing in Office documents or email stores, can be far more difficult than keeping a watchful eye on your structured data. However, it has become a critical responsibility for security teams to ensure that data is secure regardless of the format.

## 9. Unauthorized Use of Information

In 2012, Spokeo paid the FTC $800,000 to settle charges that it violated federal law by compiling and selling personal information for use by potential employers. The complaint against Spokeo alleged that it violated the Fair Credit Reporting Act by marketing its consumer profiles without making sure they would be used for legal purposes.

Many marketers and sales people scheme to aggregate as much information as possible about their targets in order to give their pitches the best chance of success. The interconnectedness of our modern culture makes this type of activity increasingly easy, but just because you can do something, doesn't mean you should.

"Just about *every website* or web-based application keeps a log of visitors to their sites"

## 10. Use Scraped Emails for Mass-Marketing Campaigns

A complaint filed in 2013 alleges that LinkedIn violated users' privacy by accessing their external email accounts and downloading their contacts' addresses. The complaint accused LinkedIn of sending marketing pitches to new users whose email addresses LinkedIn obtained as part of its effort to acquire potential new users.

Regardless of how email addresses are collected, many laws and regulations around the globe do not permit, or greatly limit, your ability to use these addresses for marketing purposes without the email address owner's consent to do so.

## 11. Unintentionally Collecting Information from Children

In an effort to boost its audience, Yelp created a streamlined sign-up process for its mobile app. Unfortunately, Yelp neglected to include a check for the applicant's date of birth. As a result, it accidentally collected personal information from minors and a $450,000 fine from the FTC for violating the Children's Online Privacy Protection Act.

Regulations aggressively protect minors. If you believe your application or service will be used by minors, make sure to include a date check to verify their eligibility to send you their personal information.

## 12. Setting a Tracking Cookie Without Notice in Europe

In 2014, the Spanish data protection authority fined two companies for failing to clearly and transparently explain their use of cookies used to track website visitors.

In 2011, the European Union (EU) Privacy and Electronic Communications Directive set requirements for websites using mechanisms that track users to obtain permission from visitors to their websites before the mechanisms, such as cookies, can be used. If you have operations or customers in the EU, ensure your website clearly explains any mechanisms in use to track visitors.

## 13. Employees Peeking at Private Information

Humans are voyeuristic by nature, and, as a case in point, when a data quality manager at the National Health Service in the UK had the opportunity to peek at the health records of over 400 female patients, he acted on his impulses. Over a nine-month period, he looked at the medical records of 413 patients a total of 597 times.

Certain roles within organizations require access to sensitive data. Training and education about appropriate use of sensitive data can limit risks of misuse, but technical controls should be in place as well to audit data access and uses.

"If you have operations or customers in the EU, ensure your website clearly explains any mechanisms in use to track visitors."

## 14. Use of SaaS Applications

In the spring of 2014, a competitor to Dropbox, the popular file-hosting service, embarrassed Dropbox when it publicized that its competitor's service hosted links to a number of sensitive files, such as financial documents, that were inadvertently publicly available. Dropbox quickly disabled access to links that were previously shared and implemented a patch to prevent shared links from being inadvertently exposed.

If users on your network with access to sensitive files make use of services such as Dropbox, GDrive or Box, you run the risk of them mistakenly exposing that information to prying eyes.

## 15. Disclosure of Sensitive Information by Association

In June 2001, Eli Lilly sent an email message to more than 650 likely Prozac users. Unfortunately, due care was not taken when addressing the email with all recipients addresses in the "To" field of the message. This inadvertently disclosed the identities of all recipients to each other. This simple lapse in judgment resulted in Eli Lilly paying out millions of dollars in fines.

Email is an effective and inexpensive method for messaging to a large group, but improper configuration of the message leading to inadvertent disclosure of sensitive information is an easy mistake to make. Proper technical controls should be put in place, or only those with proper training should be permitted to send bulk communications.

## 16. Shadow IT Services

Microsoft SharePoint is a popular tool for sharing files within an organization. It also makes it easy to publish documents to the Internet, putting sensitive information shared on the system at risk of a breach.

A specifically crafted Google search will rapidly uncover mountains of confidential information mistakenly published on SharePoint servers. Ensure users of software capable of publishing information to the Internet are properly trained or are limited via technical controls.

## 17. Unintended Discovery of Personal Details from Data Aggregation

In the mid-1990s, the Massachusetts Group Insurance Commission thought it would be a noble idea to share de-identified health information of every state employee. The hope was that this data would be used to spark innovation in the state. Unfortunately the project was cut short when Latanya Sweeney, then a grad student at Harvard and later chief technologist at the FTC, discovered the data could easily be reidentified by combining it with publicly available voter registration records.

Our increasingly interconnected world means there is an increasing number of data points tracking numerous aspects of our lives, which makes "connecting the dots" easier than ever. If sensitive data is being shared, ensure aggregation techniques cannot be used to reidentify the data subject.

## 18. Personal Defamatory Remarks on an Internal Social Network

While published examples of this are rare, one of the first things a prosecutor will do when an organization is accused of illegal behavior is to subpoena all digital records. This includes dialog on internal social networks.

Many of us consider internal chat servers, discussion boards and other internal communications to be relatively secure, but communications should be limited to business-related topics or risk potentially libelous exposure.

## 19. Capturing Search String Information from Personal Devices

With Apple's release of OS X Yosemite, version 10.10, came changes to a number of features in the operating system. One of those changes included a default setting that automatically sent any string entered into the Spotlight application back to Apple. When this was revealed there was a strong angry public backlash.

When users enter a string of characters into a search box, there is the potential they are looking for something they wouldn't want others to know about. If your application, service or security appliance is logging search strings, ensure those entries cannot be tied back to an individual or that the information is only accessible by individuals authorized to view such information.

## 20. Sharing Unique Identifier to a Third Party

Uniquely identifying users of an application is a common method for controlling access and personalizing the user's experience. In 2012, it was revealed that MySpace was inadvertently sharing its users' unique identifiers with third-party advertisers, disclosing identities in a way forbidden by its policies. As a result, MySpace will be subjected to regular outside privacy audits for the next 20 years.

If your organization is making use of unique identifiers that are ultimately tied to personal information, then the identifiers themselves should be treated with the same care as all other personally identifiable information.

## 21. Unique Identifiers Put Anonymity at Risk

In October 2014, The Guardian wrote a scathing expose on Whisper, a social media app. The article detailed allegations of how Whisper, despite promises of anonymity, was tracking its users. The news created a backlash, putting the future of the company at risk. Whisper strongly, and publicly, defended itself, but a couple of days after the story broke, Jonathan Zdziarski performed a forensic analysis of Whisper's app, revealing that regardless of what privacy options the user selects, the app will send not only location information back to Whisper but potentially unique identifiers as well, further exacerbating the backlash.

Unique identifiers are used in all sorts of applications, usually to help deliver personalization features to the end-user, but if you are promising anonymity, relying on unique identifiers is problematic.

## 22. Collecting Information for Marketing Purposes Without Permission

In 2013, Lead Concepts produced a series of emails requesting that the recipients reply with their names, the names of their spouses and their ages. No explanation was provided for why the company was requesting this information. When the Vermont Office of the Attorney General learned that the intent was to use this information to produce leads for insurance, i6 fined the company $90,000.

If your organization introduces mechanisms for lead capture, the data subject needs to be notified of the purpose of that information's collection, and if the intent is to market to them, you should ensure data subjects were asked for explicit permission to market to them at the time of capture.

## 23. Develop Applications with Security in Mind

In 2013, the FTC sued HTC America for failing to properly vet its phone's operating system for security flaws. One particular flaw created the potential for attackers to gain personal information stored on the device. The FTC suit charged that HTC failed to take reasonable steps to secure the software it developed for its smartphones and tablet computers, placing millions of consumers at risk.

If you are developing applications you must provide engineering staff with adequate security training, test the software for potential security vulnerabilities and establish processes for receiving and addressing vulnerability reports.

## 24. Do What Your Policies Say You Do

In 2001, Microsoft promised its identity product, Passport, "achieves a high level of Web Security." However, the Electronic Privacy Information Center filed a complaint accusing Microsoft of falsely representing Passport's privacy and security measures, and as a result, the FTC took action against the company. Microsoft ended up settling the complaint with the FTC.

Nearly all organizations publish policies and procedures that include promises for the protection and appropriate use of the data they steward. It is critical that organizations do everything those published materials promise.

## 25. Emailing Canadians Without Explicit Consent

On July 1, 2014, the new Canadian Anti-Spam Law went into effect. If you have operations located in Canada or are sending email to Canadian residents, then this law applies to you. Any email, instant message and text message and some social media communications containing messages encouraging recipients to take part in some type of commercial activity sent to a Canadian resident is subject to the new law.

While there is a transition period extending until July 1, 2017, during which you can take steps to ensure you are compliant with the law, the liability for noncompliance includes fines of CAD $1 million to $10 million per violation.

## 26. Use Secure Channels To Transmit Sensitive Information

Between November 24, 2003, and June 28, 2004, more than 45 million credit and debit cards of TJ Maxx and Marshall shoppers were stolen. At the time, this was believed to be the largest such breach of consumer information. The vector that allowed the theft to take place was the unsecured transmission of the card data through a wireless connection.

When transmitting sensitive data, ensuring the communications channel is properly encrypted and/or secured is an absolute must.

## 27. Know the Location of Your Sensitive Data

In June 2014, the Ponemon Institute published findings highlighting that the majority of IT practitioners identify that not knowing where their sensitive data resides is the number one issue "keeping them up at night."

In the previous year, the U.S. National Security Agency published a book on how to use Google's search engine to gain intelligence for its cyber-spies.

These are not unrelated. Knowing the location of sensitive data in your organization is the first step, and a necessary step, in ensuring that data doesn't leak out of your control and onto the publicly accessible Internet.

> "If your organization introduces mechanisms for lead capture, the data subject needs to be notified of the purpose of that information's collection"

## 28. Know Your Global Compliance Obligations

In 2011, a 24-year-old Austrian law student launched a campaign to highlight Facebook's shortcomings regarding compliance with European data protection laws. His campaign led to a probe by a European privacy regulator and questions from U.S. Congress as well as pending lawsuits.

Privacy laws and regulations around the globe vary widely between countries and regions and are changing rapidly. If you have customers and/or operations in foreign locations, it is important to understand your obligations not just at home but in those locations as well.

## 29. Encrypt Sensitive Data at Rest

In April 2014, the Department of Health and Human Services fined Concentra Health Service $1.7 million for a breach that involved the theft of an unencrypted laptop. The laptop contained protected health information from its Springfield, MO-based physical therapy center. Unfortunately, this story is increasingly common: Sensitive information is loaded onto a laptop, smartphone or tablet, which then goes missing.

If you manage the devices of executives, sales people or others who have legitimate reasons to be traveling with sensitive information, ensure that information on those devices is properly encrypted, minimizing the risk in the event of theft or loss.

## 30. Willingly Manipulating People's Emotions

In the summer of 2014, Facebook released the results of a study conducted by its data scientists. The study demonstrated Facebook's ability to manipulate users' moods by manipulating the tone of their news feeds. When researcher published the results showing that positive news had a positive contagion effect on users and negative news produced the converse reaction, people were shocked.

Not surprisingly, people do not like the idea that the web service they are using is manipulating their emotions. As a result, Facebook has implemented an ethics review board that screens future studies. Developing the culture and processes to ensure your organization approaches new projects with an eye toward maintaining ethics can prevent major headaches and brand damage.

## 31. Regulators Are Increasingly Technically Adept

In October 2014, the FTC hired privacy and technology expert Ashkan Soltani to serve as the its chief technology officer. He has a deep technical knowledge, as did his predecessor, Latanya Sweeney. The FTC and other regulatory authorities around the world are strengthening their technical expertise. This trend is leading to increasingly technical regulations that require organizations to focus on and mature their privacy and security controls.

If you are gambling on flying under the radar with lax cybersecurity and data privacy controls, then you are setting yourself up for a potentially catastrophic ripple effect throughout your organization in the event of a data breach.

## 32. Keep Software Up-To-Date

The Department of Energy, the state of Washington's court system and CorporateCarOnline, a limousine service, all suffered highly publicized attacks in 2013. The commonality among all of these attacks is that each was running an unpatched and outdated ColdFusion server.

The easiest and most dangerous posture in information technology is "if it ain't broke don't fix it." New vulnerabilities are discovered and patched all the time; you need to keep on top of it for all of your services and servers.

## 33. Social Engineering Techniques

A successful phishing attack targeting the South Carolina Department of Revenue resulted in loss of data on 3.8 million people, including information on 1.9 million dependents, nearly 700,000 businesses and the information on 3.3 million bank accounts. All it took was for one Department of Revenue employee to click on a link in an email that installed undetected malware.

Social engineering results in more data breaches than any other threat. Training users is the best way to mitigate this risk.

"People **do not** like the idea that the web service they are using is manipulating their emotions."

## 34. Carefully Monitor and Vet Applications Built on Your Platform

In October 2014, news broke that thousands of private Snapchat photos were leaked online, resulting in a regulatory order for Snapchat to submit itself to third-party privacy audits for the next 20 years. The company promotes itself as a way to share photos that disappear after a short period of time with friends and family. Snapchat also promotes itself as a platform on which other services can build their businesses. In this case, the service snapsaved.com, which built on Snapchat, was the source of the leak.

Creating a platform that can be leveraged by others, thus creating an economic ecosystem, is a newly developing business model. If your organization is heading in this direction, you need to accept some responsibility for others' security as well as your own.

> "Not knowing where their sensitive data resides is the *number one* issue 'keeping them up at night.'"

## 35. Responsibility for Sensitive Data Sent to Authorized Third Party

The Florida Department of Highway Safety and Motor Vehicles and a number of state officials were sued in 2010 for violating the Drivers Privacy Protection Act. The agency sent a large amount of sensitive data to an authorized third party who, in turn, forwarded that information to another unauthorized company.

Responsibility to protect the data in your possession extends to outside parties that lawfully obtain that data from you.

## 36. Don't Collect Information that Reveals Habits of the Individual Without Consent

In 2013, a UK blogger discovered that his LG Smart TV was automatically sending information on his viewing habits back to the Korean company. Reportedly, the company was going to use this information to profile viewers, then sell access to those profiles to advertisers. While not illegal, public reaction was less than favorable, resulting in LG updating the default preferences on those models.

Consumers don't like it when they are surprised that personal information about them is being collected and sold. While many laws and regulations require transparency about such practices, even in situations where legal obligations don't require such disclosure you should be clear about your practices to your customers.

## 37. Recording Location Information Puts Anonymity At Risk

In 2013, an Android flashlight application developed by Goldenshores was one of the most popular applications in the Google Play store. The application was free to use but, like many other free applications, financially supported itself by delivering in-application advertising. In order to deliver appropriate advertising, the application collected precise geographic location information without disclosing this practice to users. As a result, the FTC sued Goldenshores, which subsequently entered a consent decree with the FTC, agreeing to operate under the watchful eye of the regulator for the next 20 years.

GPS functionality is nearly universal in today's mobile devices, making location information easily accessible to application developers, but if your policies don't explicitly mention you are capturing that information, don't capture that information.

## 38. Collecting Sensitive Information Without Allowing the User To Opt Out

The in-vehicle communications service OnStar transmits a number of sensitive data points about the vehicles in which it is installed. In 2012, General Motors had plans to update its OnStar customer agreement to permit the sale of the information it collected. The policy update contained no mechanism for opting out of the program. A strong public outcry killed the plan before it launched.

If your organization is collecting sensitive information and plans on monetizing that data, ensure the data subjects have an easy mechanism for opting out of the program or, better yet, design the program to be opt-in.

## 39. Hash Passwords

In 2012, RockYou was fined $250,000 by the FTC for allowing hackers to access the personal information of 32 million users. During the FTC's investigation, it was discovered that passwords for the service were stored in plain text.

While hashing passwords is no guarantee that the password cannot be recovered, it is exceptionally more difficult to obtain than if it wasn't encrypted at all. There are a number of methods for encrypting sensitive information; pick one, use it and make sure it is properly implemented.

## 40. Changing the Behavior of Someone Else's Application

In 2012, Google paid $22.5 million—at the time the largest fine ever levied by the FTC—to settle allegations it breached the Apple Safari browser. The allegations accused Google of placing cookies in Safari, actively subverting Safari's tracking preferences and deceiving consumers.

Combining, enhancing and leveraging functionality from other applications and platforms is a common practice among today's applications. While this behavior is not only expected, it is encouraged; you should never intentionally subvert user and application preferences.

## 41. Over-Collection of Information Can Occur Via an Analytics Service

In 2013, Has Offers, a mobile analytics platform, was using collected Facebook data to help track the performance of its targeted advertising. Unfortunately, Has Offers over-collected, violating Facebook's service terms. In admitting its mistake, Chief Executive Peter Hamilton noted, "Our MobileAppTracking platform inappropriately allowed advertisers to obtain device-level attribution and performance data. This was a mistake on our part."

Modern platforms that help reveal trends and vet successful strategies through analytics are prolific and powerful. It is an easy choice to maximize the potential these platforms offer by collecting as much detailed information as possible, but it is just as easy to take it too far.

## 42. De-identification of Data Is Difficult; Really Difficult

In 2006, Netflix announced a $1 million prize to the individual or team that could create an algorithm to more accurately predict a user's movie preferences. To facilitate this contest, Netflix released a de-identified data set of video rental histories. Unexpectedly, some rental histories were reidentified, and that reidentification resulted in Netflix paying millions of dollars in fines.

De-identification of data is a powerful tool helping organizations maximize the value they can extract from the data they steward. However, de-identification is difficult, and the risks of reidentification are high, so proceed with caution.

## 43. Protect Backups Like You Protect Production Servers

In 2011, backup tapes containing names, Social Security numbers, addresses, birth dates, phone numbers and laboratory tests were stolen from Science Applications International. The tapes included information on 4.8 million military personnel.

Backups need to be treated with the same protection considerations as production systems; they often contain the same sensitive information.

> "There are a number of methods for encrypting sensitive information; pick one, use it and make sure it is properly implemented."

## 44. Understand Your Audience's Expectations

In 2014, the well-funded education start-up InBloom imploded. Even the backing of such luminaries as Bill Gates could not stop the backlash parents launched against the company when they found out what data was being collected on their children. Parents' protests were soon followed by similar protests from powerful politicians. The protests ultimately led to InBloom's demise.

In an environment where consumers are hypersensitized to revelations about how their data is being collected or used, it is critical that your organization communicate openly and behave in a manner consistent with consumer expectations.

## 45. Don't Collect Data You Can't Use

In 2013, in an effort to improve the performance of its application, social mobile network Path cached users' address books. That way, when a user made the decision to permit Path to obtain that information, it would happen almost instantaneously. However, when the function was reported publicly, users were upset, and the FTC sued.

Regardless of the intent, if you are gaining access to personal information, the subject must be made aware.

## CONCLUSION

Of course, this is just the tip of an iceberg of potential issues. Every organization is unique and has its own unique challenges and potential for privacy and security mishaps. You might see this list as the bare minimum going forward—commit any of these sins and you'll likely have a regulator from some jurisdiction breathing down your neck.

If you'd like to learn more about the deep and broad field of privacy and data protection, the IAPP is here to help. Come visit us at www.PrivacyAssociation.org and get started on your path to becoming a privacy professional.