Chapter 38

A Reference For Your Company

§ 38:1 Introduction

As this book demonstrates, the number of laws that companies must comply with is staggering. This chapter attempts to identify common issues for businesses generally, as well as some industry specific issues. While comprehensive coverage of every issue is beyond the scope of this chapter, it does offer examples of pitfalls, as well as policies that companies should consider in order to highlight the most common and important issues. However, it does not catalogue every issue or law identified in the preceding chapters.

§ 38:2 General issues for companies—Marketing concerns

Common examples of general issues include Internet privacy and marketing concerns, commercial e-mail laws, TCPA compliance, including Do-Not-Fax concerns at the state and federal level. For many companies, e-mail and Internet-based marketing is a common form of branding and generating leads, so these issues are becoming all the more common. The CAN-SPAM checklist is a document that helpful for companies to understand their obligations, and companies must make sure they have adequate resources and policies to ensure compliance with the TCPA, including restrictions on auto-dialers or other similar devices. Also, policies that define the conduct of affiliates and other third-parties in the marketing context should be considered. Policies regarding the use of SMS for advertising is also a best practice because CAN-SPAM can also be implicated by the use of these type of wireless messaging.

Having an Internet privacy policy is also in many cases is required, and in most cases is a best practice even if not legally required. While it is not a law that is commonly implicated, the

Lanham Act can be implicated by statements made in a privacy policy, particularly if the issue is raised by a competitor. If applicable, ensuring that compliance with Internet-based privacy laws, such as COPPA, as well as other Internet-based statutes, such as the DMCA, is also important. Finally, having policies regarding the disclosure of identifying information, as well as IP addresses, is also important.

§ 38:3 Two party consent

One of the most challenging issues for companies is managing two party consent issues.[1] While they are obvious in the telephone context, as evidenced by the disclosures that are made before calls are recorded or monitored, many of these same laws apply to electronic communications as well and can create issues when network, or email, monitoring is conducted.[2] This can be true even if the monitoring is done for security, or other reasons. These issues are generally discussed in Chapters 7 and 8, and particular attention should be paid to situations where real-time monitoring is done, where the communications also are made with non-employees, especially if the non-employee is a lawyer, or other person that can engage in a privileged communication. Discussion of when monitoring is considered to be real-time, versus a review of a stored communication, is contained in § 7:17.

§ 38:4 Defining the proper scope of investigations

The proper scope of investigations, including pretexting and wiretapping concerns, as well as concerns over disclosure of information in litigation are issues companies must address. Related issues regarding the permissible scope of searches of employees' offices, including their computers and personal e-mail accounts, as well as videotaping in the workplace are also frequent concerns as well. In some cases, the Fourth Amendment can be a concern in these situations if the government has asked a private citizen to gather information, or the employer is a government agency. There are also concerns over monitoring other forms of electronic communications, such as SMS and other similar forms of messaging, as well as concerns over reviewing communications that are potentially privileged, such as communications with an employee's attorney or spouse. Restrictions on the use of

---

[Section 38:3]

[1]See § 8:43.

[2]See, e.g., § 8:28.

polygraphs and concerns with the improper restriction of e-mail systems if union workers are present also are considerations for many companies. Moreover, the privacy implications of state constitutional and statutory rights of privacy are also important considerations.

Additionally, the implications of monitoring communications with third-parties, including customers, are also a common concern, as is the monitoring of third-party web-based e-mail systems that are accessed with company resources. In certain cases The Patriot Act and FISA can also be implicated. Finally, managing employee background checks, including as part of the employment application process are also issues that companies must be aware of, as are managing issues regarding searches for employee information in publicly available arenas, such as the Web.

Policies that should be considered include policies regarding internal and third-party investigators, policies regarding the use of polygraphs, policies to define the proper scope of searches on company premises, as well as on company equipment, including computers. Having adequate disclosures and policies that inform employees that they do not have a reasonable expectation of privacy is also important, as are policies that define the acceptable use of employee background checks, as well as for compliance with the FACT Act rules on the use of medical information and the appropriate destruction of data should also be considered. Additionally, policies regarding responding to government investigations, including subpoenas are also important to consider.

§ 38:5 E-mail footers

A common question is whether an e-mail footer is required. Putting aside CAN-SPAM compliance (most companies place certain CAN-SPAM required information in the footer), there is no general requirement to have an e-mail footer. Certain industries typically place a disclaimer in the footer and many include a statement concerning the confidential nature of the e-mail and provide guidance in the case of unauthorized disclosure or misdirection. Other, in heavily regulated industries, include a statement regarding their monitoring policies.

§ 38:6 Defining "personally identifiable information"

While not an issue tied to any specific area of the law, defining what personally identifiable information is, including whether IP addresses are personally identifiable, is a growing concern. As

new forms of information become relevant to businesses and individuals, there will be growing concerns about these issues. The EU presents unique issues since there is some indication that the EU's view on IP addresses varies from the U.S. The framework identified by the Principle of Proportionality is important to utilize as a guide for these type of issues.

§ 38:7 Information security requirements

Information security is an issue all companies must face. While the amount of resources devoted to information security will vary given the sensitivity of the data, this issue, particularly in light of FTC enforcement actions and the number of state and federal laws identified herein, is one all companies must consider. Having a plan, including an incident response plan, is helpful and placing appropriate safeguards is also important. Restricting access to sensitive information is also a strategy companies should follow. Making sure all appropriate third parties are bound to meet applicable standards is also something that most companies must consider. Having a plan, including an incident response plan, is helpful and placing appropriate safeguards is also important. Restricting access to sensitive information is also a strategy companies should follow. Making sure all appropriate third parties are bound to meet applicable standards is also something that most companies must consider. Making sure that there is an appropriate level of auditing and compliance for your company is also important. Making sure all of the relevant software is updated and common vulnerabilities are addressed is also an important step.

The importance of these issues is reflected in laws such as SOX and other federal laws have either data security, or data destruction requirements. Obviously, the FTC Act and its restrictions on deceptive trade practices and unfair acts, as well as the accompanying guidance given by the matters brought by the FTC are important for any company to consider in the data security context since data security is a fertile ground for FTC activity. Recent FTC guidance discussed in this book on safeguarding information is also of import. Data security policies, including restrictions on third-parties are policies that should be considered and implemented by many companies.

§ 38:8 Insurance, indemnity and other risk shifting mechanisms

In many cases, assessing and appropriately allocating risk for information security and privacy incidents can result in signifi-

cant savings for your company. There are now brokers who specialize in these types of insurance products and finding the appropriate policy can be very beneficial. Moreover, thought should be given to risk allocation in most contracts where personally identifiable or sensitive data is at issue. Thinking through whether there will be a cap on liability for data issues, who will pay for notice of a security breach, as well as credit insurance for the individuals, and even who will give notice in the event of a breach should be considered. Common issues with indemnities generally should be addressed, including issues regarding the scope and nature of any defense obligation if there is litigation, what level of fault by the indemnified party precludes indemnity, and issues regarding control of the defense and settlement of third party claims.

§ 38:9 Computer crime laws/Confidential information concerns

Computer crime laws are of import (the Computer Fraud and Abuse Act in particular), including for entities that have significant trade secrets since these laws can be triggered if employees take electronically-stored confidential information, or access systems that they are not permitted to. The related Economic Espionage Act is also a law that companies can use to protect their confidential information, as is state trade secret law. Policies that restrict employee access to only those with a need to know confidential information are important first steps, as are policy statements restricting access by competitors of websites that contain confidential or proprietary information. Data security policies regarding access to these types of information are also key for companies.

Computer crime laws are potentially implicated when subpoenas are issued to Internet Service Providers. There are also litigation issues that must be addressed and considered when subpoenas are issued for these types of information.

§ 38:10 Anonymous subpoenas

Anonymous subpoena issues are also important to many companies as they may face a situation where they need to identify an anonymous speaker on the Internet, or in e-mail, who seeks to do the company, or its employees, harm. While specific policies are not necessarily required, addressing this issue as part of an overall incident response plan can be helpful for companies that face these issues.

§ 38:11 Blogging and social networking

The use of blogs and social networking sites, particularly as part of a company's communication strategy, raise a number of issues, and implicate many laws discussed in this book, including cyberdefamation, disclosure of confidential information, marketing laws, as well as liability for statements by employees to other employees, or third parties. Policies regarding the appropriate use of these types of communication vehicles, particularly if they are in some way sponsored by the company are good steps to try and limit liability and exposure of inappropriate information. If these resources are not officially part of a company's communication strategy, or otherwise officially sanctioned, raise issues of misuse of company networks and computer resources, in addition to those issues raised above, and companies should consider appropriate policies to restrict access to these type of services.

§ 38:12 Security breaches

Security breach laws are top of mind for many companies these days, and the closely-related security freeze laws also may need to be complied with. Companies should take steps to try and reduce the amount of data they collect so that the chance of a security breach is reduced. Moreover, if truly sensitive data is at issue some forms of monitoring may assist companies in preventing, or limiting security breaches. As more fully discussed in Chapter 25, there are a number of differing requirements under the now 44 state (plus New York City, Puerto Rico, and Washington D.C.) security breach laws and care should be taken to comply with these laws. Having an incident response plan in place will assist your company with gathering evidence of the breach and providing timely notice to individuals, as well as other relevant entities. The plan should identify other necessary documents that need to be prepared in case of a breach (such as FAQs), identify key personnel that need to be notified, including executives and other managing agents, as well as internal or external P.R. resources, if appropriate. Key members of IT, including any necessary outside forensic consultants, should also be identified.

§ 38:13 Security freeze laws

Security freeze laws permit a consumer to place a "freeze" on their consumer reports. While this places a number of burdens on the consumer reporting agencies, it also places obligations and restrictions on other businesses that obtain or use data from consumer reports. Policies to assist your business with these laws, even if you company is not a consumer reporting agencies, are a good idea that can greatly assist your company.

§ 38:14 Red flag regulations

While not effective as of the date of this book, the "red flag" regulations promulgated under the FACT Act also are notable for businesses because they effectively apply to any company that extends credit, and require monitoring of certain activity that can indicate identity theft as well as steps to reduce identity theft. Policies to implement these requirements are mandated by these regulations so businesses must address these issues sooner rather than later.

§ 38:15 Social Security numbers

Restrictions on the use and disclosure of Social Security numbers are also important to most companies. There are a number of states that prohibit the posting, display, or transmission in certain circumstances, of Social Security numbers, unless otherwise permitted or required by law. This is an important issue for many companies because Social Security numbers are often a critical piece of identifying information. However, they are also frequently the target of identity thieves. As such, companies should consider implementing policies that limit the use, collection, display, or transmission of Social Security numbers.

§ 38:16 Credit card receipt issues

The FACT Act's restrictions on the printing, and likely computer display, of credit card numbers on receipts (including the more restrictive state laws) also impact many companies. In 2009, new, more restrictive requirements go into effect in California, which include restrictions on the storage of credit card receipts with numbers on them, so while dedicated policies may not ultimately be necessary, actively monitoring for compliance is critical because there have been a number of lawsuits brought for the violation of these laws.

§ 38:17 Spyware, phishing and pharming

Many businesses suffer from issues related to spyware, phishing and pharming attacks. Businesses are sometimes targets of spyware attacks that seek to obtain personal information or other confidential information. Moreover, many companies have their logos or web code used improperly as part of phishing or pharming attacks. Policies related to intellectual property enforcement, particularly trademarks, can be implicated and prove helpful in phishing and pharming situations, and all of these issues, including spyware, can implicate a company's data security policy.

§ 38:18 Cloud computing

Cloud computing is a recently developed style of computing that uses the Internet to provide programs and resources. Because the resources are shared on the Internet, there are a number of privacy and data security concerns. While there are no laws that specifically address cloud computing, privacy and security laws discussed in this book are applicable and it is likely that new laws will be passed to cover this emerging area.

§ 38:19 Transfers in M&A, bankruptcy, and retroactive changes to privacy policies

In the merger and acquisition context, as well as if there is a potential bankruptcy of a company, making sure that transfers of information is permitted is something companies must be cognizant of. Having a privacy policy that contemplates these issues can be critical, particularly if the change is to be applied retroactively.

§ 38:20 Internet concerns

Doing business on the web opens a company up to a variety of issues that must be addressed. In addition to the issues identified previously regarding marketing, making sure your company does not collect more information than it needs via the web, as well as ensuring that any transfers of sensitive personal information are handled securely, are important. Moreover, concerns over the collection of date of birth are issues that companies must address even if they are not sites targeted to children 12 and under because merely collecting a data of birth can potentially make the company have to comply with certain portions of COPPA.

While not purely a privacy issue, the Communications Decency Act, can impact businesses both from blocking their ability to sue the "publisher" of a defamatory publication on the Internet, as well as potentially protecting them from liability for certain postings on their Internet pages. This is all the more true under the new guidance from the Ninth Circuit, discussed in Chapter 4.

Finally, the DMCA also can have privacy implications because content owners can request the disclosure of certain personally identifiable information to identify alleged infringers and companies should consider having policies in place to deal with these type of requests, as well as the removal of content if it is infringing, the limitation or elimination of access to the website or service for repeat offenders, and counter-designation policies for people who are accused of infringement and dispute the allegations.

§ 38:21 Public display of information

A number of states have restricted certain entities from publicly displaying personally identifiable information regarding law enforcement and other individuals, particularly if there is a threat of harm. These issues are generally discussed in Chapter 2, and an overview of the issue is included in § 2:32.

§ 38:22 Behavioral advertising

While the issue has recently come to light again, and will continue to grow in importance, behavioral, or targeted, advertising, is an issue that has broad implications for many companies. This type of advertising uses data about the consumer that is gathered by the company, or a third-party, to target certain advertisements to the consumer. This is an area where the FTC is actively engaged and is attempting to set best practices. Typically concerns center around notice and choice for consumers regarding their information. Setting standards and considering the type of linkage between advertisements and personally identifiable information, as well as limiting the broad dissemination of this type of information is something that companies must consider.

Internet companies that have a search engine function also have unique issues regarding the retention, processing, and disclosure at government request, of search engine data which in many cases is retained and used as part of behavioral advertising.

§ 38:23 Genetic privacy

With the arrival of GINA, genetic privacy has now arrived as a top of mind issue. While GINA has federalized a common standard, there are a number of state laws that are also relevant. Typically, these laws prohibit discrimination by employers or insurers based upon genetic information. There are also restrictions on the use of genetic testing of individuals, as well as their family members in certain cases. Civil remedies are typically available for the breach of these laws.

§ 38:24 Payment Card Industry standards

For any company that permits customers to use credit cards, PCI standards, which are set by the credit card companies, are a growing area of concern and the recent laws that have been enacted in certain states that impose liability on merchants that improperly retain certain credit card information is also a compliance hurdle. The PCI standards are quite detailed and compli-

ance is mandatory in most cases. Having the requisite policies in place is critical because failures in this regard can lead to identity theft, as well as the loss of the ability of the merchant to accept payment by credit card.

§ 38:25 Biometrics

The gathering and processing of biometric data is an issue that is becoming more of a concern. Many companies are starting to consider using biometric data as an identifier and one of the major drawback is that once it is compromised it cannot be changed. As a result, there have been some concerns about its use, as well as civil liberty issues raised over the use and processing of fingerprints. While specific policies are not necessarily required, they should be considered and the reduction or elimination of the collection of unnecessary biometric data should be considered. In certain cases, a numerical representation of the biometric data can be collected, which may reduce some of these issues.

§ 38:26 RFID/GPS

Radio Frequency Identification is a growing concern, as is the use of GPS systems. RFID and GPS can be used to track goods, as well as individuals, in certain cases. Cell phones all have GPS tracking built-in that can be monitored by the government in certain cases. Moreover, certain states require parolees to be monitored via GPS. This type of technology raises civil liberty concerns, particularly as the ability to track individuals is increasing, but it offers a significant advantage to business in that it permits increased monitoring and control of goods.

§ 38:27 International issues

As businesses become more global, concerns over the international transfer of information, particularly to the United States, are increasing and international privacy is a large compliance issue. Whether it is customer data, or data regarding your company's employees, many countries impose significant restrictions on the transfer and processing of data in the United States. Moreover, as noted in *Information Security and Privacy: A Guide to International Law and Compliance*, there are many conflicts with United States and international law, including with SOX, so managing compliance can be challenging. Moreover, when systems are implemented to share contact and other information regarding employees across borders, there can be significant risk and compliance issues. As discussed in *Information Security and Privacy: A Guide to International Law and Compliance*, many

companies are starting to opt to comply with the EU laws via Binding Corporate Rules, although Model Contracts and Safe Harbor also remain as available options. BCRs require extensive policies, as do the other two options for EU compliance, so care must be taken to ensure that all necessary policies and training are implemented.

Moreover, differences about the definition of what is personally identifiable information, particularly the brewing debate over whether IP Addresses are personally identifiable in the EU, is also an issue that companies must address.

§ 38:28 SOX

For publicly-traded companies, the internal controls requirements of Sarbanes-Oxley, as well as Rule 404, are privacy and data security concerns. If there is no data security regarding the company's sensitive data, particularly financial data, in many cases the company may lack internal controls. As noted above, whistleblower requirements can conflict with EU laws, so finding the correct compliance path can be challenging.

§ 38:29 Responding to government requests

Compliance with the Patriot Act, as well as the Foreign Intelligence Surveillance Act, including responding to National Security Letters, is a less common, though important issue. Having the appropriate policies in place to ensure compliance with these requests is critical for companies, particularly those, such as telecom companies and ISPs, that receive a number of these type of requests.

§ 38:30 Application of consumer reporting agency laws

One issue that has received some legislative attention is regulation of consumer reports. These laws are typically use-based restrictions and the laws typically only apply to certain types of entities—consumer reporting agencies. While there are 3 clearly recognized consumer reporting agencies that maintain files on a nationwide basis regarding consumers, many of these laws, particularly at the state level, sweep many other companies into their definition of a consumer reporting agency. As a result, companies other than the "Big 3" need to consider whether they are regulated by these laws. A selection of these laws is discussed in Chapter 17.

§ 38:31 Employment applications

While the Fair Credit Reporting Act, and the state analogues,

are focused on financial issues, many other forms of conduct are regulated by these laws, including employers' use of information in connection with hiring, or firing employees. These laws are discussed in Chapters 16 and 17.

§ 38:32 Industry specific concerns—Energy companies

Energy companies face some unique privacy and security issues. In many cases there are additional privacy burdens imposed on utilities in state Public Utility Codes. There are also restrictions regarding the denial of credit to victims of identity theft in certain circumstances. Moreover, given the unique physical security issues that many companies face given this central nature of this industry to the American economy, there is a different level of balancing of privacy interests that may result in more extensive security clearance and background checks, as well as restrictions on offshoring certain data. In addition to increased physical security, in many cases increased technical and administrative security are also common, particularly if there are nuclear plants involved. Also, the Red Flag regulations are important to note as well.

§ 38:33 Industry specific concerns—Financial institutions

Financial institutions are subject to a number of special requirements under state and federal law, including GLB, FCRA, and state financial privacy laws, as well as lending laws that can have privacy and information security implications. A complete discussion of these additional requirements, including the requisite policies, is contained in the relevant chapters, but common issues include concerns over affiliate sharing, making sure all required notices under these statutes, particularly GLB, are given, and information security. Pretexting is also a concern for financial institutions and it is specifically regulated under GLB, as is compliance with the Bank Secrecy Act.

§ 38:34 Industry specific concerns—Hospitals and medical providers

HIPAA is one of the more well known privacy laws, though it was not truly intended as a privacy law. Covered entities must comply with HIPAA, as well as more restrictive state law in certain cases, regarding the disclosure of PHI, or Protected Health Information. Privacy and security policies are required to comply with HIPAA, as are audits, assessments, training, and other requirements. Health care providers also must comply with infectious disease laws, which in some cases prohibit, mandate or

permit disclosures, as well as restrictions on the storage, retention, and destruction of medical records. Moreover, entities that are not covered by HIPAA, as well as those that are, are also subject to medical marketing laws, and certain states have enacted restrictions on the disclosure of physician's prescription history.

Genetic privacy, including how information used for research regarding the human genome can be processed, are also concerns for health care, and related, entities.

§ 38:35 Industry specific concerns—Government employers

Government employers face unique disclosure and privacy issues. In many cases, government employers are subject to FOIA, or similar public records requests, so they may be under broad disclosure obligations. However, they are also subject in many cases to Fourth Amendment warrant requirements before they search an employee's computer, depending on the circumstances of the search and seizure. There are also restrictions upon the posting of certain information regarding government employees by others that are important to note.

§ 38:36 Industry specific concerns—Social Networking sites

Social networking sites are at the forefront of many privacy issues. They face many issues that all companies face, but must address them in unique ways, because the very purpose of the service is to share personal information, including information that can be very sensitive. Concerns over the DMCA, the CDA, behavioral advertising, government requests for information, as well as many other issues must be addressed. Balancing the need for disclosure on the sites, with user's privacy expectations, is often the most difficult issue to address.

§ 38:37 Industry specific concerns—The airline industry

Given the unique physical security issues faced by the airline industry, there are unique privacy concerns, and a different balancing of expectations of privacy. Airlines are much freer to search individual's personal belongings, and airports obviously serve in many cases as the site of a border search, though this is not done by the airlines themselves. Disclosures under FISA and the Patriot Act are common concerns, as is the related and ongoing debate with the EU over the disclosure of Passenger Name Records, or PNRs.

§ 38:38 Industry specific concerns—Retail issues

Retailers face a number of privacy issues, which in part arise from their collection of information consumer buying patterns, as well as collection of payment information. PCI compliance and other issues regarding credit card information (including credit card receipt laws) are common concerns, but these are just the beginning. Data destruction is a common issue, and behavioral advertising is becoming a larger issue for retailers, as shown by the recent FTC enforcement action against Sears. The Red Flags Rule also can impact retailers and many other laws can raise compliance hurdles.

§ 38:39 Industry specific concerns—Telecom

Telecom companies face a number of issues, both as ISPs, as well as telephone providers. Pretexting, NSLs, Patriot Act compliance, as well as disclosure to the government of other information, including under the ECPA and Pen Register laws are also common concerns. Subpoenas in civil litigation that seek to identify users who have engaged in misconduct are also common issues that must be addressed by telecom companies, including under the DMCA. There are also Public Utilities Code restrictions on telecom providers regarding the disclosure of certain forms of information. Cellular providers face similar issues in different contexts, including the disclosure of SMS content, but they are subject to some different requirements.

§ 38:40 Industry specific concerns—Insurance companies

Insurance companies must comply with many of the financial privacy laws, to the extent they are covered by them, but they must also comply with state insurance privacy laws. They also face issues similar to those faced by financial institutions regarding security of information under many of these laws, or the general information security laws, given the sensitivity of this information. Medical privacy laws can be implicated in certain circumstances, depending upon the nature of the information contained in the insured's file, as well as the source of the information.

§ 38:41 Industry specific concerns—Publishers

Publishers, particularly those on the Internet, frequently face issues about the disclosure of anonymous posters, as well as First Amendment concerns over the reporter's right to keep the identity of their sources private. The publisher may in many cases set a

policy to determine if, or when, it will disclose these types of information.

§ 38:42 Industry specific concerns—Cable and video companies

Cable and video companies are subject to particular privacy requirements that prohibit the disclosure of subscriber information. As DVRs become more common, questions regarding the disclosure of information gathered from these devices will be raised, including whether this information is covered under existing law. A related issue is what standards apply to cable providers when they are providing ISP services, and are not simply providing cable service only and there is a conflict in the law on this point. Cable companies and video companies face a number of issues that are similar to telecom companies, including managing government requests for information.