Assessing public information in the digital age

By Jedidiah Bracy, CIPP/E, CIPP/US

Though public records stand among the pillars of an open society, the information economy is challenging traditional notions of what should be considered readily accessible to the general community. As information brokers collect and store greater amounts of information, public agencies implement e-government initiatives and telecommunications systems improve the ease with which information flows across the globe, should the line around what constitutes public data be reassessed?

A number of recent incidents may be exposing fault lines that could call for a different mode of thinking.

What’s public? What’s private?

In early March, a New Jersey appellate court ruled that an individual’s right to obtain documents under the state’s Open Public Records Act (OPRA) “trumped” the right to privacy of home addresses. In the case, the plaintiff requested a list of addresses of senior citizens who had signed up to receive mailings from Union County, NJ, for the purpose of expressing her views on the contents within county mailings. To protect the recipients, Union County officials redacted the addresses. In response, the plaintiff argued that she had the right to those addresses under the OPRA. The state appellate court agreed with the plaintiff, and now citizens who provide personal information to the mailing list are subject to the OPRA and may have their data shared with other third parties upon request.

One local official fears the ruling sets a dangerous precedent for companies that want to mine data on the cheap. Also, some are concerned that the precedent could “put a chill on people seeking” government services once citizens realize their names and addresses could be shared with third parties.

Similar red flags have been raised about whether emergency call transcripts should be available to the public. George Washington University Law School Prof. Daniel Solove points out in a Concurring Opinions piece that 911 calls often involve the disclosure of personal medical information. “Doctors and nurses are under a duty of confidentiality,” opines Solove, “so why not 911 call centers, especially when people are revealing medical information?”
Though 911 call centers are not regulated under HIPAA, Solove argues the public release of 911 calls without the consent of the caller “violates people's constitutional right to information privacy.”

Deborah Peel of Patient Privacy Rights argues in a GovInfoSecurity report that public release of emergency calls is a violation of HIPAA because 911 operators “are in effect working on behalf of hospitals and emergency centers as part of the patient’s treatment team.”

Some argue that public release of 911 calls promotes transparency and provides citizens with a window into the effectiveness of call centers. Yet, Solove has said this can be done without violating the privacy of callers. “I would think,” writes Solove, “that if 911 operators didn’t handle the call well, most people would consent to disclosure so the 911 center could be held accountable.”

In light of the recently publicized 911 call of actress Demi Moore, California Assemblywoman Norma Torres (D-Pomona) plans to introduce legislation to bar the disclosure of such calls. Missouri, Pennsylvania, Rhode Island and Wyoming all have laws that keep 911 calls private, and lawmakers in Alabama, Ohio and Wisconsin are considering similar rules.

The pros and cons of e-Government

Mining of public agencies' data is also being used for identity theft. Media reports show that the Social Security Administration’s Death Master File (DMF) has been under recent scrutiny by citizens and lawmakers because of alleged inaccuracies within the list and the ease with which identity thieves can access the public data.

The government-backed database lists more than 87 million deceased Americans, including their names, addresses and Social Security numbers. Intended to assist medical research and help government, financial, investigative and credit reporting organizations fight identity fraud and verify a citizen's death, the DMF can be purchased and distributed online. In some cases, using the Freedom of Information Act, information in the file is sold to private companies and posted on the Internet. The information is also commonly used for genealogy research.

Identity thieves have used data gleaned from the DMF to file bogus tax returns, and the practice has become widespread enough to gain the attention of those in public policy.

According to Fox 6 Now, the National Consumers League (NCL) has expressed concern over the availability of DMF data. NCL Vice President of Public Policy John Breyault said, “While NCL generally supports transparency of government data... In this case, we believe the risk that DMF data can be used for nefarious purposes outweighs the benefit.”

SSA Inspector General Patrick P. O’Carroll, Jr., testified in February that as many as 1,000 cases each month have involved a living individual mistakenly being added to the DMF. Additionally, a 2008 Social Security audit revealed that as many as 20,000 living Americans’ Social Security numbers were publicly disclosed through the DMF. Though O’Carroll suggested that public disclosure be limited, it would take an act of Congress, he said.

In response to these issues, LifeHealthPro reports Rep. Sam Johnson (R-TX) has introduced the Keeping IDs Safe Act of 2011. Pending in the House Ways and Means Committee, the legislation would limit the public disclosure of DMF data.
Court records are also public data, serving legal scholars, investigative journalists and others. As New York University Prof. Helen Nissenbaum writes in her book *Privacy in Context*, "With few exceptions, court records of both civil and criminal cases are also part of the larger class of public records and contain a great deal of personal information." In addition to plaintiffs and defendants, court records can also reveal personal information about jurors and jury member pools and can include Social Security numbers, financial, medical and other "exquisitely personal" information.

These records—once only on paper—were concealed in what some call "practical obscurity." Because material documents were housed in specific locales, accessing the records required some degree of physical limitation. In digital form, court documents are not only easily accessible, Nissenbaum writes, they "can be rapidly retrieved, searched and reassembled in novel ways not previously imagined." A simple query on a search engine by a potential employer could return compromising information that might not appropriately reflect a job applicant's current situation, for example.

Nissenbaum also notes that, as a consequence, the twofold combination of public record digitization and e-Government initiatives that are making access to public records easier across government agencies, allows "interested parties, from journalists and information brokers to identity thieves and stalkers," to "avail themselves of these services."

**A shifting privacy paradigm?**

According to a recent article by Alexis Madrigal in *The Atlantic*, NYU's Nissenbaum has "played a vital role in reshaping the way our country's regulators think about consumer data." The concept of context—or what she refers to as "context-relative informational norms"—was used in the Federal Trade Commission's recently released privacy report 87 times.

Rather than treat what is public and private as a strict binary, Nissenbaum has put forth a need for recognizing "contextual integrity" with a "reasonable expectation of privacy." Over the course of time, society's norms and values change, and, depending on the social situation, expectations of privacy change.

For example, new technologies such as facial recognition are challenging our notions of privacy while in public. When entering the public sphere, we are not only letting ourselves be identified, but we can also identify other people. It's a two-way street, and while not everyone knows everyone else, facial recognition can potentially collect, store and identify individuals in the public sphere and connect those images with a vast database. In this latter context, our expectation of privacy most likely does not match the flow of information captured from images of our face to a database. Yet, the expectation changes when this same technology is employed in a casino to help troubled gamblers who have opted in to the gambling-prevention program.

As Madrigal writes, "Nissenbaum puts the context—or social situation—back into the equation." What we decide to share with our friends, we might not share with our boss. What we share with a doctor, we might not share publicly, and so on. "Furthermore," he adds, "these differences in information sharing are not bad or good: they are just the norms...Perhaps most importantly, Nissenbaum's paradigm lays out ways in which sharing can be a good thing." Using facial recognition to prevent an addiction to gambling could be one such example.

Rethinking traditional notions of what is private has also made its way to the U.S. Supreme Court.
In *United States v. Jones*, justices countered the government’s argument that “citizens have no privacy interests in their public movements.” The placement of a GPS monitoring device without a warrant was essentially trespassing on private property. Yet, as Kashmir Hill points out in a *Forbes* report, what if a suspected criminal used a GPS navigation device in his vehicle? According to the third-party doctrine, privacy is lost once information is shared with a third party, as are any Fourth Amendment protections against illegal searches and seizures.

The concurring opinion of Justice Sonia Sotomayor, in this case, however, suggests a potential reconsideration of the third-party doctrine.

Noting that “an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties,” Sotomayor queried whether the doctrine is “ill suited to the digital age” since so much information is now shared with third parties during “the course of carrying out mundane tasks.”

As an *American Criminal Law Review* blog post points out, “It’s unclear whether other justices on the court share” Sotomayor’s concurring opinion, “but this will probably affect arguments in future information privacy cases before the court.”

---

**Legislative roundup: Public-Private**

By Kasia S. Park, University of Maine School of Law

Technology has greatly increased the accessibility of public records. While this makes research more time- and cost-efficient, there are potential dangers concerning privacy and security, especially if there is personally identifiable information contained within the public records. This has prompted the introduction of several state bills addressing these growing concerns in the U.S. Here are some examples.

**New Jersey**

New Jersey is considering legislation that would exclude from disclosure as a public record the e-mail addresses of individuals provided to government entities for the sole purpose of receiving emergency notifications. [Assembly Bill 2481](https://www.njleg.state.nj.us/billinfo/2013a2014/b2481r16b1h/b2481r16b1h.xml) is pending and was referred to the Assembly State Government Committee on February 21.

**Tennessee**

Two bills were introduced in January of this year that would classify consumer-specific energy usage data as a private record. The House Committee on Conservation and Environment recommended passage, as amended, of [TN House Bill 3758](http://www.tnonline.com/laws/111/session3/HB3758.xml). An identical bill, [TN Senate Bill 3608](http://www.tnonline.com/laws/111/session1/SB3608.xml), passed in the Senate and is now held on the House desk.

**Virginia**

Legislation that would exempt personal information in constituent correspondence from the Freedom of Information Act (FOIA) passed both the Senate and House and was signed by the Governor on April 4, 2012. It will go into effect on July 1, 2012. [VA House Bill 141](https://www.vaconline.law.gov/web/consumer/legislative/history/bills/2011/2011HB141.htm) provides an exemption from the mandatory disclosure provisions of the FOIA for the names, physical addresses, telephone numbers, and e-mail addresses contained in correspondence between an individual and a member of the governing body, school board or other public body of the locality in which the individual is a resident.
Social networks seek workplace privacy protections

The debate over access to people’s Facebook and Twitter profiles is heating up, as a number of legislators seek to ban employers from forcing people to disclose their access credentials. But at the same time, intelligence and law enforcement agencies report that they’re starting to troll social networks for suspicious activity.

By Mathew J. Schwartz

Should job applicants be required to submit their Facebook username and password to prospective employers, or step through their posts and photographs while an interviewer “shoulder surfs”?

That Maryland Department of Public Safety and Correctional Services requirement for anyone interviewing—or recertifying—for a job, ostensibly to look for gang affiliations, drew international attention in part because it highlighted the existing disparity between people’s embrace of social networking and the apparent lack of privacy protections afforded to such communications, at least in the workplace.

Department of Corrections Officer Robert Collins said he felt he had to comply with the request—he needed a job—which was made during his reinstatement interview, following a leave of absence he took after his mother died. But Collins also reported the practice to the American Civil Liberties Union of Maryland, which alleged in a complaint that the requirement violated the Stored Communications Act (SCA). While other legal experts have said that it’s not clear whether the law applies to social media, the corrections department has backed off.

But the department wasn’t alone in its demand for applicants’ Facebook passwords. Similar demands have been made by everyone from the city of Bozeman, MT, and the McLean County Sheriff’s Office in Illinois, to an Ontario law enforcement agency and a New York lobbying firm.

The bigger issue is that legal privacy protections often lag advances in communications technology. For example, under current workplace laws, discounting jobs that require a security clearance, employers in the United States—and many other countries—can’t require job applicants to submit to a polygraph test. In addition, employers are prohibited from discriminating on the basis of race, religion, security, age, marital status, sexual orientation, disability, national origin or veteran status, which is why most employers studiously avoid any related questions during job interviews. But imagine what trawling a Facebook profile might reveal.

No wonder Facebook has decried social media background checks involving private data. “If you are a Facebook user, you should never have to share your password, let anyone access your account or do anything that might jeopardize the security of your account or violate the privacy of your friends,” said Facebook Director of Privacy and Public Policy Erin Egan last month in a blog post. She also warned that employers might be legally liable for having improperly accessed Facebook communications involving a person’s race, sex or other protected information, as well as for violating the social network’s terms of service, which specifically prohibit users from sharing their passwords.

The Maryland case, amongst others, has led many legislators to begin rethinking privacy protections for the social media age. Already, the Maryland House and Senate have passed bipartisan legislation—set to take effect October 1—that protects employees against such practices, even when labeled as
“voluntary,” as well as any retaliation for failing to share social network access credentials. Other states—including California, Illinois, Michigan, New Jersey, New York and Washington—are weighing similar legislation, as is Congress.

What’s the story outside of the United States? Attorney David Fraser, who runs the Canadian Privacy Law Blog, has said that a “patchwork” of laws covers Canadian workplace privacy. While the country’s privacy laws require that any collection of personal information be reasonable in nature, Alberta has warned any company that tries to vet people via Facebook or Twitter to “take a really careful look” at the law, suggesting that it will be watching such practices closely. Likewise, British Columbia has published a detailed set of guidelines for social media background checks.

Outside of North America, many privacy officials are likewise urging caution. “We would have serious concerns if employers were regularly asking employees for their Facebook login details in the UK,” said a spokesperson for Britain’s Information Commissioner’s Office by phone. He emphasized that the country’s Data Protection Act prohibits the storing of “excessive” personal information.

The embrace of Facebook, Twitter, Google+, Flickr and their social media ilk has triggered sharp privacy questions beyond the workplace realm too. New European regulations, introduced in January, would extend “right to be forgotten” rules to personal data stored by any business that markets to EU citizens. In other words, anyone who cancels their Twitter account could demand that the microblogging platform remove every post they’ve ever made, “without delay.”

But law enforcement demands could add a wrinkle. In Britain, for example, government officials have been pushing service providers to retain subscribers’ communications, including Facebook and Twitter messages. Related debates have been influenced in part by last year’s riots in England, which were coordinated—at least in part—using social networks.

Meanwhile, the U.S. Department of Homeland Security already monitors social networks. Likewise, the FBI in January issued a request for information to contractors for its own social media monitoring system. That revelation, perhaps predictably, led to a privacy outcry, with civil rights groups questioning whether the bureau should be trawling people’s Facebook profiles.

Since then, however, FBI Special Agent Ganpat “Gunner” Wagh said at a conference that the bureau works hard to balance privacy concerns with the need to monitor social networks during some types of investigations. He also said the FBI—in close consultation with its in-house attorneys—only conducts targeted, deep dives of social networks during the course of an investigation.

Given the popularity of social networks, not to mention their self-surveillance side effect, should the bureau’s moves be surprising? Cyber investigations, notably, used to focus only on online crimes. But with everyone today carrying a laptop or cell phone, investigators say that almost any case might have a cyber-investigation component. Likewise, it’s no wonder that for major cases, law enforcement agencies want to study social networks to gain a clearer picture of suspects’ activities.

The related “ripped from the headlines” cop-show angle writes itself: A murder suspect gets exonerated because he checked into a restaurant with Foursquare then sent food snaps to Instagram at the time of a murder. Obviously, that example isn’t real. But as more people mirror their everyday thoughts and activities on social networks, expect the related privacy demands—notably, to keep people’s private social media communications private, barring a court order—to intensify.

Mathew Schwartz reports on information security and privacy issues for InformationWeek, The Privacy Advisor and Inside 1to1: Privacy.

Read more by Mathew Schwartz:
In response to increasing reports of employers asking employees and job applicants for their Facebook user names and passwords, 10 U.S. states have introduced legislation that would bar this practice. The bills would prohibit employers from requesting or requiring employees or prospective employees to disclose information to access social media or electronic accounts. The bills vary in scope regarding who they would protect and what types of electronic accounts to which the prohibition would apply.

There will likely be federal legislation introduced in the near future as well. Sen. Richard Blumenthal (D-CT) has announced plans to introduce an analogous federal bill and Rep. Patrick McHenry (R-NC) is drafting similar legislation.

Furthermore, Sen. Blumenthal and Sen. Charles Schumer (D-NY) have asked Attorney General Eric Holder to investigate whether this practice violates federal law, specifically the Stored Communications Act and/or the Computer Fraud and Abuse Act. The senators are calling on the Department of Justice and the U.S. Equal Employment Opportunity Commission to launch investigations.

**California**

Assembly Bill 1844 would prohibit employers from requiring a prospective employee to disclose a user name or account password to access a personal social media account. It is pending before the Assembly Judiciary Committee. Senate Bill 1349 would go a step further; it would prohibit postsecondary educational institutions and employers from requiring or formally requesting a student or employee—or a prospective student or employee—to disclose the user name or password for a personal social media account. It is pending before the Senate Education Committee.

**Illinois**

House Bill 3782 would amend the Right to Privacy in the Workplace Act to prohibit an employer from asking any employee or prospective employee to provide any password or other related account information in order to gain access to a social networking website. The bill is currently pending with the Senate.

**Maryland**

On April 10, Maryland became the first state to pass a bill to keep social media passwords safe from employers or potential employers. The legislation, Senate Bill 433 and House Bill 964, prohibits an employer from requesting or requiring that an employee or applicant disclose a user name or password for accessing electronic communications devices. The bill also protects employers by prohibiting employees from downloading an employer’s proprietary information of financial data to a personal website or account.

**Michigan**

House Bill 5523, the Social Network Account Privacy Act, prohibits employers and educational institutions from requiring disclosure of information that allows access to social networking accounts. If passed, the bill would protect employees, prospective employees, students and prospective students. The bill is currently pending in the House Committee on Energy and Technology.

**Minnesota**
A bill (H.F. No. 2963) is pending before the House that would prohibit employers from requiring, as a condition for employment or consideration of employment, an employee or prospective employee to provide a password or other account information in order to gain access to the employee’s or prospective employee’s social networking website.

**Missouri**

House Bill 2060 prohibits employers from requesting or requiring an employee or applicant to disclose information to access a personal account or service though an electronic communications device. The bill is currently pending with the House.

**New York**

Senate Bill 6831 prohibits employers from requesting or requiring an employee or applicant to disclose information to access a personal account or service through an electronic communications device. The bill is currently pending with the Senate Labor Committee.

**South Carolina**

House Bill 5105 prohibits employers from requesting a password or other related information in order to gain access to an employee’s or prospective employee’s profile or account on a social networking website. The bill is currently pending before the House Judiciary Committee.

**Washington**

Sen. Steven Hobbs (D-Lake Stevens) introduced the “Facebook bill” (S.B. 6637) which would prohibit employers from requesting a password from a current or prospective employee for the purpose of gaining access to a social networking site.
Maryland "Facebook law" raises new obstacles for employers vetting applicants and investigating employees, but with important exceptions

By Philip L. Gordon

The momentum in the media made it almost inevitable: the first state law to expressly restrict employers from asking applicants and employees for social media account login credentials has been passed. Not surprisingly, Maryland, where the issue first burst onto the scene in April 2011, wins the “honor.” However, Maryland likely has opened the floodgates. Bills currently are pending in California, Illinois, Minnesota, New Jersey and Washington. Employers seeking to understand the implications of the Maryland law must look beyond the blaring headlines to the details of the statute.

To begin with, the law’s general prohibition is both broad and narrow. Effective October 1, 2012, assuming the governor signs the law, employers are prohibited from requiring, or even asking, that applicants or employees disclose “any means for accessing,” such as a username or password, for “any personal account or service” accessed through “computers, telephones, personal digital assistants and other similar devices.” In other words, the prohibition extends far beyond Facebook and other social media sites to include personal e-mail accounts, personal online banking accounts and any other online communications or service account.

The Maryland law prohibits an employer from taking or threatening any form of adverse action based on an employee’s or applicant’s refusal to provide a user name or password to a personal account accessed through a communications device. An employer cannot discharge, discipline or otherwise penalize an employee. An employer cannot reject an applicant for engaging in the protected conduct.

Notably, the Maryland law contains no enforcement provision. The law does not authorize applicants or employees to sue. The law does not even delegate authority to the Maryland Division of Labor and Industry, or any other government agency, to enforce it. It is possible that an employee terminated in violation of the law might have a claim for wrongful discharge in violation of public policy. However, because that claim typically applies only to discharge, it is unclear whether an employee who is disciplined short of discharge would have a claim. It also is uncertain whether an applicant who is denied employment in violation of the law would be able to assert a claim.

While the law seems overly broad at first blush, it is critical for employers to understand the types of conduct that the law does not prohibit. Some of these exceptions are expressed in the statute itself; others are implicit.

- **Access To Employer’s Internal Systems:** The law expressly permits employers to require that employees disclose login credentials “for accessing nonpersonal accounts or services that provide access to the employer’s internal computer or information systems.” In other words, employees cannot rely on the law to prevent employers from gaining access to information stored on the employer’s own information systems.
- **Violations of Securities or Financial Laws or Regulatory Requirements:** If an employer receives information that an employee is using a personal online account for business purposes, the law “does not prevent” an employer from conducting an investigation to ensure that the employee is complying with “securities or financial law or regulatory requirements.” This exception appears intended to apply in a situation where an employee of a financial services company uses a personal online account to trade securities or engage in other financial transactions on the employer’s behalf.
• **Protection of Trade Secrets:** If an employer receives information that an employee has downloaded the employer’s proprietary information, without authorization, to a personal online account, the law “does not prevent” an employer from conducting an investigation into such suspected misconduct.

• **Passwords to Devices:** While the Maryland law bars employers from requesting login credentials for "accessing a personal account or service," the law does not prohibit employers from requesting or requiring login credentials to access an employee’s personal device, such as a smartphone or tablet. This distinction is critical as employers increasingly are implementing “Bring-Your-Own-Device” policies.

• **Nonpersonal Accounts:** The law protects login credentials only for “personal” accounts. Maryland employers should clearly define which accounts are personal and which are nonpersonal. For example, if an employee uses a corporate e-mail address to establish a LinkedIn profile or Twitter account, the employer should ensure that employees know from the outset that such an account is “nonpersonal” for purposes of the Maryland law.

• **“Shoulder Surfing”/Printing:** Because the Act’s restrictions on their face arguably apply only to the disclosure of log-in credentials, it remains to be seen through judicial interpretation whether the Act’s restrictions bar an employer from, for example, asking an employee or applicant to log into a personal account without disclosing the log-in credentials to the employer so the employer can observe the content of the personal account or asking an employee or applicant to print the content of a personal account. Before an employer chooses this route, they should speak with their employment counsel to educate themselves about the legal risks of doing so.

---

**Phil Gordon** is a shareholder at Littler in Denver, CO. He is chair of the firm’s Privacy and Data Protection Practice Group. He may be reached at pgordon@littler.com.
A practical guide to making good use of your PII inventory

By Brian Beauchamp, CIPP/G, CIPP/IT, Meghan Farmer, CIPP/G, CIPP/US, and Elliott Tomes, CIPP/G, CIPP/IT, CIPP/US

Since the publication of recommendations by the President’s Identity Theft Task Force and the Office of Management and Budget (OMB) Memo 07-16, federal agencies are required to review their holdings of all personally identifiable information (PII) and ensure they are accurate, relevant, timely and complete. Agencies are also required to reduce PII to the minimum necessary for the proper performance of a documented agency function and eliminate unnecessary collection and use of Social Security numbers.

Performing maintenance on PII creates benefits beyond satisfying the OMB requirements. The process is an opportunity to significantly reduce privacy vulnerability, promote awareness and enhance processes, thereby reducing breach incidents. These opportunities are not exclusive to government-controlled systems. Also susceptible to privacy vulnerability are information systems owned or controlled by private-sector organizations.

Of importance is the methodology used to determine inventory and conduct maintenance. The level of scrutiny by the review team and the willingness to modify business processes by stakeholders can make a difference in the effectiveness of a “review and reduce” program. While each organization is different, the following areas of focus are essential for a thorough review aimed at reducing privacy vulnerability:

- Collection of PII not necessary for actual performance of the business process;
- Collection of the same PII more than once from a record subject or another source;
- Collection of PII at a point in time not reasonably proximate to its actual need;
- Maintaining PII longer than necessary for performance of the business process;
- Maintaining duplicate databases or files of PII where consolidation is feasible;
- Displaying PII unnecessarily on human-readable system outputs, including user-facing or customer-facing online views of a record.

Each of these areas of focus represents an effort to fulfill the Fair Information Practice Principles (FIPPs) of data minimization, use limitation and/or data quality and integrity. To help ensure cooperation and meaningful discussion towards resolution, the importance of these principles should be discussed with organization stakeholders before introducing the “review and reduce” findings.

Nuts and bolts

First, a word on the tools needed to complete a PII “review and reduce” inventory. Most prominently, Privacy Impact Assessments (PIAs) are a great resource. Although PIAs first emerged as a tool to ensure compliance, many private companies now implement PIA programs to establish privacy risk assessment into the fabric of the organization. In addition to PIAs, one may also seek information on a more granular level by interviewing system users and owners or by interacting with the system or application itself.
Because a PIA is customarily performed on a single system, it may be difficult to understand the overall effect of operations in terms of privacy risk. It may appear reasonable that a particular system compiles or maintains PII in the manner it does when it is examined in isolation. However, other hidden but avoidable risks may be revealed when a system is viewed in relation to others with which it interconnects. The first step in this analysis is to define general business areas. Operations that depend on compiling and maintaining PII should be divided into broad business areas, which will usually correspond to organizational hierarchies already established by HR or marketing teams. It’s worth noting that an area can be supported by one standalone system or by several interconnected systems and databases.

If necessary, the business area can be subdivided into business processes. From the standpoint of compilation or use of PII, a business process usually has a beginning and an end and achieves a specific need or purpose different from other processes under the business area. For example, recruitment is a business process within an organization’s general HR business area.

The final step in organizing a top-down approach is to ensure each system that involves PII is mapped to the business process it supports. Documentation, whether in a PIA or internal system architecture mapping, can be analyzed to understand how systems within a process are sequenced or interoperate.

Once the business areas and business processes are established and mapped, the fact-gathering step begins. Standardized data sheets can be created to assist in this step, which will ordinarily be the most labor-intensive part of “review and reduce.” Such sheets guarantee commitment to principles of uniformity while retaining a special focus on those characteristics bearing on risk. A data sheet may describe one of three kinds of entities that exist in business processes:

- A **collection** is a natural business transaction; e.g., paper form, web form, interview result, that assembles personal facts and is likely completed by the system user.
- A **stored record** is information about a record subject maintained in a system. A stored record usually manifests itself in a computer master file or a database.
- An **output** may be in the form of a computer-generated report of persons’ records, a printout of individual records or a computer-readable database extract comprising PII.

After an assessment of the inventory is reviewed and opportunities for risk mitigation are discovered, formal findings should be discussed with each corresponding office. After these discussions take place, revised findings, conclusions or resolutions supported by the program can be incorporated.

**Challenges and lessons learned**

After successfully inventorying PII within an organization and identifying opportunities for data reduction, the next step is to work with stakeholders to incorporate the resolutions and risk mitigation measures. An effort to reduce PII within an organization will likely present challenges. Common issues that arise include:

*Converting to a unique identifier other than SSN*

Often an organization assumes that the SSN, sometimes in combination with the date of birth (DOB), is the best—or only—way to accurately distinguish an individual among all the personal records maintained in a system. This assumption increases risks associated with identity theft. It can also result in the creation of duplicate identity records in multiple corporate IT systems and inhibit identity integration across the enterprise.

Alternatives to the use of the SSN to accurately distinguish record subjects exist. Organizations should be encouraged to consider viable alternatives to the SSN such as a unique employee ID number. This ID should be unique to the individual and should be something that the individual can remember. Besides decreasing risks associate with identity theft, additional benefits include the ability to correlate identity
data for the same individual across multiple systems, enable modernized access controls and provide better visibility into how identity data is used across the enterprise.

**Generating awareness that duplicate collections of PII increases vulnerability**

Frequently, organizations maintain duplicate files or databases of PII even where consolidation is feasible, thereby increasing privacy vulnerability. The PII inventory identifies such duplicate collections, but system owner participation is required to reduce them. Often this situation arises when different offices within an organization are unaware that the same data is being maintained in other offices, do not have access to the other collections of PII or are unwilling/unable to rely on/share PII from another point of collection.

Meeting with system owners or other stakeholders to discuss the importance of PII minimization within an organization and share duplicate collections that have been identified is a key component of a successful “review and reduce” effort.

**Next steps**

The reduction of PII within an organization, and the corresponding reduction of privacy risk, should be an ongoing endeavor. The final product of a “review and reduce” effort provides a solid foundation from which to assess and mitigate privacy risk. It is important, however, to continue to review the organization’s PII inventory regularly and assess progress towards the agreed upon resolutions.

*Brian Beauchamp is an analyst in the Privacy Division at SRA International, Inc. He can be reached at Brian_Beauchamp@sra.com.*

*Meghan Farmer is a senior consultant in the Privacy Practice at Booz Allen Hamilton. She can be reached at farmer_meghan@bah.com.*

*Elliott Tomes is a senior associate in the Americas Data Protection and Data Privacy Office at Ernst & Young LLP. He can be reached at Elliott.Tomes@ey.com.*
Singapore released proposed personal data protection bill

By KK Lim

The Ministry of Information, Communications and the Arts (MICA) released the proposed personal data protection bill on 19 March and invited comments from the public ending 30 April.

MICA conducted two public consultations on the proposed data protection (DP) regime as well as the Do-Not-Call Registry (DNC) in 2011. The DP regime covers the scope of the proposed DP law; related rules on use, collection, disclosure and transfer of personal data outside Singapore; data accuracy; retention of personal data, and penalty and enforcement-related matters. Following the DP consultation, there was strong public interest and a call for a national DNC, and DNC public consultation was conducted on 31 October 2011. Collectively, the following are the salient features of the proposed legislation known as Personal Data Protection Act. (PDPA).

Structure
Part I deals with the preliminary matters of the act; Part II on the Data Protection Commission (DPC) and administration; Part III on the general rules on protection of personal data; Part IV on collection, use and disclosure of personal data; Part V on access to and correction of personal data; Part VI on care of personal data; Part VII on enforcement (Part III to Part VI); Part VIII on appeals to the Data Protection Commission Appeal Committee, the High Court and the Court of Appeal; Part IX on the DNC, and Part X on general matters. Note that there are 10 schedules accompanying the PDPA.

Definition of personal data
The term personal data is defined as data about an individual who can be identified from that data or together with that data and other information to which the organization is likely to have access. Note that the definition does not differentiate between true and false personal data; that it is immaterial whether it is a single piece of information or a group of information taken together that may relate to an identified or identifiable individual as they will be considered as personal data, and the term data covers both electronic and non-electronic forms of personal data.

Coverage
PDPA is a "baseline" regime that covers all private organizations, including small companies with low annual turnover as opposed to excluding companies with minimum turnover such as those in Australia, which excludes businesses with less than A$3 million unless they are health service providers or trading in personal information. Public organizations are excluded from PDPA’s coverage. The standard imposed by the government on the protection of personal data may be the same, if not stricter, than PDPA in some cases.

Companies collecting personal data
The PDPA will cover organizations engaged in data collection, processing or disclosure within Singapore even though the specific organization concerned is located outside of Singapore.

The wide coverage is so despite the difficulty of prosecuting a pure online entity. This approach is in line with other enacted legislation such as the Computer Misuse Act (CMA). Part 1 (Application) spells out in great detail on the affected personal data with a "Singapore link."
Exclusions from PDPA
The PDPA also excludes:
- personal data in a record for 100 years;
- a data intermediary that processes data on behalf of another party except as to the rules applicable on safeguarding the data;
- information on deceased individuals to be protected from disclosure and safeguarded for up to 10 years from date of death without further obligation to retain them apart from current retention requirements;
- business contact information unless provided in a personal context, and
- information for educational purposes such as examination marks and personal data in scripts and other related documents as well as universities in the process of admitting students. Note that exclusions to the PDPA are contained under Section IV of the PDPA as well as in the third, fourth and fifth schedules, respectively.

Contact point of organization
PDPA requires that an organization needs to appoint someone responsible for the organization’s compliance to PDPA such as handling queries from the public. The organization is finally accountable for the compliance of the PDPA but not the individual.

Conditional supply of services or products/explicit, implied deemed consent
Organizations are prohibited from requiring an individual to consent to the collection, use or disclosure of personal data beyond what is reasonable as condition for supplying a service or product to an individual. The key principle is not to prescribe in great detail the manner in which consent is given. However, organizations need to be upfront on the purpose for collecting the information with the individual so as to avoid any misunderstanding with the consumers in relation to the implied use of the information in the future. In all cases, what is reasonable is the key determinant in deciding whether an organization is compliant to the spirit of the PDPA. At the same time, organizations are not allowed to assume that consent is automatically given by an individual within a certain timeframe, the so-called “failure to opt out as deemed consent” option, in dealing with individuals, as this exposes individuals to unnecessary risks.

Withdrawal of consent
Consent may be given to an organization that in turn may outsource the processing of the data to a third party. If the consent is withdrawn later by the individual, the organization is obliged to comply with the individual’s request but not beyond that, so as not to overburden the organization with unnecessary compliance cost. The individual is of course free to inform the third party regarding the withdrawal of the consent.

Penalty, enforcement regime and transitional arrangements
Similar to other jurisdictions, the administrative body of PDPA, the Data Protection Commission (DPC) is given powers to give directions to organizations that have been found to breach the requirements of PDPA. An individual may commence private civil proceedings against an organization for breaching the PDPA after a final determination by DPC on the specific complaint. A proposed sunrise period of no less than 18 months is proposed for all organizations to comply with the PDPA after enactment.

Do-Not-Call Registry (DNC)
The DNC is contained in Part IX of PDPA, and below is a summary of the key points:
- The proposed types of messages include SMS and MMS messages but exclude messages delivered by post as well as those sent through cell broadcast for the time being.
- The specific message is addressed to a Singapore telephone number regardless of where it originates or the technologies used for transmitting the message, for example, VOIP.
• Business numbers may be registered with DNC only by an organization that owns the number or by their authorized employees.
• Any individual not wishing to receive any messages must register with DNC. Registration is free, and it remains until withdrawn or if associated with any telecommunication service, until the service terminated.
• Correspondingly, organizations are able to send messages to those who have provided consent to receive them. However, note that there is no exception for existing business relationships and these organizations should leverage on their existing business relationships to obtain fresh consent.
• Senders need to provide the originating number or suitable contact information in those messages sent.
• The DNC would adopt a “filtering” approach where organizations need to send their proposed list of numbers at least once every 30 days to confirm whether any Singapore numbers are listed on the register. The registry would also provide small quantity number lookup service for businesses.

Summary
The DPDA provides a baseline platform for the management and protection of personal data against abuse due to the intrusive nature of modern communication technologies used both by individuals as well as organizations. Overall, it takes a commonsensical approach, balancing the needs of the individual vis-a-vis the needs of commercial organizations without overburdening them with excessive operational costs. The key principle embedded throughout the PDPA is what a reasonable person or organization should aim for and operate with regarding the collection, use and disclosure, accuracy, protection, retention, access and correction of personal data.

KK Lim is the president of Singapore Cloud Forum, a not-for-profit organization for cloud computing professionals, and an editorial member of The Journal of Information Privacy and Security (JIPS), published by University of Wisconsin-Whitewater, Global Business Resource Center. The opinions expressed here do not necessarily represent the views or opinions of these organizations. He may be reached at kklim@live.com.sg.
CANADA—The use of facial recognition technology

By John Jager, CIPP/C, CIPP/US

The use of facial recognition technology is becoming more and more prevalent in modern society, note such examples as Facebook’s introduction of such technology in 2011; Google’s attempt to introduce a facial search engine, and even an online dating site that was launched on the premise of matching people based on “facial compatibility.”

It is not surprising, therefore, that privacy advocates and privacy enforcement authorities are becoming increasingly interested in these developments. Recently, the Office of the BC Information and Privacy Commissioner (OIPC) released an Investigation Report into the use of facial recognition technology by the Insurance Corporation of British Columbia (ICBC). The investigation was triggered by ICBC’s offer to the police of the use of its facial recognition software in the identification of individuals involved in riots in Vancouver in the spring of 2011.

The OIPC took the opportunity to examine not only the proposed assistance to the police but also issues relating to the original purposes for the facial recognition program.

ICBC’s facial recognition program

The OIPC noted that the facial recognition technology was introduced as a means to address fraudulent acquisition and use of driver’s licences and British Columbia ID cards. A number of inadequacies were identified by the OIPC relating to the manner in which the ICBC’s privacy impact assessments (PIAs) were completed. While a PIA on the privacy issues related to use of biometrics was conducted by external legal counsel and internal staff very early on in the process, years later—when implementing the facial recognition technology—no comprehensive PIA was completed on the solution purchased. The organization’s documentation listed some basic privacy rules in the Personal Information Protection Act (PIPA) and conclusions reached but did not provide detailed analysis as to how the conclusions were reached. The OIPC also determined that the role of the ICBC’s privacy lead had not been adequately communicated throughout the organization. In examining the ICBC security arrangements for the facial recognition system, the OIPC determined that these arrangements met the standard of reasonableness; for example, all information transmitted and stored in the database were encrypted—using 128-bit and 256-bit encryption, respectively; access was limited to specific workstations and users, by their specific role(s), and audit logging was in place for all workstations and servers that were part of the facial recognition system.

Sharing of information with law enforcement authorities

As noted above, in the aftermath of riots following the Vancouver Canucks’ Stanley Cup loss, the police collected thousands of images of rioters that had been posted on various websites and Facebook pages. The ICBC offered the use of its facial recognition software to assist police in identifying the alleged vandals and rioters. The OIPC noted that the ICBC is authorized to disclose personal information in response to an order that satisfies the requirements of section 33.1(1)(t) of PIPA, which provides that disclosure is authorized in order to comply with a subpoena, warrant or order issued or made by a court, person or body in Canada with jurisdiction to compel the production of information. While ICBC cited section 32(c) of PIPA, which provides that a public body may use personal information in its custody or under its control only for a purpose for which that information may be disclosed to that public body under sections 33 to 36, as its authority to disclose information to the police, the OIPC determined that this section does not permit the use of every record in the ICBC’s entire database for the purposes of
responding to a disclosure request about a single individual. The OIPC found that, in this case, in the absence of a subpoena, warrant or order from a court, the use of ICBC’s facial recognition software and database for the purposes of responding to disclosure requests from police is not authorized under PIPA. The OIPC recommended that where a police force intends to ask for a subpoena, warrant or order, the ICBC should provide the court with a detailed description of the process that it must undertake when attempting to identify individuals using its facial recognition database; this will assist the court in understanding the nature and extent of the change in use that is being requested.

John Jager, CIPP/C, CIPP/US, is vice president of research services at Nymity, Inc., which offers web-based privacy support to help organizations control their privacy risk. He can be reached at john.jager@nymity.com.
EU—Article 29 Data Protection Working Party Opinion 01/2012 on the data protection reform proposals

By Jan Dhont and Emily Hay

On 23 March, the Article 29 Data Protection Working Party (Working Party) adopted its opinion on the data protection reform proposals of the European Commission. The Working Party broadly welcomes the proposals for seeking to reinforce the position of data subjects, enhance the responsibility of controllers and strengthen the position of supervisory authorities both nationally and internationally. In spite of this positive stance, however, the Working Party believes that parts of the proposal for a regulation need clarification and improvement. Regarding the proposed directive in the area of police and justice, the Working Party underlines the need for stronger provisions and expresses disappointment with the commission’s level of ambition in this field.

The Working Party’s comments cover a range of areas including consistency and comprehensiveness; the role of DPAs and EDPB; the role of the European Commission; recommendations regarding particular provisions, and areas where provisions are lacking.

Consistency and comprehensiveness
The Working Party would have preferred a comprehensive reform proposal in one legal instrument rather than a separate directive and regulation. To this end it believes that the substantive provisions of the regulation and directive should be brought closer together and consistency between the texts should be ensured. The Working Party believes that the EU institutions should be bound by the same rules that apply at member state level, meaning that Regulation 45/2001 should be aligned with the proposed regulation. While encouraging consistency and comprehensiveness in the regime, the Working Party emphasizes such efforts should in no way lower current data protection standards. The Working Party regards the broad and unspecified exceptions for public authorities as unjustified and suggests that, as far as possible, the private and public sectors be treated in the same way.

Role of DPAs and EDPB
The Working Party believes that its important role in policy making—until now and in the future as the European Data Protection Board (EDPB)—should be reflected in the proposals. It also suggests that the European Parliament, as well as the commission, be empowered to ask the EDPB for an opinion on any question covering the application of the regulation under Article 66(1)(b). Such request could result in the EDPB issuing guidelines, recommendations or best practices addressed to the supervisory bodies in order to encourage consistent application of the regulation. The Working Party strongly suggests including an obligation that the commission consult the EDPB regarding adequacy decisions (Article 41), standard data protection clauses (Article 42), European codes of conduct (Article 38) and delegated and implementing acts (Articles 86 and 87). It believes DPAs should have the power to carry out audits as well as investigations and to define their own priorities. The Working Party considers that criteria are necessary for determining the lead DPA in a particular case and that cooperation between DPAs, where more than one is concerned, should involve assessments made by consensus.
Role of the European Commission
The Working Party is concerned with the extent to which the commission is empowered to adopt delegated and implementing acts. Because some provisions of the regulation cannot be applied without those acts in place, essential elements should be inserted into the regulation to ensure legal certainty. At the very least, the Working Party calls for a timetable of acts that the commission intends to adopt in the short, medium and long term. The Working Party also has strong reservations regarding the role foreseen for the commission in individual cases which have been dealt with under the consistency mechanism. It believes this role will encroach upon the independent position of DPAs, and that instead, the commission should provide its legal assessment but in principle refrain from interference in the process.

Particular provisions
The Working Party makes suggestions regarding the following provisions:

- Thresholds designed to alleviate burdens on micro, small and medium enterprises (MSMEs) should be based on the nature and extent of data processing carried out by enterprises rather than the size of the enterprise itself.
- Further clarification is needed regarding the meaning of “offering goods and services” and “monitoring of their behavior” in Article 3(2), which defines the scope of the regulation as it applies to a controller not established in the union that is processing the personal data of data subjects residing in the union. Offering goods and services should include “services provided without financial costs to the individual.”
- Recital 24, which defines personal data, is unduly restrictive and should include, for example, IP addresses and cookie IDs.
- Article 4(11), defining biometric data, should be amended to focus on what types of data are to be considered biometric data instead of defining it as data that allows the unique identification of an individual, which would exclude data used for authentication rather than identification.
- Article 4(13) and Recital 27 determine the location of the main establishment of a multinational company but require clarification. This could take into account whether one establishment has “dominant influence” over processing operations for data protection rules. These rules are vital for determining the lead DPA in terms of Article 51(2); the DPA of the member state where the controller has its main establishment is deemed the DPA competent for the supervision of processing activities in all member states.
- The concept of pseudonymisation should be introduced more explicitly.
- Article 6(4) allows further processing of data to be carried out, even where the purpose of the processing is not the same as that for which it was collected, as long as a legal basis can be found in Article 6(4)(a)-(e). This provision should be deleted or redrafted as it leaves open the possibility of further processing of data for incompatible purposes.
- Article 25(2)(a) should be deleted. This provision removes the obligation to designate a representative within the European Union for controllers established in a third country where the European Commission has decided that the third country ensures an adequate level of protection. Data protection impact assessments, which are required under Article 33 where processing operations present specific risks to the rights and freedoms of data subjects, should also be required when processing operations are “likely to” present those risks and not just when the risk is clear.
• Article 73(1) provides that every data subject shall have the right to lodge a complaint with a supervisory body in any member state. This should be amended to allow a complaint to be lodged only in the jurisdiction where a data subject resides or where the controller or processor is located rather than in any member state.

Provisions lacking
The Working Party regrets that the following areas have not been specifically addressed by the regulation or directive:

• The issue of the collection and transfer of data by private parties or non-law enforcement public authorities that are in fact intended for law enforcement purposes;
• The manner in which rights can be executed by representation, for example for minors, incapable persons and by lawyers;
• Third-party compliance with the right to be forgotten;
• The use of Mutual Legal Assistance Treaties in case of disclosures not authorized by EU or member states law should be obligatory;
• How to enforce the judgment of a court of one member state; i.e., where the data subject has habitual residence, when the controller or processor is established in another member state.

Jan Dhont heads the privacy practice of Lorenz Brussels. He specializes in data protection and privacy, telecommunications, media and technology law. He can be reached at j.dhont@lorenz-law.com.

Emily Hay is a member of the Data Privacy Team at Lorenz Brussels.
GERMANY—Facebook "Friend Finder" functions violate German privacy rules

By Flemming Moos

Several functions of the social network Facebook have been under scrutiny by German data protection authorities for some time. Now, a first judgment has been issued: In its decision dated 6 March, the Regional Court of Berlin held that certain Facebook "Friend Finder" functions, which have been amended meanwhile, shall violate the Federal Data Protection Act and the German Act Against Unfair Competition. The suit was filed by a German consumer protection organization. According to the court, the invitation and reminder e-mails were sent out for marketing purposes. Therefore, opt-in consent by the recipients would have been required; however, such consent was not given. The court further decided that the access to and the upload of address book data—especially e-mail addresses for the purpose of the friend finding function—also lacked valid consent of the users. The court held that the consent wording was not specific enough. In particular, adequate information on the purpose and the way of processing the data was lacking. Interestingly, the court affirmed the applicability of German law because the Facebook users and Facebook had—in their opinion—made a respective choice of law under the Rome I regulation.

It can be doubted that German data protection law is actually applicable as the court decided. In order to determine the applicable law, both the Federal Data Protection Act and also the EU Directive 95/46/EC refer to the location of an establishment of the data controller located within the EU. As Facebook Europe is established in Ireland, it seems as if Irish data protection laws should have been applied. Generally, it seems doubtful whether a choice of law exists with respect to data protection rules. The relationship of the EU Directive 95/46/EC and the Rome I regulation is an unsettled issue.

Flemming Moos is a partner at Norton Rose in Germany and a certified specialist for information technology law. He chairs the IAPP KnowledgeNet in Hamburg and can be reached at flemming.moos@nortonrose.com.
UK—UK CBI: Draft regulation “risks strangling innovation”

By Brian Davidson

The UK Confederation of British Industry (CBI), the UK's largest business lobbying group, responded to the Ministry of Justice’s Call for Evidence on the draft EU Data Protection Regulation on 16 March, stating the regulation will threaten many innovative business models and place a compliance cost burden on businesses, which may deter investment and be passed on to consumers.

The CBI is calling upon the European Commission (EC) to revise its proposals in favour of a proportionate, risk-based approach to the scope of data protection regulation, taking into account the benefits versus the costs of any changes and their impact on innovative business models.

“We're concerned that the EC’s proposed data protection reforms will put European businesses at a competitive disadvantage in a global market by placing restrictive controls and high cost-burdens on innovation and investment,” said CBI Director for Competitive Markets Matthew Fell.

“Many novel business models rely on data-sharing to generate revenue and offer a more individually tailored user experience. Advertising and subscription-based online music sharing services are a good example where we’ve recently seen groundbreaking innovation through partnerships with social networking sites. Sharing information about music likes and dislikes online, without sharing the actual content, means millions more customers can now enjoy listening to music online legally—a lifeline for the flagging music industry” continued Fell.

The CBI also identified the EC as having overestimated the financial benefits to businesses of the proposed regulation and underestimating compliance costs. In particular, it specified the associated costs in changing current IT systems, retraining staff and reissuing customer terms and conditions. It estimated that equipping a call centre to handle issues arising from the changes alone could cost around £100,000.

The CBI identified the requirement to appoint a data protection officer over a two-year period as a potential business cost of between £30,000 and £75,000 per year and expanding the role of the UK Information Commissioner’s Office (ICO) to process the additional data protection work as placing an additional cost burden on UK tax payers.

UK—Plans for greater Internet monitoring powers spark privacy debate

By Brian Davidson

Government plans to allow for wider monitoring of the public's e-mail and social media communications by police and national security services have divided opinion and attracted criticism from civil liberty campaigners.

The proposals, which are understood to permit access to the date, time and parties of a communication, may be introduced to Parliament via the Queen's speech on 9 May and rely on Internet service providers (ISPs) gathering the information and allowing government intelligence operatives to scrutinise it. The
plans have been criticised by some campaigners as potentially facilitating unfettered access to communications, building on laws such as the Regulation of Investigatory Powers Act—which are already accused by some of undermining the privacy of individuals.

The UK government argues that updated laws are necessary for police and security services to obtain communications data in certain circumstances in order to investigate serious crime and terrorism and to protect the public.

The UK Information Commissioner's Office said in a statement, “The information commissioner's role in this Home Office project, both under this government and the last, has been to press for the necessary limitations and safeguards to mitigate the impact on citizens' privacy. We will continue to seek assurances, including the implementation of the results of a thorough privacy impact assessment (PIA). Ultimately, the decision as to whether to proceed with the project is one which has to be taken by Parliament.”

**UK—ICO issues updated guidance on identifying data controllers and data processors, “disproportionate effort” and “regulatory activity”**

By Brian Davidson

The UK Information Commissioner's Office has updated some of its practical guidance documents aimed at assisting organisations in dealing with their data protection obligations.

“Identifying data controllers and data processors” recognises the difficulty in identifying the relevant parties as a result of the variety of different interrelationships that exist between organisations involved in the processing of personal data to any degree jointly with others. The guidance refers to various practical examples of where “controller-processor” and “joint controller” relationships may exist and offers definitions on the types of different client and service provider that can exist in order to help organisations determine their applicable responsibilities and obligations.

“Disproportionate effort” sets out the obligations of an organisation to comply with a subject access request—and to what extent it can rely on the “disproportionate effort” exemption—the guidance again provides practical examples and clarifies that the scope of the exemption only applies to the task of responding to a subject access request by providing a copy of the information in permanent form—it does not apply to the effort required to locate the personal data.

Finally, “Regulatory activity” sets out the circumstances in which the regulatory activity exemption under Section 31 of the Data Protection Act may be used by organisations to withhold requested information or to be provided under the subject information provisions of the act.

**Brian Davidson** is a privacy and information advisor in Field Fisher Waterhouse's Privacy & Information Law Group. He may be reached at brian.davidson@ffw.com.
Employers are making good use of applicants’ social network profiles, but should they?

By Angelique Carson, CIPP/US

Making a good first impression when it comes to applying for a new job no longer involves simply spell-checking a resume. That's because employers are now capable of eyeballing more than just a candidate's job history and references; these days, social media profiles provide a much broader picture.

Some employers are now using social networking pages to create a profile of a job candidate—a sort of “Facebook score” comparable to a credit score with the difference being that employers must obtain an applicant’s consent for a credit score and even then don’t get such access as a front-row seat to the applicant’s most recent “Friday night out” or posts about ex-relationships.

Proponents of Facebook scoring might point to new research showing the correlation between one's Facebook persona and predicting their future job performance, according to a February MSNBC report. Professors from Northern Illinois University, the University of Evansville in Illinois and Alabama’s Auburn University have determined a “Facebook personality score.” The study looked at 56 Facebook users and scored them based on personality traits such as conscientiousness, emotional stability, agreeableness, extraversion and openness as perceived via data posted on each user’s page. Those scores were compared with supervisors' evaluations of the users six months later, and the research showed a positive correlation: the higher the Facebook score, the higher the evaluation.

It’s a theory employers seem willing to test out. A 2012 study conducted by Harris Interactive for CareerBuilder.com questioned more than 7,000 employers and found that two in five companies are, in fact, using social networking sites to make hiring decisions. Forty-nine percent said a candidate’s “provocative or inappropriate” photos or information contributed to the decision to deny the applicant a job offer, and 33 percent said posts about former employers or coworkers were determining factors.

Conversely, 29 percent said they in fact hired a candidate based on social networking research due to indicators such as a “good personality,” a conveyed “professional image” or “great communication skills.”

Fifteen percent of those who said they do not conduct online research about candidates said their company bans the practice. Employers predominantly use Facebook to screen applicants, the study indicated, but LinkedIn, MySpace, Twitter and blogs are also surveyed.

A similar CareerBuilder.com survey conducted in 2009, however, indicated that 45 percent of those polled used social networking pages to screen candidates, The New York Times reported, marking a drop of eight percent in three years.

Meanwhile, last year, Mashable reported on social media monitoring service Reppler's survey of more than 300 hiring professionals that found that more than 90 percent had visited an applicant’s social networking profile and that 69 percent had rejected the applicant based on findings.

A Reppler reputation-management tool allows individuals to continuously monitor their online profiles on sites like Facebook, LinkedIn and Twitter by flagging content that could be harmful to an individual’s reputation and allowing users to make real-time decisions about whether they want to remove the photo or comment from public view, for example.
The year-old service is popular not only for job seekers but also anyone conscious of how they might be portrayed online, according to Lyn Chitow Oakes of TrustedID, an identity theft and credit monitoring company that recently acquired Reppler.

“People are making hiring decisions based on data available at their fingertips to evaluate a candidate,” Oakes said. “Your interview may be your Facebook page.”

CareerBuilder Senior Career Advisor Ryan Hunt said there are likely a variety of reasons employers choose not to use social media in hiring decisions, ranging from legal concerns to a belief that the traditional hiring process continues to be the fairest.

However, he points to the research indicating many employers’ decisions to hire based on applicants’ online data, noting that “savvy job seekers are able to turn their social or professional networking profiles into an extension of their resume without sacrificing their privacy,” said Hunt.

Attorney Lisa Sotto of Hunton and Williams said hiring decisions based on applicants’ online data is indeed a topic of concern to her firm’s clients, noting “The question is what is sort of ethically acceptable and what is not?”

Phil Gordon, an attorney at Littler specializing in employment and workplace privacy law, said when considering the ethics of such practices, it’s important to recognize that social media data was never really private to begin with.

“It’s simply not,” Gordon said. “It’s being shared with potentially dozens of people, none of whom are under a legal or contractual duty to maintain the privacy of the information. Anyone could disclose the information on a restricted Facebook page or other social media site to a reporter or could themselves republish it on a publicly available blog.”

Sotto said the onus is on the user to determine what data they would like to publicly post online.

“I think it’s very difficult to impose rules on employers because there is a slippery slope once you go down that path.”

Can employers ask for social media passwords?

In early April, Maryland became the first state in the U.S. to ban employers from asking employees and job applicants for their online account passwords, and national lawmakers as well as states including California, Illinois and Michigan are preparing similar laws aiming to address what employers can and cannot do with employees’ and job applicants’ data.

Gordon said there often will be cases in which an employer must access employee data, such as if the employer has information that trade secrets are being mishandled or if security or financial laws are being broken. The Maryland law recognizes and allows for these exceptions, Gordon says, adding the law also has its shortcomings. (See Gordon’s article, “Maryland ‘Facebook law’ raises new obstacles for employers vetting applicants and investigating employees but with important exceptions,” in this month’s edition.)

Gordon noted that of the hundreds of private employers he counsels, he’s not aware of any asking candidates for their passwords in order to create a Facebook score.

Sotto says the public—particularly young people who don’t yet have the necessary foresight but tend to be very open communicators online—needs education on the potential perils of posting data to social networking sites.
“That will happen over time, but because this is all so new, it hasn’t happened yet. We’re still in the nascent stage,” she says.
IAPP Privacy Vanguard and HP-IAPP Privacy Innovation Awards nomination period now open

Nominations are now being accepted for the 2012 HP-IAPP Privacy Innovation Awards and the 2012 IAPP Privacy Vanguard Award.

The IAPP Privacy Vanguard Award is given each year to the privacy professional who “best demonstrates outstanding leadership, knowledge and creativity in the field of privacy and data protection, whether through spearheading projects or programs that positively impact the privacy profession or through achievements over the course of an entire tenure or career.”

The HP-IAPP Privacy Innovation Awards, meanwhile, recognize winners in the large organization, small organization and technology categories. For the large and small organization categories, the IAPP defines an innovative privacy program as a program “implemented by an organization for the purpose of safeguarding the privacy of consumer, citizen, supplier and/or employee data.” For the technological innovation category, the IAPP defines innovative privacy technology “as a product or service that also serves to safeguard the privacy of consumer, supplier and/or employee data.”

Acxiom Corporation Executive for Global Public Policy and Privacy Jennifer Barrett Glasgow, CIPP/US, received the 2011 IAPP Privacy Vanguard Award. In honoring Barrett Glasgow, IAPP Past Chairman Bojana Bellamy, CIPP/E, said her “extensive body of work and deep expertise has helped advance and influence global data protection in tangible ways.”

For 2011, the HP-IAPP Privacy Innovation Award went to Warner Bros. Entertainment for its “Put Yourself in the Picture Awareness Campaign” in the large organization category. The not-for-profit Ontario Telemedicine Network was the winner in the small organization category for its efforts to reduce privacy incidents by including privacy in its strategic plan and building and executing a successful two-year strategy to improve data protection. In the technology category, Heartland Payment Systems won the HP-IAPP Privacy Innovation Award for its E3™ end-to-end encryption solution for preventing credit/debit card fraud by protecting cardholder information through the entire transaction.

Nominations for the 2012 awards will be accepted through August 3, and the awards will be presented at the Privacy Dinner on October 11 in San Jose, CA. For full details on the awards and the nomination process, visit the IAPP website.

— IAPP Staff

View Photos
(Must be a Facebook user and logged in to view.)