CPOCORNER
Interviews with Leading Chief Privacy Officers
By Ruth Hill Bro

NAME
Catherine Kurtz

TITLE
Global Data Privacy Officer

COMPANY/ ORGANIZATION
Sterling Commerce, Inc.

1. What career path led you to your current position (and are you a lawyer)?

A fairly interesting path led me here! My career has spanned the entire IT gamut: from coding and network software installations for large financial institutions, to consulting, to directing sophisticated development and integration teams. Not being a lawyer, I had minimum experience with the regulatory sphere; however, I did possess intimate subject matter expertise in data life cycles, data flows, and strategic and tactical project and policy development and implementation—all important components at the core of data protection analysis.

After 20 years of those data, technology, and managerial experiences, I was challenged by Y2K to determine the impact of European data protection laws on a global organization with a U.S.-centric data model. After weeks of real research and a theoretical base of information, I cold-called some prominent CPOs to understand what the "gold standard" of data protection might look like. That challenge, and the subsequent privacy program, led to the first telecom to join Safe Harbor in 2001, and my first appointment as CPO.

2. What is the name of your department, and where is it positioned within the organization (do you report to the GC, CEO, CIO, etc.)?

As global data privacy officer, I am positioned in the Global Information Protection Group and report up through the chief compliance officer, who reports to the CEO.

3. How many people in your organization are tasked with some aspect of privacy compliance, and what are their job functions? Consider direct reports and budgetary responsibility, as well as those outside your group.

Because Sterling Commerce solutions are used by 80 percent of the financial companies in the FORTUNE® 1000, every employee at Sterling Commerce is part of our privacy compliance solution. Aside from mandatory participation in several levels of annual privacy training, we all own a piece of the compliance puzzle.

The privacy compliance team itself is a highly matrixed compilation of international employees making reasonable and dedicated efforts to implement compliant and consistent global processes, with help from participants throughout the organization, including legal, business subject-matter experts, customer care professionals, human resources, PR/corporate communications, senior executives, and especially information security. My team also partners with the regulatory, legal, and compliance professionals of our parent corporation as necessary.

4. Why did your organization appoint a chief privacy officer, when did this occur, and is this a full-time position?

Sterling Commerce has a history of proactive compliance and customer focus. The position of chief data privacy officer was established as a result of an ongoing analysis of the company's data protection strategy, coupled with the changing regulatory environment. The head of Security and the CIO evaluated the progress of Sterling Commerce's then-current data protection program against strategic goals and agreed it was time to augment the project with a dedicated, full-time privacy officer. I came on board in early 2006.

5. What factors do you think are key to a privacy officer's effectiveness? Consider not only education and skill set, but also budget, head count, level within organization, etc.

First and foremost, a privacy officer requires the ability to easily explain complex and sometimes contradictory international data protection laws in layman's terms.

Other key attributes are liaising, communicating, diligence, and tenacity. A privacy officer needs to be proactive and proficient at liaising with an array of levels and business functions throughout an organization to achieve the goals of reasonable risk reduction and adequate compliance.

Additionally, security is rarely convenient, and privacy is perhaps less so, because it adds a new dimension to security precautions. It requires a new way of thinking about data—not just as a commodity with a life cycle owned by a business, but instead as pieces of someone else's personal property. A privacy officer who is successful in empowering employees to treat personal data (whether it relates to a fellow employee, a valued customer, or a third party) in a careful, protected, and "borrowed" fash-

Bro is a partner at Baker & McKenzie LLP in Chicago, Illinois, and the Chair of the Section of Science & Technology Law. She can be reached at bro@bakernet.com.

Published in The SciTech Lawyer, Volume 6, Number 1, Summer 2009. © 2009 American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

ion, while also attending to the employees' other responsibilities, will be highly effective.

6. Who is your biggest ally in your organization and why?

For my team at Sterling Commerce, it has been vital to create a high level of synergy between international security, privacy, and legal. There are strategic and tactical differences in how each of these teams will approach and assess the issue and formulate a solution that, if worked on together, will be greater than the sum of its parts in terms of highest impact on corporate risk reduction.

7. How do you make the case internally for resources and explain the value of what you do (ROI)?

Sterling Commerce's strategic and customer-oriented approach to privacy compliance requirements simplifies the justification of dedicating resources for identified company privacy initiatives.

8. How do you measure the success of your privacy initiatives?

- How well customer and employee personal data is protected is the true measure of success: employees embracing the culture of privacy, and their awareness of data protection requirements and knowing where to turn with questions, regardless of where they're located around the world.
- Sterling's ability to effectively respond to customer inquiries regarding the company's personal data protection efforts.
- The degree to which privacy is incorporated into company process, practices, and strategies and not just into company policy.

9. What percentage of your day is spent on: creating policy, providing privacy consulting, conducting training, assessing/auditing compliance, or other responsibilities?

Today, with a significant portion of my global program largely established, I am focused on the assessment and audit for internal corporate compliance as well as for Safe Harbor compliance, while staying up-to-date with emerging international regulations, trends, and privacy cases. I also concentrate on mitigating any findings while staying on top of new regulations. Privacy is a cyclical process—your global practice may be established, yet new laws are still emerging while your business goals are also morphing with the times.

Initially, when a privacy officer is tasked to launch a global compliance program, the majority of the day will be spent assessing current compliance and formulating a gap analysis. Gaps are then prioritized based on the company's tolerance for risk while considering cost and effort. Gaps are then mitigated by introducing new or modified policies, processes, and procedures. Adequately training the workforce is critical. I keep a running list of employee training Frequently Asked Questions and Answers available to global employees. Although highly interrelated, my team manages three data protection practices concentrating on Europe, the United States, and Asia/Pacific.

No matter what phase of project development, consulting the business is always a top priority.

10. When there aren't clear answers, what is your framework for managing risk and charting compliance, and to whom do you turn for advice (others within the organization, outside law firms/consultants, others)?

Whether within the United States or abroad, answers are rarely clear in this complex arena of state and federal laws and regulations as well as industry standards. I am proud that Sterling Commerce has proactively pursued full-disk encryption and other risk-reducing measures, but I usually rely on the Department of Commerce's guidance that a company's compliance goal should be to put reasonable precautions and data protection in place.

When a new risk is identified, I have a defined risk-mitigation approach that incorporates research, collaboration, and action. I generally conduct research until an appropriate foundation of knowledge has been developed and then collaborate with my security professionals to review, discuss, and prioritize. Next, I partner with in-country, in-house legal colleagues. If clear direction isn't readily agreed upon, we may turn to subject matter experts from our parent company for assistance. For industry- or country-specific issues, I have access to regional outside law firms that we may contact in specific situations.

11. How do you handle multistate and multicountry privacy law compliance?

We handle multijurisdictional compliance with

Published in The SciTech Lawyer, Volume 6, Number 1, Summer 2009. © 2009 American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

dexterity. The complexity of competing, emerging, overlapping, and sometimes nonharmonious state and country privacy laws is certainly an area of concern for privacy officers and multinationals. This is part of what energizes the privacy discipline and keeps it fun.

I think you make your best effort to stay abreast of developing privacy requirements, remain in compliance with current laws that impact your business, and abide by your own stated privacy policies at all times.

Should a situation arise where there are conflicting compliance requirements, an assessment of any potential competing priorities using the risk-mitigation framework outlined above should be performed and supplemented with discussions with experts and the authorities. I have the utmost confidence that should there be a conflict or concern, authorities take into consideration long-standing and significant efforts toward global privacy compliance.

12. What challenges and opportunities do technology and electronic media present in your privacy initiatives?

Technology can be used to bolster policy initiatives—e.g., implementation of state-of-the-art, full-disk encryption technology while having a policy that prohibits personal data on workstations. Together these initiatives can significantly reduce the potential risk of an "equipment malfunction" breach. Electronic media and mobile devices that are getting smaller, cheaper, and easier to use (and hide) will continue to challenge security and privacy initiatives for a long time to come.

Again, I feel strongly that if you can get your employees and third parties to understand the value to the business of all personal data they encounter through the normal course of business, you can reduce the risk of unintentional loss of personal data through electronic or paper media.

13. How do you keep up with the ever-changing privacy landscape (laws, technology, policy, etc.)? Which privacy websites, publications, conferences, certifications, and other resources do you find to be valuable?

I am a Certified Information Privacy Professional (CIPP) through the International Association of Privacy Professionals (IAPP), and I find IAPP's multitude of resources to be valuable, namely, the Daily Dashboard, industry working groups, and international conferences. I am fortunate to co-chair the IAPP's Denver KnowledgeNet privacy group where local experts speak and network over lunch with local professionals regarding relevant and interesting topics. In addition, I rely on the Internet and my security and privacy peers. It is most enjoyable, and rare, to work with a group of esteemed peers that are effective and generous at working together to share strategies and solutions.

14. What is your approach to training? In particular, what vehicles for training do you offer, and what steps do you take to help foster a privacy-aware environment so that each employee can take an active role in privacy?

When data protection was predominantly an EU concept, I spent a lot of time interviewing U.S. employees regarding their data practices and then training employees and senior executives live, in small-group or one-on-one sessions; this was very effective but was neither a sustainable nor scalable solution. Now, privacy training is incorporated into live or online new-hire orientation, online customer care training, IT requirement definitions, security policy, occasional department meetings, and mandatory annual corporate online training.

15. What have you done to address privacy issues associated with third parties who conduct business on your company's behalf or in support of your business objectives (e.g., outsourcing, service providers, etc.)?

I recommended to my stakeholders that joining the Department of Commerce's Safe Harbor program would demonstrate our commitment to adequately protecting personal data to our employees and customers. The Safe Harbor tenet of Onward Transfer necessitates determining how data flows to third parties. To assess Sterling Commerce's compliance with this principle, I have reviewed data architecture renderings, examined vendor contracts, and interviewed third-party providers, beginning with those with access to the most sensitive employee data, to further my understanding of their data protection practices and policies.

Sterling Commerce now has a formal vendor-management process that includes mandatory contractual language for third-party vendors who

Published in The SciTech Lawyer, Volume 6, Number 1, Summer 2009. © 2009 American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

access sensitive personal data of employees or customers. This process is vetted by Security and Privacy personnel. Sterling Commerce enrolled in Safe Harbor in August 2006.

16. What do you see as the next big privacy issue/trend? And what are you gearing up for in your own organization?

One trend I see is that customers and prospects are now asking questions about their data.

Privacy compliance is much more of an intricate part of business processes and strategy.

We are gearing up to meld the privacy arena into the overall corporate compliance program rather than considering it a stand-alone risk or program. In my experience, privacy compliance has been an outlier for many years as it was unclear to many in the United States how/when/if noncompliance would be enforced. Additionally, I am earnestly awaiting an update to the IT Act of 2000 and monitoring the advances of the Asia Pacific Economic Cooperation group and European data security breach laws.

17. What keeps you up at night when it comes to privacy? And why?

Personally, what keeps me up at night is the lack of transparency on what databases my personal data currently resides in. I recently received an invitation to a college reunion and was informed that some of the college address data in the invitation came from a database purchased 10 years ago. I was pretty surprised about both the retention and sale of that data.

It keeps me up at night that privacy is an established human right in Europe and is not declared as such in the U.S. Constitution, and yet breach notifications are mandatory in the United States and are currently voluntary in Europe.

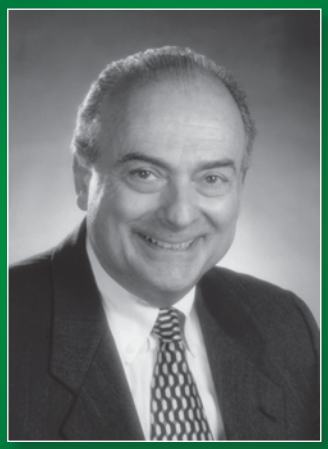
The seamless and instantaneous movement of personal data around the globe with varying levels of regulation, practices, and enforcement keeps me up because of the opportunity that movement presents to steal, breach, retain, and delete data, again transparently.

The dichotomy of privacy and the fascinating advent of social networking keeps me up. I put a chip in my pets; would I chip my child? ◆

Note

The views expressed here represent those of the interview subject and do not necessarily represent the views or practices of Sterling Commerce, Inc., its parent corporations, affiliates or subsidiaries, or any other party.

This article previously appeared in CPO Corner by Ruth Hill Bro, http://meetings.abanet.org/webupload/commupload/ST2300006/sitesofinterest_files/ABA_CPO_Corner_Catherine_Kurtz.pdf, May 2009, Issue 12. Copyright 2009 The American Bar Association. Reprinted by permission.



Edward G. Fiorito, 72, of Dallas, Texas, a past Section Chair of the ABA Section of Science & Technology Law (1984–1985) and of the ABA Section of Intellectual Property Law (2000–2001), died on Monday, April 27, at the home of his son, Thomas Fiorito, in Florida.

Mr. Fiorito received his J.D. from Georgetown Law Center and his B.S. in electrical engineering from Rutgers University. His many years in corporate practice included positions with B.F. Goodrich, Dresser Industries, IBM, Burroughs, and Energy Conversion Devices. He was a member of the U.S. Delegation to the WIPO Diplomatic Conference on Patent Harmonization and an alternate member of the Secretary of Commerce Advisory Commission on Patent Law Reform.

He was preceded in death by his loving wife of more than 45 years, Charlotte, who was tragically killed in an automobile accident in February 2004. Both Ed and Charlotte were great friends of the Section of Science & Technology Law and will be missed.

Published in The SciTech Lawyer, Volume 6, Number 1, Summer 2009. © 2009 American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.