Bloomberg Law

Privacy and Security Law Report®

Reproduced with permission from Privacy & Security Law Report, 16 PVLR 356, 3/6/17. Copyright © 2017 by The Bureau of National Affairs, Inc. (800-372-1033) http://www.bna.com

Privacy Pros

Hiring managers and in-house counsel are finding themselves interviewing candidates for senior in-house positions or important outside counsel roles, even though the interviewers lack expertise in privacy and data security, the author writes as he provides hiring managers with advice for interviewing candidates.

Interviewing the Privacy/Data Security Candidate: A Guide for the Non-Expert Hiring Manager

BY STEPHEN L. TUPPER

Privacy and data security is hot. Hiring managers and in-house counsel are finding themselves interviewing candidates for senior in-house positions or important outside counsel roles in those fields, even though the interviewers aren't experts in privacy and data security. Complicating all of that is the fact that, just as with other great industrial booms, there are plenty of carpetbaggers and pretenders vying for the enterprise's attention and resources. How's a hiring manager or an in-house lawyer to separate the wheat from the chaff?

Here are a few lines of questioning that hiring managers and in-house counsel can use in interviews with would-be privacy and data security personnel, as well as some background information for each and what it means if a candidate gets the answer right or wrong. Some questions are foundational and designed to identify non-hackers early. Some are more fine-tuned and nuanced and can let you make finer distinctions between the candidates.

Any interview should, of course, be wide-ranging and cover more than just these items. But, for the non-specialist hiring manager, these questions and answers can let the manager start from something other than an empty page. And perhaps serve as a jumping-off point for other questions that are important to the job description.

Stephen L. Tupper is a member of Dykema Gossett PLLC in Bloomfield Hills, Mich., in the Privacy, Data Security & E-Commerce Practice Group.

Policy Questions

Policy questions let you understand both the candidate's knowledge and practical application. You might ask the candidate to talk about whether, and how, the company might make use of the personal information that it holds about its customers for marketing purposes. The candidate should, at a minimum, talk about

go/no-go decisions about using the information and how the marketing might be carried out.

The go/no-go decision should include considerations, including:

- whether the company has the right to use the information to market;
- whether the company obtained the data subject's consent to market when it collected the information;
- whether there's any legal prohibition on marketing to the data subjects;
- what were the data subjects' expectations about use of the personal data were when it was collected;
- whether any public relations fallout would occur if the company used the information for marketing (best paraphrases ''would this seem creepy?'');
- whether the data is subject to any particular limitations because of the kind of data involved (here meaning ''nonpublic personal information'' under the Gramm Leach Bliley Act, ''protected health information'' under Health Insurance Portability and Accountability Act (HIPAA), information about persons younger than 13 under the Children's Online Privacy Protection Act (COPPA), and similar kinds of information); and
- whether the information will be combined with other information from other sources.

Things to think about in deciding how to go about marketing should include:

- if e-mail communication is used, compliance with the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN SPAM) Act;
- if telemarketing, including text messaging, is used, compliance with the Telephone Consumer Protection Act (TCPA);
- special considerations under TCPA when using text messaging, fax or mobile phones (which can require heightened levels of consent by the person to whom you're marketing, opt-out notices, use of autodialers and inclusion of very specifically worded and presented notices required by regulation);
- Federal Trade Commission and other guidance about behavioral marketing (defined by the FTC as ''tracking of a consumer's online activities over time—including the searches the consumer has conducted, the web pages visited, and the content viewed—in order to deliver advertising targeted to the individual consumer's interests;'' and
- best practices published by organizations like the Mobile Marketing Association.

A candidate should be able to talk engagingly about rights in data, expectations of the receivers of the communications, the regulatory environment and other relevant considerations. A reasonably detailed and practical discussion by the candidate should give the candidate the benefit of the doubt. A candidate who is clutching at straws probably doesn't understand the environment, hasn't done this work before, or both, and is probably not going to be helpful to you. Note that, even if marketing isn't one of the company's major considerations, (a) it likely will be at some point and (b) electronic marketing is such a core part of the canon of privacy practice that, absent a really good explanation for the lack of knowledge, a candidate who's not familiar with this subject matter deserves a jaundiced eye.

A candidate should be able to talk engagingly about rights in data, expectations of the receivers of the communications, the regulatory environment and other relevant considerations.

International Issues

Cross-border data flows can have major consequences. Different countries and regions have very different approaches to privacy law. Europe is probably the most important example. Asking a candidate about the differences between U.S. and European privacy law is a great way to tease out the candidate's knowledge.

The U.S. has a ''sectoral'' model of privacy law. For example, financial privacy is governed mainly by the Gramm Leach Bliley Act, health-care privacy is governed by the HIPAA, education is covered by the Family Educational Rights and Privacy Act (FERPA) and so on. Things that aren't covered by specific law tend to be covered by the Federal Trade Commission Act or tort law or aren't covered at all.

Europe has a ''holistic'' model that covers everything. It's really broad. All personal data is covered (not just name and credit card numbers, but dog's name, sports team preferences, etc.). And just about anything you can do with the information—from collecting it to sorting it to sharing it and even destroying it—(what the Europeans call ''processing'') is covered. Absent the consent of the data subject or several narrow exceptions, European law requires that the personal data of European Economic Area member state citizens remain subject to those European-style protections wherever it goes (thus all the attention to the European Union-U.S. Privacy Shield, Standard Contractual Clauses and similar means of exporting such data).

Any candidate who will be dealing with personal data from Europe absolutely must get this one right. And candidates interviewing for positions that deal only with U.S. data should at least be aware that Europe is different, even if they don't know the specifics.

Certification

Certification is available to data privacy and security professionals. You should ask any candidate what certifications they hold.

The International Association of Privacy Professionals (IAPP) is the leading organization for the education and certification of privacy professionals. Such certifications include Certified Information Privacy Professional (CIPP) (with versions for the U.S. public sector, U.S. government sector, Europe, and Canada and the IAPP will soon test one for Asia), Certified Information Privacy Manager (CIPM), Certified Information Privacy Technologist (CIPT) and a new Fellow of Information

 COPYRIGHT © 2017 BY THE BUREAU OF NATIONAL AFFAIRS, INC. PVLR ISSN 1538-3423

Privacy (FIP). These certifications are covered by ANSI/ISO standard 17024:2012.

The Information Systems Security Certifications Consortium, Inc. ((ISC)2) offers many certifications in data security, including Certified Information Systems Security Professionals (CISSP), Certified Cloud Security Professionals (CCSP) and Systems Security Certified Practitioners (SSCP). These practitioners know their data security and often know a lot about privacy as well. Just follow up with reasonable additional poking and prodding to make sure that their expertise includes the policy and law that's so important to the position.

IAPP or (ISC)2 certification is probably the best litmus test of whether you're interviewing a pretender or carpetbagger. A candidate who has at least one certification is paying attention to the field and has taken at least the amount of time an effort necessary to become certified. Candidates who have more than one certification are still the exception, but they're becoming more common. More than one certification is usually a signal that the candidate is pretty serious and knowledgeable. (Not that a single certification is an indicator that the candidate is a slouch. Many of the panelists and experts at national events have only a single certification and it's likely that they're too busy doing actual high-level privacy work to add other certifications.)

You can verify a claimed IAPP certification with the IAPP at www.iapp.org or by calling the IAPP at 603-427-9200 or 800-266-6501.

Industry Connections

It's hard to be a privacy or data security pro in a vacuum. The best go to conferences and mingle with others in the field to stay up to date. Find out which conferences the candidate attends. Be specific. Privacy pros get extra points for having attended IAPP conferences, especially the IAPP Global Privacy Summit or any ''Intensive'' or ''Comprehensive.'' Data security pros get extra points if they attended Black Hat, RSA, DEF CON, ShmooCon, the SANS Series or InfoSec World.

While mere attendance at one or more conferences does not make a candidate a talented practitioner, candidates who attend at least one conference each year are much more likely to be committed to the field and less likely to be pretenders. The best conferences are not cheap, either to register or to travel and attend. In addition to commitment, the candidate is much more likely to understand the field, even if only by osmosis. Double points for a candidate who has not only attended but *presented*.

Contracts and Agreements

Find out what the candidate knows about the contractual arrangements that you'll need to make with customers, vendors and others. Ask the candidate what matters in agreements with your organization's service providers.

The kinds of personal data matter. This is especially true with ''nonpublic personal information'' under the Gramm Leach Bliley Act, ''protected health information'' under HIPAA (which might even require what's called a Business Associate Agreement that must have certain provisions in it), ''cardholder data'' under the Payment Card Industry Data Security Standards, and other personal data that's covered by regulatory, industry, or other requirements. The origin of the data matters, too, especially if any of it comes from Europe.

Find out what the candidate knows about the contractual arrangements that you'll need to make with customers, vendors and others.

Limitations of liability can result in the company having a right without a remedy. A low dollar limit or a limitation on kinds of liability (aren't the damages from a data breach nearly always ''consequential'' damages?) can thwart the company's efforts that went into negotiating the service provider's data security obligations.

Extra points for any candidate who calls out that a general confidentiality obligation usually isn't adequate to cover privacy or data security obligations. It's best to deal with privacy and data security by imposing specific obligations to protect the data, refrain from using the data in unauthorized ways, allowing inspections and audits and immediately reporting any actual or suspected breaches.

A particularly sophisticated candidate might bring up ways in which the parties can allocate liability, the more objective, the better. This might include (a) physical demarcations (like the outermost point on the vendor's firewall with the public internet), (b) processes (encryption—at rest or in transit—using particular processes), (c) standards (like IEEE P1619/D16 for encryption on certain devices), or other means. The specifics aren't that important. Thinking about allocation of liability in a way that strikes a balance between protecting personal data and the time and energy required to get to a contract is.

Almost any privacy/data security pro will have to review, if not negotiate and manage, contracts that cover service providers' handling of personal data. Facility with the usual issues is essential. If a candidate talks intelligently about the process, you're on the right track. On the other hand, a candidate who doesn't have a good grip on service-provider obligations probably doesn't have experience that you need in the organization.

And One to Identify the Superstars

If you want to hire someone with real chops in the information economy, ask the candidate if he or she has a Bitcoin wallet.

Bitcoin is a digital asset and a payment system that came into being in 2008. It is a ''virtual currency'' or ''cryptocurrency.'' Bitcoins don't exist in physical space. They exist virtually as a part of a public ledger (called the ''blockchain'') and a number of parties that maintain copies of the blockchain (called ''nodes''), which verify transactions and the ownership of particular bitcoins. A ''Bitcoin wallet'' or ''lightweight client'' is an account or other means of storing a private key and it allows the holder to store information about the holder's Bitcoins, and send and receive Bitcoin payments.

Concepts that usually indicate that the candidate understands the field include any discussion of wallets,

public-key cryptography, full clients, lightweight clients, the blockchain, authentication, whether a server can be trusted and similar matters.

Most privacy and data security work doesn't require this kind of knowledge and a candidate who gets caught flat-footed on this one would be in pretty good company. But, if you need a person who understands cryptography or payment systems—or if you want an acid test for whether a candidate really *plays* in the e-commerce or FinTech space—this line of questioning will separate the high-flyers from the posers (and even the merely high-functioning).

There's no guarantee that any particular battery of questions will separate the rock stars from the roadies. But hiring or retaining privacy professionals is a fact of life and having a basic set of questions and answers goes a long way toward selecting the right professionals.

 COPYRIGHT © 2017 BY THE BUREAU OF NATIONAL AFFAIRS, INC. PVLR ISSN 1538-3423