Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

EYE ON PRIVACY

NOVEMBER 2012

Welcome

As the dust settles from last week's election, privacy and data security issues remain as important as ever. Expect to see the Obama administration and the FTC continue their respective pushes for increased regulatory oversight. In the near term, leadership changes at the FTC may result in an increase in privacy and data security enforcement actions. And as Congress returns to work, expect the bipartisan issue of privacy legislation to gain traction again.

Meanwhile, in Europe, our privacy and data security experts in Brussels have prepared WSGR's EU Data Protection Regulation Observatory, available at http://www.wsgr.com/eudataregulation/. This website is designed to track developments related to the EU legislative proposal for a General Data Protection Regulation, which will affect all companies doing business in Europe. We'll continue to keep an eye on these and other privacy developments and report back with the highlights.

In this year's final issue of *Eye on Privacy*, we provide insight into data breach notification requirements in the EU, address two of the FTC's recent $1 million-plus privacy settlements, analyze California's new law prohibiting employers from demanding social media passwords, and summarize a recent privacy class action dismissal in Michigan involving the online music-streaming service Pandora. If there are other topics you'd like to see us cover in future editions, please let us know at PrivacyAlerts@wsgr.com. See you next year!

Lydia Parnes
Partner, Washington, DC
lparnes@wsgr.com

European Data Protection Law: Breach Notification Requirements – A Global Approach

Christopher Kuner
Senior Of Counsel, Brussels
ckuner@wsgr.com

Anna Pateraki
Associate, Brussels
apateraki@wsgr.com

Cyber attacks, hacked passwords, compromised credit card information, and data thefts—in recent years, data breaches have become commonplace. Under data protection law, data breaches may have to be reported to regulators, who then will decide whether action against a company should be taken, and potentially to individuals as well. Due to the global nature of the Internet and the evolving digital environment, data breaches may not be limited to one country and the same incident may trigger notification requirements in a variety of countries. For example, a breach related to a database located in the United States that also is distributed among different European Union (EU) countries or that may otherwise concern the data of EU citizens might trigger notification requirements in the EU.

Europe is not one country, however. It is comprised of 27 sovereign countries and different national laws, and therefore the question of whether, when, and under what conditions notification is required can be answered only on a case-by-case basis. Multinational companies expanding their businesses in Europe are worried about EU breach notification requirements and potential action by EU regulators. The high-level overview of the EU data breach notification regime given below explains why a global approach is the most effective

Continued on page 2...

In This Issue

way of addressing complex data breaches with transatlantic dimensions.

General Data Breach Rules

In the EU, the breach notification regime has two dimensions. One concerns notifying the relevant regulator with jurisdiction over the breach, and the other concerns notifying the affected individuals. The term "data breach" is broadly construed and can include any breach of security that may lead to the accidental or unauthorized access, disclosure, or alteration of personal data. Currently, there is a general (rather than sector-specific) legal requirement to provide notification of data breaches only in a few European countries. For example, a legal obligation to notify regulators and affected individuals (under certain circumstances) of data breaches exists in Germany and Norway. In contrast, some countries, such as Austria, have a legal requirement to notify individuals but not the regulator, whereas other countries have a voluntary regime based on codes and guidelines issued by regulators, such as Denmark, Ireland, and the United Kingdom.

Generally speaking, specific thresholds may apply as to the triggers (e.g., types of data, assessment of harm), timing, scope, and addresses of the notification. Additional requirements may apply depending on the type of the breach and the affected country. For example, in some countries, national laws may require the involvement of the works councils for data breaches affecting HR data. Therefore, it is necessary to examine the individual situation in each affected country before reaching a conclusion as to whether it is legally required to notify data breaches in the EU and on what terms. However, as explained further below, the absence of a legislative requirement to notify in all countries should not preclude a general EU-wide notification in a particular case.

Sector-Specific Security Breaches (E-Privacy)

In the EU, there is a sector-specific requirement for telecom providers and Internet service providers (ISPs) to notify regulators and adversely affected individuals of all security breaches. This requirement is based on the E-Privacy Directive that EU countries are required to implement into their national laws. A security breach is broadly construed and may include any fault in servers, networks, and other electronic communication systems having an impact on subscribers' data. Depending on the nature of the breach, notification of regulators must include remedial steps to address the breach. However, notification of individuals may not be required if the provider demonstrates sufficiently to the regulator that it had taken steps to comply with data security requirements prior to occurrence of the breach. More country-specific requirements may be provided by national laws and guidelines of regulators.

Draft Data Protection Regulation

The Draft EU General Data Protection Regulation (Draft Regulation) is draft EU legislation that introduces a mandatory general data breach notification regime that likely will become law in a few years and will apply throughout Europe. The Draft Regulation is currently in the legislative process, and therefore the current status of the relevant provisions may be subject to change. The general breach notification regime contained in the proposal is generally endorsed by regulators and advisory bodies in Europe, which reflects the current trend in the EU for transparency with regard to data breaches. EU regulators traditionally communicate with each other and exchange views, and the Draft Regulation explicitly requires that they communicate among themselves in carrying out enforcement actions. This means that European regulators will usually be able to find out about data breaches in other countries and take action separately or jointly depending on the case. Consequently, multinational companies should develop a strategy for addressing data breaches that affect different EU countries.

Tips for Multinational Companies – A Global Approach

Although the EU legal landscape is not harmonized and most European countries currently do not have a mandatory notification regime for general data breaches (i.e., other than those applicable to telecom providers and ISPs), European regulators may take action if they were not notified but they learn about a breach through the press or following a complaint or investigation. If a data breach is (or has to be) notified by a company in the U.S., it should probably be notified in the EU as well to avoid the possibility that EU regulators may take action against the company if they find out about the breach. If a data breach is notified in the EU, it likely will have to be notified in more than one of the affected countries and not only where an explicit legal requirement applies.

This approach likely will become the rule in a few years when the Draft Regulation becomes effective. In the interim, many EU countries are considering introducing general breach notification regimes applicable to all business sectors, and companies tend to proactively notify regulators of data breaches as an indication of goodwill and cooperation. However, the specifics of the particular case should be taken into account, and any conclusion as to whether notification is required and how it should take place should be based on an appropriate evaluation of the facts and the risks for the affected individuals.

For more information about the Draft Regulation, please visit our new WSGR EU Data Protection Regulation Observatory, available at http://www.wsgr.com/eudataregulation/.

FTC Announces $1 Million Penalty for Children's Privacy Violations by Fan-Club Website Operator

Matthew Staples
Associate, Seattle
mstaples@wsgr.com

Sharon Lee
Associate, Palo Alto
shlee@wsgr.com

On October 4, 2012, the Federal Trade Commission (FTC) announced the settlement of a case it had filed the previous day against Artist Arena, an operator of fan websites for music stars, alleging violations of the FTC's Children's Online Privacy Protection Rule (the COPPA Rule),[1] which implements the Children's Online Privacy Protection Act (COPPA).[2] The COPPA Rule regulates the online collection of personal information from children under 13 years of age, as well as the use and disclosure of such information. It applies to the operators of commercial websites and online services that are directed to children or that collect children's personal information with actual knowledge, and requires such operators to meet specific requirements prior to collecting online, using, or disclosing personal information from children. For example, such operators may not collect, use, or disclose children's personal information without giving direct notice of their information practices to parents and obtaining verifiable parental consent from them.[3]

The FTC alleged, among other things, that children were able to register online to join a fan club, create online profiles, post on the walls of other website members, and subscribe to fan newsletters on websites operated by Artist Arena (such as www.RihannaNow.com, www.DemiLovatoFanClub.net, www.BieberFever.com, and www.SelenaGomez.com) without the sites providing parental notice or obtaining verifiable parental consent.[4] According to the FTC, Artist Arena falsely stated that it would neither collect children's personal information nor activate a child's online registration without parental consent. The complaint further specified that Artist Arena knowingly registered more than 25,000 children and collected personal information from nearly 75,000 more children who had begun but did not complete registration.

The FTC's complaint alleged that Artist Arena violated the COPPA Rule by failing to provide notice to parents of its information practices and failing to obtain verifiable parental consent before collecting, using, and disclosing personal information from children online.

Settlement

Artist Arena agreed in the settlement to several different remedies, including requirements to pay a $1 million civil penalty, delete the children's personal information that it collected in violation of COPPA, and abstain from committing future COPPA violations. The settlement also requires Artist Arena to provide clear and conspicuous notice of the child online privacy website www.onguardonline.gov in its privacy policy, in its information practices notice sent to parents, and at each location on any of its websites or online services where personal information is collected.[5]

Implications

The Artist Arena settlement illustrates the importance to operators of websites and online services that are directed at children or that have actual knowledge of their online collection of children's personal information of complying with the COPPA Rule, as well as not misrepresenting COPPA compliance efforts. Children's privacy continues to be a point of emphasis for the FTC, and the penalties for failure to comply with COPPA can be significant. This is demonstrated not only by the $1 million civil penalty agreed to by Artist Arena, but also by several other significant civil penalties agreed to by entities that have entered into COPPA-related settlements with the FTC.[6]

Additionally, as covered previously in *Eye on Privacy*, the FTC presently is in the process of updating the COPPA Rule and has proposed two sets of modifications.[7] Final modifications to the COPPA Rule are anticipated soon, and operators of websites and online services directed to children, or that have actual knowledge of collecting personal information online from children, will need to evaluate their practices with respect to children when the final modifications are released.

---

[1] 16 CFR Part 312.
[2] 15 U.S.C. §§ 6501-6506.
[3] *See* 16 CFR §§ 312.4 and 312.5.
[4] For information from the FTC regarding the settlement, please see http://www.ftc.gov/opa/2012/10/artistarena.shtm.
[5] *See* http://www.ftc.gov/os/caselist/1123167/121003artistarenadecree.pdf.
[6] For example, Playdom, an operator of online virtual worlds, agreed to a $3 million settlement in 2011. *See* http://www.ftc.gov/opa/2011/05/playdom.shtm.
[7] For our coverage of the FTC's proposed COPPA Rule modifications, please see our WSGR Alert regarding the FTC's initial proposed modifications at http://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/pdfsearch/wsgralert-childrens-online-privacy-protection.htm, as well as our coverage of the FTC's additional proposed revisions in our September 2012 issue of *Eye on Privacy* at http://www.wsgr.com/publications/PDFSearch/eye-on-privacy/Sep2012/index.html#5.

Tip Improving security is one of the simplest ways to enhance privacy.

Company That Purchased and Sold Sensitive Consumer Data Agrees to $1.2 Million Settlement with FTC

Tonia Klausner
Partner, New York
tklausner@wsgr.com

Jason Mollick
Associate, New York
jmollick@wsgr.com

As part of its ongoing efforts to address consumer privacy, the Federal Trade Commission (FTC) announced[1] on October 10, 2012, that credit reporting agency Equifax Information Services LLC and data marketer Direct Lending Source, Inc., have agreed to collectively pay approximately $1.6 million to settle alleged violations of the Fair Credit Reporting Act (FCRA), with the marketing company and its principals responsible for $1.2 million.[2] The settlement arises out of allegations that Direct Lending purchased consumer data regarding mortgage payments from Equifax and resold it to third parties who used it to market debt-reduction and other products aimed at financially distressed consumers. The settlements reflect not only the FTC's continued strong enforcement of the FCRA, but also its view that marketing to consumers based on sensitive information such as financial data implicates consumer privacy concerns and will be closely scrutinized.

Use and Sale of Consumer Reports under the Fair Credit Reporting Act

The FCRA imposes various duties and restrictions on consumer reporting agencies and users of "consumer reports." The FCRA defines a "consumer report" as any communication of information by a consumer reporting agency bearing on a consumer's credit worthiness, "which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for" credit or personal insurance, employment purposes, or any other purpose authorized by the statute.[3] The act prohibits any person from obtaining or using a consumer report for any purpose other than specified "permissible purposes," and bars consumer reporting agencies from furnishing such reports unless they have reason to believe that the purchaser has a specified permissible purpose for the information.[4] In addition, anyone who furnishes consumer reports—either as a consumer reporting agency or through resale to third parties—must maintain "reasonable procedures" to ensure that the reports are used by recipients only for a specified permissible purpose. End users must be required to identify themselves, certify the precise purpose for which the information is being sought, and certify that the information will be used for no other purpose. Prior to sale, the distributor must take "reasonable efforts" to verify these required identifications and certifications.[5] Resellers are further obligated to disclose the identity and certified permissible purpose of each ultimate end user to the consumer reporting agency that originally furnished the data.[6] Any violation of these and other requirements under the FCRA constitutes an "unfair or deceptive act or practice" in violation of Section 5(a) of the Federal Trade Commission Act.[7]

The FTC's Complaints

The FTC brought an administrative complaint against Equifax[8] and a judicial complaint against Direct Lending in the Southern District of California.[9] The FTC alleged that from January 2008 to early 2010, Equifax sold more than 17,000 "prescreened lists" of consumers to Direct Lending and its affiliates. These lists contained, among other things, the names of consumers who were 30, 60, or 90 days delinquent on their mortgage payments. According to the FTC, such lists are "consumer reports" under the FCRA, and their only permissible use in connection with credit transactions is to make a "firm offer of credit or insurance" to the consumer.[10] The use of prescreened lists to send general marketing solicitations is *not* a permissible purpose, said the FTC.

According to the complaints, the prescreened lists were used and resold to third parties by Direct Lending for the impermissible purpose of soliciting services to persons in financial distress such as loan modification, debt relief, and foreclosure relief. Notably, many of the companies that purchased the prescreened lists from Direct Lending were the subject of separate law enforcement actions based on allegations that the products they sold to consumers were bogus.

The FTC alleged that Equifax violated the FCRA by selling the prescreened lists to Direct Lending, because Direct Lending did not have a permissible use for the data. The FTC alleged that Direct Lending violated the FCRA by obtaining the prescreened lists without a permissible purpose and reselling that information to end users who further misused the data. In addition, the FTC alleged that both Equifax and Direct Lending failed to maintain reasonable procedures and efforts to ensure that the lists would be used only in connection with permissible purposes.

---

[1] FTC News Release, "FTC Settlements Require Equifax to Forfeit Money Made by Allegedly Improperly Selling Information about Millions of Consumers Who Were Late on Their Mortgages," Oct. 10, 2012, *available at* http://www.ftc.gov/opa/2012/10/equifaxdirect.shtm.
[2] 15 U.S.C. § 1681 et seq.
[3] FCRA § 603(d).
[4] *Id.* at § 604(a), (f).
[5] *Id.* at § 607(a), (e).
[6] *Id.* at § 607(e).
[7] *Id.* at § 621(a).
[8] Draft Complaint, *In the Matter of Equifax Info. Servs. LLC*, FTC File No. 102-3252, *available at* http://www.ftc.gov/os/caselist/1023252/121010equifaxcmpt.pdf.
[9] Complaint, *U.S. v. Direct Lending Source, Inc.*, No. 12-cv-2441 (DMS) (BLM) (S.D. Cal. Oct. 9, 2012), *available at* http://www.ftc.gov/os/caselist/1023000/121010directlendingcmpt.pdf.
[10] *Id.* at § 604(c); *see also id.* at § 604(l) (defining a "firm offer of credit or insurance" as, generally, "any offer of credit or insurance to a consumer that will be honored if the consumer is determined, based on information in a consumer report on the consumer, to meet the specific criteria used to select the consumer for the offer").

Continued on page 5...

Company That Purchased and Sold . . . *(continued from page 4)*

Settlements

The parties, without admitting any of the allegations in the complaints, have agreed to pay a total of approximately $1.6 million in fines and civil penalties to settle these matters—Equifax agreed to pay roughly $393,000[11] and Direct Lending agreed to pay $1.2 million, secured by the property of its principals.[12] In addition, the parties are prohibited from failing to comply with the FCRA in the future, and are barred from furnishing, using, or selling consumer reports in connection with solicitations for debt-relief or mortgage-assistance products and services offered by entities charging advance fees.[13] Both parties are also subject to certain compliance reporting and recordkeeping obligations, particularly Direct Lending, which must, among other things, maintain highly detailed compliance records for the next 20 years.

Implications

These settlements are yet another reminder to buyers and sellers of consumer data of the increasing government scrutiny of the use of sensitive consumer data for marketing purposes. Data marketers should be particularly mindful of the FTC's concerns when targeting marketing campaigns based on financial information about consumers. The FTC has taken a broad view of the definition of a "consumer report" under the FCRA, and has shown a willingness to take aggressive enforcement action, particularly where it appears that consumers have been harmed by the ultimate users of the data.

[11] Agreement Containing Consent Order, *In the Matter of Equifax Info. Servs. LLC*, FTC File No. 102-3252, *available at* http://www.ftc.gov/os/caselist/1023252/121010equifaxagree.pdf.
[12] Stipulated Final Judgment and Order, *U.S. v. Direct Lending Source, Inc.*, No. 12-cv-2441 (DMS) (BLM) (S.D. Cal. Oct. 11, 2012), *available at* http://www.ftc.gov/os/caselist/1023000/121010directlendingstip.pdf.
[13] Subject to limited exceptions as applied to Equifax.

California Law Prohibits Employers from Demanding Social Media Passwords from Employees and Applicants with Limited Exceptions

Fred Alvarez
Partner, Palo Alto
falvarez@wsgr.com

Ulrico Rosales
Partner, Palo Alto
urosales@wsgr.com

Rebecca Stuart
Associate, Palo Alto
rstuart@wsgr.com

Last month, California became the third (and largest) state to regulate employer access to the social media accounts of applicants and employees. The law, A.B. 1844—which takes effect on January 1, 2013—is intended to protect California employees and applicants from "unwarranted invasions of their personal social media accounts." However, it contains many undefined and unclear provisions that create potential landmines for California employers.

A.B. 1844 was passed against a backdrop of renewed legislative interest in some employers' practice of asking their employees and applicants to divulge social media passwords, permitting employers to review social media profiles for suspicious or inappropriate activity. The media, advocacy groups, legislators, and the general public have refocused attention on the subject—an area that implicates individual privacy rights and the limits of an employer's ability to access the social media information of its current and prospective employees. Before California's passage of A.B. 1844, both Maryland[1] and Illinois[2] passed similar laws regulating employer access to applicant and employee social media account information.

The recent increase in interest can be traced partially to a 2010 incident in which the Maryland Division of Corrections demanded Facebook log-in credentials from a corrections officer, Robert Collins, following his return from leave.[3] Mr. Collins was not, however, the first employee subjected to such a request by a government agency; job applicants in Montana and Illinois similarly have been required to provide social media log-in information for jobs at places including a sheriff's office and a school district.[4]

Earlier this year, Facebook issued a statement condemning the practice of requesting social

[1] S.B. 433 and H.B. 964.
[2] H.B. 3782.
[3] Emil Protalinski, "Employer Demands Facebook Login Credentials During Interview," ZDNet.com, Feb. 20, 2011, *available at* http://www.zdnet.com/blog/facebook/employer-demands-facebook-login-credentials-during-interview/327?tag=mantle_skin;content; Manuel Valdez, "Job Seekers Getting Asked for Facebook Passwords," Time.com, March 20, 2012, *available at* http://techland.time.com/2012/03/20/job-seekers-getting-asked-for-facebook-passwords/.
[4] Manuel Valdez, "Job Seekers Getting Asked for Facebook Passwords," Time.com, March 20, 2012, *available at* http://techland.time.com/2012/03/20/job-seekers-getting-asked-for-facebook-passwords/.

Continued on page 6...

media log-in information from job applicants, stating in part, "This practice undermines the privacy expectations and the security of both the user and the user's friends. It also potentially exposes the employer who seeks this access to unanticipated legal liability."[5] In addition, Facebook has made it a violation of the company's Statement of Rights and Responsibilities to share or solicit a Facebook password. In line with this cautionary note from Facebook, many employer attorneys have counseled against this practice. Nonetheless, the California legislature has decided to create a legislative "solution" to a problem that may not have been widespread in California to begin with.

California's A.B. 1844 prohibits an employer from requiring or requesting that an employee or applicant for employment do any of the following: (1) disclose a username or password for the purpose of accessing personal social media; (2) access personal social media in the presence of the employer; or (3) divulge any personal social media information, except as provided for in the bill.[6] The law clarifies that employers' *existing* rights and obligations to request personal social media information remain intact *if* that information is reasonably believed to be relevant to an investigation of allegations of employee misconduct or an employee's violation of applicable laws and regulations, and only *if* the social media is used *solely* for the purposes of that investigation or a related proceeding.[7] A.B. 1844 does allow employers to require or request a username, password, or other method of accessing an employer-issued electronic device.[8] The law also prohibits any discharge, discipline, threat to discharge or discipline, or other retaliation against an employee who fails to provide information requested in violation of the law.[9]

Despite the California legislature's attempt to resolve the problem of employers indiscriminately asking for social media credentials, California's new law creates many potential pitfalls for employers, including the following:

1. "Bring Your Own Device" Policies. A.B. 1844 specifically allows employers to require or request that an employee disclose a username, password, or other information for the purpose of accessing an *employer-issued electronic device*. However, the line between an employer-issued device and a personal device connected to the employer's information systems is becoming blurred. Indeed, many companies have enacted so-called "bring your own device" (BYOD) policies that enable employees to use personal devices for professional purposes as a company policy. In addition, employers often permit their employees to use their own electronic devices to connect to company networks or other electronic systems. It is not unusual, for example, for an employee to use his or her smartphone to access work email or other network services. Depending on what constitutes an "employer-issued" device under A.B. 1844, employers may not have access to those personal devices. This ambiguity could be especially problematic if, for example, an employer is required to comply with a "litigation hold" or a discovery request in litigation, but is not able to retrieve or preserve the necessary information.

2. Investigation of Employee Misconduct/Violation of Applicable Laws. A.B. 1844 allows an employer to require or request social media credentials if it reasonably believes them to be relevant to an investigation of employee misconduct or an employee's violation of applicable laws and regulations, but only if the social media is used solely for the purposes of that investigation or a related proceeding. The statute's language is not clear as to who can be asked for social media credentials, whose social media can be reviewed, and what relation that social media use must have to an investigation in order to meet the requirements of the law. For example, if an employer investigates allegations of trade-secret theft, fraud, or sexual harassment by Employee A, can the employer ask Employee B for Employee B's social media credentials to monitor or review Employee A's online behavior? Or is the employer limited to asking Employee A for Employee A's credentials? Additionally, this exception for the use of social media is limited to only two types of investigations: (1) employee misconduct and (2) employee violation of an applicable law or regulation. One can imagine other scenarios in which an employer might wish to review employee social media for reasons that may not rise to the level of these exceptions, including insubordination or even poor performance. Seeking social media credentials for such uses, however, likely is complicated by California's law.

3. Incongruity of Defined Terms. A.B. 1844 defines "social media" as "an electronic service or account, or electronic content, including, but not limited to, videos, still photographs, blogs, video blogs, podcasts, instant and text messages, email, online services or accounts, or Internet Web site profiles or locations." Essentially, any online activity—including email—is considered social media for the purposes of the statute. However, the statute does *not* define "*personal* social media," which is the type of social media protected throughout the statute. Consequently, employers are left somewhat in the dark as to what is restricted by the prohibitions on requiring an applicant or

[5] "Protecting Your Passwords and Your Privacy," Erin Egan, Chief Privacy Officer, Facebook, found on the "Facebook and Privacy" page at http://newsroom.fb.com/Announcements/Protecting-Your-Passwords-and-Your-Privacy-134.aspx.
[6] A.B. 1844(b).
[7] A.B. 1844(c).
[8] A.B. 1844(d).
[9] A.B. 1844(e).

Continued on page 7...

employee to "access personal social media in the presence of the employer" or "divulge any personal social media," except as otherwise provided in the statute. The legislation also leaves unanswered what "personal" means when social media blends into the increasingly popular forms of web-based, business-related networking. For example, recently an employer had to defend its action to take control of a social media account that the company claimed it owned from a terminated employee who had used the social media account as her own.[10] Such cases underscore the need for clear, written policies establishing ownership of such business-related social media accounts, and they also indicate that the ambiguity created by California's new law could have very real consequences.

Conclusion

What is clear following California's passage of A.B. 1844 is that the social media landscape continues to evolve in the employment context. Competing interests exist. Employers often wish to inspect and monitor social media activity as it relates to matters affecting the workplace. Employees, on the other hand, have certain reasonable expectations of privacy and do not believe an employer may encroach on territory deemed personal. The National Labor Relations Board's recent activity and ruling regarding social media policies speaks to yet other interests at play (e.g., those interested in preserving concerted activity) with respect to the use of social media in the workplace. California's statute demonstrates that states are not waiting for employers or the federal government to act with respect to the practice of requesting social media credentials from applicants and employees. Employers therefore must act cautiously and prudently as they address the increasing number of social media issues arising in the workplace, especially with respect to policies and practices dealing with social media use.

[10] *Eagle v. Morgan*, No.: 11-4303 (E.D. Pa. filed Oct. 4, 2012).

Court Dismisses Michigan Class Action Claims Alleging Pandora Improperly Disclosed Profile Information and Musical Preferences

Wendell Bartnick
Associate, Washington, DC
wbartnick@wsgr.com

Gary Greenstein
Of Counsel, Washington, DC
ggreenstein@wsgr.com

The U.S. District Court for the Northern District of California recently concluded that providing a free streaming audio service is not the same as selling, renting, or lending songs. Accordingly, the court dismissed a class action lawsuit against Pandora Media, Inc., finding that a Michigan law prohibiting certain data disclosures by companies that sell, rent, or lend songs was inapplicable to Pandora.

The class action plaintiffs—comprised of Michigan users of Pandora's streaming audio service—alleged two missteps by Pandora. First, the plaintiffs alleged that Pandora made user profile information public despite its privacy policy. Second, the plaintiffs alleged that Pandora unilaterally shared their listening records with their Facebook friends.

These actions, according to the plaintiffs, violated two Michigan laws. The first, Michigan's Video Rental Privacy Act (VRPA), prohibits businesses that sell, rent, or lend sound recordings from disclosing records or information regarding such purchasing, leasing, renting, or borrowing in a way that would identify the consumer. The second, Michigan's Consumer Protection Act (MCPA), makes "unfair, unconscionable, or deceptive methods, acts, or practices in the conduct of trade or commerce . . . unlawful."

On September 27, 2012, the court granted Pandora's motion to dismiss. While the court dismissed the case with leave to amend, the plaintiffs declined to file an amended complaint. The case is now set up for possible review by the Ninth Circuit, should the plaintiffs appeal.

Video Rental Privacy Act

The VRPA applies only to businesses that sell, rent, or lend sound recordings. The court agreed with Pandora that the VRPA does not apply to Pandora's service because Pandora's streaming service does not consist of renting, lending, or selling sound recordings.

Pandora Did Not Rent Songs. First, the court found that Pandora did not rent sound recordings. To rent a sound recording, Pandora would need to receive payment and

Continued on page 8...

the user would need to use the sound recordings. The court noted that the plaintiffs did not pay Pandora for the audio service. Moreover, the plaintiffs did not use the sound recordings, because Pandora selected the songs, placed the temporary files on the user's computer, and deleted the files when the songs were done playing. Finally, the court reviewed Pandora's Terms of Use, which states that users shall not "copy, store, edit, change, prepare any derivative work of or alter in any way any of the tracks streamed through the Pandora Services." Therefore, under the terms, users may only listen to the sound recordings and cannot manipulate the files in any way. For all of these reasons, according to the court, Pandora does not rent songs when it streams them to users.

Pandora Did Not Lend Songs. Second, the court found that Pandora did not lend sound recordings. To lend a sound recording, the court stated, Pandora would need to allow the temporary use of the recording on the condition that it would be returned. Here again, the plaintiffs did not use the sound recordings because Pandora took all the actions. Moreover, since Pandora deleted the sound recordings, the plaintiffs could not have returned the sound recordings to Pandora. Therefore, Pandora did not lend the sound recordings.

Pandora Did Not Sell Songs. Third, the court found that Pandora did not sell sound recordings. The plaintiffs can use a link provided by Pandora to visit music sellers to purchase music; however, any such sale is between the plaintiffs and the third parties. In addition, none of the information allegedly disclosed by Pandora included details about song purchases from these third parties.

Pandora's Public Performance Rights Do Not Allow Renting, Lending, or Selling. For Pandora to stream music in compliance with federal copyright law, it has obtained a statutory license to the public performance of the music. Under this license, Pandora may only transmit the sound recording—it does not have the right to distribute copies of the sound recording. Because Pandora does not have the right to distribute copies of the sound recording, by definition, it cannot rent, lend, or sell the sound recording. Pandora's Terms of Use is consistent with these rights, as it only grants users a limited license to listen to the music.

Consumer Protection Act

Under the MCPA, plaintiffs in a class action lawsuit must allege that they have suffered a loss. The plaintiffs admitted that they did not allege harm, and the court dismissed the claim without reviewing whether Pandora's actions actually caused any harm.

Implications

The Pandora case highlights the interaction between state consumer protection laws, federal copyright law, a company's Terms of Use, and the technical details of how a service works. Companies that provide Internet services may benefit by ensuring that their terms of use documents are accurate and up to date. In this case, the court found that Pandora's Terms of Use only granted certain licensing rights to its users, which foreclosed claims under the VRPA.

Moreover, decision-makers and attorneys who understand the technical components of a business's service can make better decisions when drafting terms of use documents and considering business risk. For example, in this case, Pandora's control over its streaming music service placed Pandora under a different set of applicable laws than would have been the case if Pandora had allowed users to self-select songs or actually download and manipulate song files.

For interactive, on-demand streaming services, however, where end users may rent access to sound recordings during the term of the end user's subscription to the service, laws similar to the VRPA may apply. Thus, for example, the sharing of an end user's listening information on a subscription service on Facebook without permission may give rise to liability.

Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

650 Page Mill Road, Palo Alto, California 94304-1050 | Phone 650-493-9300 | Fax 650-493-6811 | www.wsgr.com

Austin Brussels Georgetown, DE Hong Kong New York Palo Alto San Diego San Francisco Seattle Shanghai Washington, DC