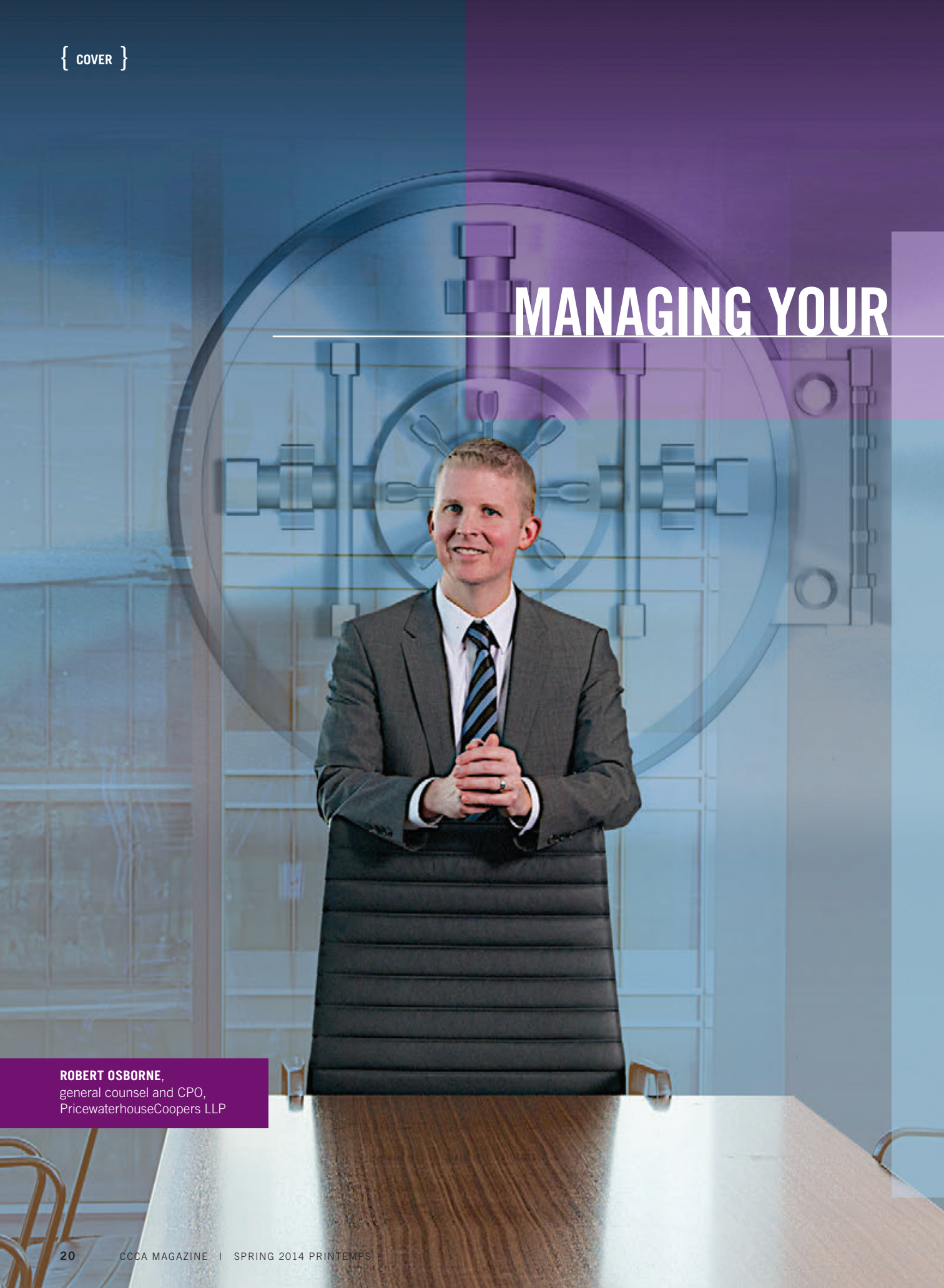
MANAGING YOUR



ROBERT OSBORNE,
general counsel and CPO,
PricewaterhouseCoopers LLP

PRIVACY RISK

AN IN-HOUSE GUIDE

By Pablo Fuchs

"It wasn't even on our radar back then. In my first month on the job here, our then general counsel came to me and asked, 'How would you like to be our expert on privacy law?'" says Robert Osborne, general counsel and chief privacy officer (CPO) with PricewaterhouseCoopers LLP in Toronto, who began working with the global accounting giant nine years ago.

"Since then, we have expanded our focus on privacy," he continues. "We have a small [legal] team here of six lawyers, and in addition to myself, we have another lawyer who is now certified as a privacy professional, and a third lawyer who's taking courses and getting up to speed in this area because it affects our business on multiple levels."

Osborne is only one of many corporate counsel across Canada who has been affected by the drastic change in the workplace when it relates to privacy-related matters, with these issues having gone from an afterthought to top of mind in only a decade.

COMPLYING WITH LEGISLATION

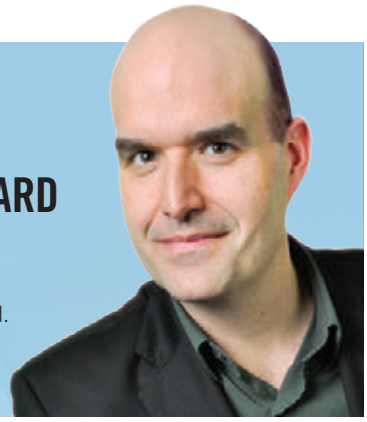
Although Quebec was the first jurisdiction in Canada to put into force private-sector privacy legislation in 1994, things took off in 2004 with the full implementation of the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) and similar provincial legislation — the *Personal Information Protection Act* (PIPA) — in British Columbia and Alberta. The federal *Privacy Act*, which has been in force since 1983, imposed obligations on federal government departments and agencies to respect the privacy rights of individuals, but PIPEDA and the PIPAs go far beyond that, extending the protection of personal information to private-sector organizations. And while the federal and provincial legislations are substantially similar, each has its own unique set of rules and regulations by which companies must abide.

Meanwhile, some other provinces, such as Ontario, have no PIPAs, but they do have privacy acts that relate to personal health information. As well, companies operating in Manitoba will soon have to wrap their heads around that province's privacy legislation, the *Personal Information Protection and Identity Theft Prevention Act*, which was passed in the fall of 2013 but is not yet in effect. Thus, navigating this legislative minefield is no easy task for corporate counsel.

"You have a patchwork of different legislation and you really need to understand what your obligations are to employees in those various jurisdictions. So, when you have employees spread out across the country, you really have to make sure you're compliant with all these different layers of legislative requirements as it pertains to privacy. What we do at Xerox is take the most stringent provision and make it the standard for all employees in Canada," says Daniel Bourque, senior corporate counsel and CPO with Xerox Canada Ltd. in Toronto.

And if being in tune with the various laws weren't enough, new and emerging case law is redefining the landscape. In November, the Supreme Court of Canada released a significant deci-

> **"WE TAKE THE MOST STRINGENT PROVISION AND MAKE IT THE STANDARD FOR ALL EMPLOYEES IN CANADA."**
>
> Daniel Bourque, senior corporate counsel and CPO, Xerox Canada Ltd.



sion in *Alberta v. United Food and Commercial Workers, Local 401,* in which it stated that even though Alberta's PIPA plays an important role in protecting privacy, it infringes the constitutional right to freedom of expression under the *Canadian Charter of Rights and Freedoms* and, as a result, it must be struck down. The court has given Alberta's government a year to amend the legislation. (It's likely that changes to the other provincial acts and PIPEDA will also be made because of this decision.)

Another notable case is the Ontario Court of Appeal overturning a lower court's decision in *Jones v. Tsige* in 2012. "[This] established the new common law tort of intrusion upon seclusion, which is very important because until this case, there was no recognized tort of invasion of privacy in Ontario — and this tort can fill a lot of the gaps that exist in the statutory framework," says Lyndsay Wasser, a partner with McMillan LLP in Toronto who focuses on employment and privacy law, and co-authored the recently released guide, *Privacy in the Workplace, 3rd Edition*, with fellow McMillan partner Éloïse Gratton in Montreal.

COLLECTING AND PROTECTING INFORMATION

Weighing against all this is that companies are using advances in technology to gain greater knowledge on both employees and prospective employees, and to manage data across various jurisdictions. Ensuring that your company stays on the right side of the law is critical when engaging in such activities. "The most common issues that tend to come up over and over again regarding privacy and employee information," says Wasser, "relate to background checks and several matters relating to the hiring process, as well as transferring of employee information across borders, and the monitoring of employees."

In terms of background checks and the hiring process, most companies want to know how far they can go in getting information about prospective employees. For instance, many firms now want to do a check on a person's medical history, driving record or credit history. "More and more, we're seeing on employment forms prospective employees agreeing to have their information disclosed to a prospective employer," says Gratton, noting that this is a legal requirement for doing background checks. "The bottom line, though, is that the information has to be relevant for the job. So, let's say it's a criminal background check. If the employee will work in a sensitive capacity, with the elderly or children, or managing funds, this is justified. But if the employee is just stocking shelves in a warehouse, this is not relevant."

In addition, Wasser points out that if you're collecting more information than you need — even with consent — you could violate the privacy laws, whether it's a background check or the information a company is collecting on the application forms. As an example, she says some companies get applicants to put their social insurance numbers (SINs) on the application forms, "but you don't need the SIN of every applicant; you only need the SINs of people that you hire."

Once employees are hired, the two other most common issues that Wasser cites come into play. In today's globalized society, firms may need to transfer private employee information to another jurisdiction. This may be to head office, an affiliate or an employee benefits provider, which could be located in the U.S. or overseas. "There are — again, depending on which jurisdiction you're in — specific rules around that, the most restrictive of which, in the private sector, is Quebec. But there are some notice requirements in Alberta and there's some case law under PIPEDA about things you have to do when moving information across borders," she explains.

There are guidelines from the federal Office of the Privacy Commissioner that recommend certain measures be taken to protect the information when it crosses the border. "[But] in Quebec, you need to let the service provider know what type of security measures they need to adopt [to meet Quebec's laws] and you need to have a contract. It's a legal requirement to do so," Gratton says. "Another thing that needs to be taken into account: let's say the human resources department is outsourcing the payroll services to a U.S. company, which happens all the time, it needs to provide the service provider with only the necessary information for the outsourcing activity. So all they need to know is the employees' banking information. They don't need the complete profile, and that's a mistake many make."

MONITORING EMPLOYEES

As for the monitoring of employees, "this is becoming more and more of an issue because of the various ways that employers want to monitor their employees," Wasser says. In the past, she notes, this was mostly limited to installing surveillance cameras for security purposes or to prevent theft, "but these days, you have a lot of computer monitoring, such as watching what people are doing on the Internet, accessing employees' emails. And companies are also adopting new technologies, such as GPS tracking, or fingerprint or retina scanning for security purposes, so the ways employees are being monitored is increasing."

The challenge, she adds, is that the privacy commissioners in each jurisdiction have adopted slightly different tests to determine when monitoring will be acceptable — "but the one common theme that comes up is that the purpose of the monitoring is very important." So, if security is the purpose of the monitoring, there's generally less scrutiny than if it is trying to track an employee's proficiency, productivity and performance.

This latter point is very concerning to Dr. Avner Levin, chair of the law and business department, and director of the Privacy and Cybercrime Institute at Ryerson University in Toronto. With employers now using technology to make the workplace more productive, "the big risk is that technology is replacing human beings in terms of discretion and evaluation and decisions in which to take action. So when you automate the process, the risk is that you lose sight of the human being who's working for you," he explains.

In particular, Levin cited several cases in which an employee's privacy was violated when companies used technology to monitor an employee's lack of productivity where a conversation with the employee would have sufficed. "The concern for workplaces is that you're now relying on software to do the job for you. The introduction of technology must be proportional. You can't just violate an employee's privacy for a purpose that's not worth the violation," he says.

"MORE AND MORE, WE'RE SEEING PROSPECTIVE EMPLOYEES AGREEING TO HAVE THEIR INFORMATION DISCLOSED."

Éloïse Gratton, partner, McMillan LLP

STAYING CURRENT

It's no surprise then that as a result of all this, corporate counsel — many of whom have also been designated with the CPO title — have to take privacy matters very seriously. Given the constant changes taking place in this area, it's important to have a good network of external counsel upon which to rely, says Osborne, but that's only the first step. "It's a changing area of law and it's critical that someone in the in-house group is familiar with the law," he explains. "It's important not to rely exclusively on external counsel. You need somebody internally who knows the business and who understands where the risks are in an organization."

"THE NEW COMMON LAW TORT OF INTRUSION… CAN FILL A LOT OF THE GAPS THAT EXIST IN THE STATUTORY FRAMEWORK."

Lyndsay Wasser, partner, McMillan LLP

"THE BIG RISK IS THAT TECHNOLOGY IS REPLACING HUMAN BEINGS IN TERMS OF DISCRETION AND EVALUATION."

Dr. Avner Levin, Ryerson University

These people then need to dedicate themselves to privacy, Bourque explains, noting that they should know the legislation and "follow very closely changes in the law, either by way of amendments to the legislation or case law, and how they apply to your organization." This is critical, he says, because even though most large companies already have established privacy policies in place, the CPO or lawyer in charge of this needs to look at them "at least on a yearly, if not on a biyearly, basis to make sure they address everything that you've encountered along the way."

Once all this has been taken care of, it's important that the information is shared in a collaborative manner with critical departments within your organization to ensure not only the necessary changes are made, but also all the players in the company are aware of the way things must now be done. It's also critical to have the will and full backing from senior management to make this all happen.

"You need to have support from the top and that means having privacy representatives or coordinators in each of the key departments, such as Marketing, HR and IT, with whom the CPO and legal team can work," says Heather Innes, counsel, global process leader, international trade law and CPO with General Motors of Canada Ltd. in Oshawa, Ontario. "Having a privacy team that can work collaboratively is key to ensuring that your organization identifies and appropriately addresses privacy issues in the developmental stages of product and initiative strategies. You want to have the privacy issues identified early. That means less disruption, a more effective and often less expensive solution. Once you have your privacy team in place, it's equally important to establish a process that permits the continuous sharing of privacy information and updates throughout your organization."

Having such a structure in place is critical because privacy issues will be constantly evolving in the workplace. Not only will legislative amendments and case law lead to critical changes, but also the evolving nature of the workplace itself will make all this more challenging than ever before. "The big thing corporate counsel need to think about is what technology is doing in blurring the boundaries between work and personal lives," Levin says. "It's no longer a 9-to-5 simple relationship anymore; it's a very different workplace these days and that's where the challenges lie." ▮

Pablo Fuchs is a freelance writer based in Toronto.

"YOU WANT TO HAVE THE PRIVACY ISSUES IDENTIFIED EARLY…LESS DISRUPTION, A MORE EFFECTIVE AND OFTEN LESS EXPENSIVE SOLUTION."

Heather Innes, counsel, global process leader, international trade law and CPO, General Motors of Canada Ltd