The Metropolitan
Corporate Counsel®
National Edition
www.metrocorpcounsel.com
Volume 22, No. 7

July/August 2014

Data Privacy & Security: Growing Concerns For New Jersey Businesses

Peter J. Torcicollo, *a Director in the Business & Commercial Litigation Department at Gibbons P.C., has recently been appointed leader of the firm's Privacy & Data Security Task Force.*

According to Gartner, Inc., one of the leading information technology research and advisory firms in the world, the financial impact of cybercrime will grow 10 percent per year through 2016, due to the continuing discovery of new vulnerabilities.[1] The average cost of a data breach to a company already exceeds $5.4 million.[2] State and federal governments regularly pass new legislation and implement new regulations in attempts to deal with cybercrime and privacy and security breaches; New Jersey has been particularly active on this front, so businesses based in the state have to keep track of an expanding set of complex rules with which to comply. Clearly, this growing risk can seriously derail operations for a company that does not face it head on and work to prevent costly breaches of data privacy and security, respond swiftly and comprehensively in the event of such breaches, and manage any resulting litigation.

Gibbons established its Privacy & Data Security Task Force to advise clients on privacy and data security compliance, responses to data security breach incidents, written privacy and data security policies, software issues, financial privacy, social networking, and payment card data security, among other related issues, including litigation. The Task Force focuses on technology, e-commerce, cloud computing transactions and advice, and software licensing and commercialization.

Following is a discussion with Mr. Torcicollo on the mission and makeup of the Task Force and the issues the Task Force has been tackling for the firm's clients.

Editor: Why a Privacy & Data Security Task Force, and why now?

Torcicollo: The number of data security breaches rose 62 percent in 2013.[3] The recent Target fiasco demonstrated how badly a security breach can harm a company's operations and reputation, and hackers are increasingly motivated and sophisticated. Malicious or criminal attacks are the leading cause of data breaches, comprising over 40 percent of such incidents.[4] But common system glitches and human errors that also cause data breaches can be avoided – and if they do occur, they must be appropriately addressed. Businesses can no longer ignore this problem, because the risks are just too high. The Gibbons Privacy & Data Security Task Force provides counseling, breach management, and litigation services designed to minimize exposure and return businesses to their normal operations.


Peter J. Torcicollo

Editor: What have been the firm's initial goals for the Privacy & Data Security Task Force?

Torcicollo: Quite simply, we set out to counsel our clients on data protection requirements and all aspects of compliance with them, including U.S. federal and state laws like HIPAA and TCPA; international laws like the EU Personal Data Directive for our clients doing business overseas; and emerging industry standards, which have quickly been evolving. We also set out to assist clients in complying with the laws regarding individual privacy and the protection of data.

Editor: How do you help your clients meet that baseline objective of compliance?

Torcicollo: Our Task Force members start by helping the client to develop a privacy and data security infrastructure, establishing concrete policies and workplace procedures to address general privacy and data security compliance with both domestic and international laws, data sharing, privacy and data security audits, data retention, and payment card data security, among other foundational concerns. Our Task Force members are also equipped to help companies create and fill privacy ombudsman roles when appropriate.

Editor: If your client does suffer a privacy or data security breach, how do you assist?

Torcicollo: We guide the client through the most important first step, which is notification, particularly if the breach impacts the general public. Companies have a legal responsibility to notify consumers about incidents that have caused their personal information to be acquired by unauthorized persons, but the interests of law enforcement must be balanced with those of consumers. Early notification empowers customers, allowing them time to limit damage by, for example, canceling credit cards and alerting credit bureaus to prevent further fraud, which in turn helps them – and the broader public – retain their trust and confidence in the company. These common sense measures can sometimes help a company avoid litigation that has the potential to become a major headache for its in-house legal team, and a major distraction for the core business of the client.

Editor: Are there specific rules for New Jersey businesses regarding notification of a breach?

Torcicollo: By state law, a New Jersey business or any company that engages in

Please email the interviewee at PTorcicollo@gibbonslaw.com with questions about this interview.

commerce in New Jersey must disclose a security breach affecting its electronic data to any customer who is a New Jersey resident. This disclosure must be accomplished as soon as possible, without unreasonable delay. Notice can be written or electronic, depending on the cost of providing written notice, the number of customers to be notified, and whether the company possesses precise contact information for all customers. There are various exceptions to the timing and methods of disclosure if law enforcement is actively engaged in its investigation of the data security breach. Depending on the number of affected consumers, the company may also need to notify the major credit reporting agencies and the New Jersey State Police. It is prudent and, depending on the unique circumstances, can be required that each step in the notification process be documented and such records be retained for a minimum of five years. It is also worth noting that notification may not be required if the company can demonstrate that misuse of the information is not reasonably possible.

Editor: What do you do if there is any additional fallout?

Torcicollo: We have provided advice and counsel to our clients on several occasions in connection with investigations by state and federal regulators, and particularly the Federal Trade Commission, of data security incidents in which our clients were the victims of computer hackers, but faced regulatory scrutiny and potentially huge penalties. We conduct forensic investigations into the root causes of these incidents and help remediate any problems that are uncovered through the audits. Task Force members also handle data breach litigation, consumer protection litigation, and class action defense.

Editor: Are certain kinds of companies particularly at risk?

Torcicollo: According to Symantec, a global leader in data security, storage, and systems management, companies in the computer software, information technology, and healthcare sectors are most vulnerable.[5] And again, given the worldwide headlines surrounding Target's data breach, it should come as no surprise that retailers, especially those engaging in e-commerce, have an increased security breach risk. We have counseled clients that have been victims of cyberhacking and have worked in a matter involving the U.S. Department of Justice's then-largest ever cyberhacking investigation.

Editor: Are there any areas of particular concern for companies that are just launching?

Torcicollo: The business environment in which a startup company today is attempting to get a foothold is more reliant than ever on computerized operations and online commerce. New businesses must be sensitive to consumer and employee data privacy from the outset, setting up adequate systems to secure employee and customer data to the best of their ability and developing, implementing, and enforcing workplace procedures to notify in a timely manner anyone impacted by a data security breach that compromises personal information.

Editor: What are some other unique issues you address?

Torcicollo: There are a number of interesting side issues – tangential but related to the Task Force's standard advice regarding infrastructure development, breach notification, investigations, and litigation – that we look at in order to advise clients holistically on data privacy and security issues. These issues include the risks of cloud computing and certain apps; identity theft risk "red flags" and mitigation; company and employee social networking accounts; online advertising and behavioral marketing; and direct marketing activities. There are also unique privacy requirements connected to particular industries, including healthcare and pharmaceutical; financial services; education; telecommunications; cable and utilities; retail; and mobile/geolocational service providers, among others. In addition, anyone dealing with children must comply with a host of privacy regulations.

Editor: Talk about the mix of talent on the Task Force.

Torcicollo: Our team is the definition of multidisciplinary. We have members who provide counseling, investigatory, and/or litigation services that focus primarily on specific areas – for example: cloud computing and breach reporting obligations; privacy, HIPAA, data security, and related criminal matters in the healthcare arena; general criminal matters that touch on privacy and data breach issues; electronic technology in the securities markets; e-discovery and information management; brand protection, including anti-counterfeiting and trademark enforcement; privacy matters and restrictive covenant and misappropriation litigations in the employment area; and data security technology.

The Task Force works hard to educate all the firm's clients on these issues, preferably before they have to become Task Force clients specifically. For example, we cover data security and privacy topics extensively on various Gibbons blogs, particularly the *IP Law Alert* (iplawalert.com), *E-Discovery Law Alert* (ediscoverylawalert.com), and *Employment Law Alert* (employmentlawalert.com). The firm's popular, annual "Gibbons E-Discovery Conference" typically contains at least one data security panel and has also included a primary focus on privacy and data security.

---

1. http://www.gartner.com/doc/1857814?ref=SiteSearch&refval=&pcp=mpe
2. https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-20...
3. http://www.symantec.com/content/en/us/enterprise/fact_sheets/b-whats-new...
4. https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-20...
5. http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=...