Volume 5, Issue 1, January/February 2014

SOCIALLY AWARE

THE SOCIAL MEDIA LAW UPDATE

THE BURTON AWARDS FOR THE PURSUIT OF PERFECTION
2011 BEST LAW FIRM NEWSLETTER

IN THIS ISSUE

EDITORS

John F. Delaney
Gabriel E. Meister
Aaron P. Rubin

CONTRIBUTORS

John F. Delaney
Adam J. Fleisher
D. Reed Freeman Jr.
Matthew W. Janiga
Christine E. Lyon
Gabriel E. Meister
Julie O'Neill
Obrea O. Poindexter
Mary Race
Aaron P. Rubin
Nathan Salminen
Naho Marcella Tajima
Nathan D. Taylor

FOLLOW US

Morrison & Foerster's Socially Aware Blog

@MoFoSocMedia

MORRISON FOERSTER

In this issue of Socially Aware, our Burton Award-winning guide to the law and business of social media, we summarize the FFIEC's recently-issued final guidance on social media use by financial institutions; we report on a new NLRB decision holding that particularly egregious social media postings by employees may fall outside the protections of the NLRA; we provide an update on the California Attorney General's guidance regarding compliance with the state's "do-not-track" disclosure requirements for websites; we discuss a recent case that calls into question the status of domain names as intangible property; we take a look at the latest in a string of cases exploring the First Amendment status of social media activity by government employees; and we highlight an important FTC settlement with a mobile app publisher related to data collection and sharing disclosures.

All this plus a collection of surprising statistics about the most popular people, videos, tweets and hashtags of 2013.

FFIEC ISSUES FINAL GUIDANCE ON SOCIAL MEDIA USAGE BY FINANCIAL INSTITUTIONS

By Obrea O. Poindexter, John Delaney, Nathan D. Taylor and Matthew Janiga

On December 11, 2013, the Federal Financial Institutions Examination Council (FFIEC) issued final guidance for financial institutions relating to their use of social media (the "Guidance"). With its release, the FFIEC adopts its January 2013 proposed guidance in substantially the same form. (*Socially Aware*'s overview of the proposed guidance is available here.)

Financial institutions should expect that the federal banking agencies, Consumer Financial Protection Bureau and National Credit Union Administration (the agencies that comprise the FFIEC) will require supervised institutions to incorporate the Guidance into their efforts to address risks associated with the use of social media and to ensure that institutional risk management programs provide effective oversight and controls related to such use. As a result, financial institutions should consider the appropriateness of their social media risk management programs and should be cognizant of potential technical compliance traps that could result from the use of social media to interact with consumers about products governed by consumer financial protection laws, such as the Truth in Lending Act.

CHANGES TO THE PROPOSED GUIDANCE

Although adopted in substantially the same form as the proposed guidance, the Guidance does attempt to address some concerns raised by commenters. For example, the FFIEC clarifies that compliance should not be viewed as a "one-size-fits-all" process and that institutions should tailor their approach based on their size, complexity, activities and third-party relationships. Additionally, the Guidance clarifies that stand-alone messages sent through traditional email and text channels will not be considered social media. Nonetheless, the Guidance cautions that the term "social media" will be viewed broadly by the agencies.

While the FFIEC attempted to clarify a financial institution's obligations with respect to service providers involved in the institution's social media activities, the Guidance provides limited specific considerations. For example, the Guidance directs institutions to "perform due diligence appropriate to the risks posed by the prospective service provider" based on an assessment of the third party's policies, including the frequency with which these policies have changed and the extent of control the financial institution may have over the policies.

Another area where the FFIEC attempted to clarify its expectations is the extent to which a financial institution would be required to monitor consumer communications on Internet sites other than those maintained by the institution ("Outside Sites"). While the preamble to the Guidance notes that "financial institutions are not expected to" monitor Outside Sites, the Guidance provides that the public nature of social media channels may lead to increased reputational risk, and that compliance considerations may arise if, for example, a consumer raises a dispute through social media. Further, the Guidance states that institutions are still expected to make risk assessments to determine the appropriate approach to monitoring and responding to communications made on Outside Sites. The Guidance also continues to state that, based on the risk assessments, institutions will need to consider the need to "monitor question and complaint forums on social media sites" to review and, "when appropriate," address complaints in a timely manner.

COMPLIANCE CONSIDERATIONS

The cornerstone of the Guidance continues to be the expectation that a financial institution will maintain a risk management program through which it identifies, measures, monitors and controls risks related to its use of social media. The Guidance provides that a financial institution's risk management program should include the following components:

- **A governance structure** so that social media use is directed by the institution's board of directors or senior management.
- **Policies and procedures** regarding the institution's use of social media, compliance with applicable consumer protection laws and regulations, and methodologies to address risks from online postings, edits, replies and retention.
- **A risk management process** for selecting and managing third-party relationships for social media use.

The cornerstone of the Guidance continues to be the expectation that a financial institution will maintain a risk management program through which it identifies, measures, monitors and controls risks related to its use of social media.

– A LOOK BACK –

SOCIAL MEDIA 2013

FACEBOOK

- Most discussed topic (globally): Pope Francis
- Most discussed topic (U.S.): Super Bowl
- Most fans: Facebook for Every Phone (378,766,508 fans)
- Most fans for a non-Facebook brand: Coca-Cola (79,075,939 fans)

TWITTER

- Most followers: Katy Perry (49,893,944 followers)
- Most tweets/second in 2013 (and ever): Miley Cyrus' MTV Music Video Awards performance (306,100 tweets/second)
- Most re-tweeted: Glee's Lea Michele's message reporting the death of co-star Cory Monteith (350,000 re-tweets)

INSTAGRAM

- Most "liked" photo: Justin Bieber with Will Smith
- Most popular hashtag: #love
- Most geotagged location: Siam Paragon Shopping Mall in Bangkok

YOUTUBE

- Most watched video: Psy's "Gentleman M/V" video (nearly 600 million views)
- Second, third and fourth most watched videos are all related to Miley Cyrus

GENERAL

Social media sites by percentage of U.S. adults that used them:*

1. Facebook – **71%**
2. LinkedIn – **22%**
3. Pinterest – **21%**
4. Twitter – **18%**
5. Instagram – **17%**

Percentage of the users of a given social media site that visited the site daily:*

1. Facebook – **63%**
2. Instagram – **57%**
3. Twitter – **46%**
4. Pinterest – **23%**
5. LinkedIn – **13%**

*SOURCE: http://pewinternet.org/~/media/Files/Reports/2013/Social%20Networking%202013_PDF.pdf

- **An employee training program** incorporating the policies and procedures, and informing employees of appropriate work and non-work uses of social media (including defined "impermissible activities").
- **An oversight process** for monitoring information posted to proprietary social media sites administered by the financial institution or contracted third party.
- **Audit and compliance functions** to ensure compliance with internal policies and applicable laws, regulations and the Guidance.
- **Parameters for reporting** to the institution's board of directors or senior management to enable periodic evaluation of the effectiveness of the social media program and whether the program is achieving its stated objectives.

Moreover, the Guidance continues by focusing on identifying potential risks related to a financial institution's use of social media, including risk of harm to consumers. In particular, the Guidance identifies potential risks within three broad categories: (1) compliance and legal risk; (2) reputational risk; and (3) operational risk. While the Guidance catalogs the many risks presented by the use of social media, the focus is on the risks associated with compliance with consumer protection requirements, including:

- **Fair Lending Laws:** While it focuses on an institution's compliance with time frames for adverse action and other notices required by the federal fair lending laws and regulations, the Guidance also highlights possible compliance traps if a financial institution fails to carefully consider whether the institution's social media use is consistent with applicable law. For example, the Guidance highlights that, where applicable, the Fair Housing Act would require mortgage lenders who maintain a Facebook page to display the Equal Housing Opportunity logo.
- **Truth in Lending Act/Regulation Z:** The Guidance highlights that the Regulation Z advertising requirements would apply to relevant advertisements made through social media. Credit card issuers in particular will be familiar with Regulation Z's disclosure requirements for advertisements that include trigger terms and reference deferred interest promotions, and should be cognizant of the application of these requirements in social media advertisements.

- **Truth in Savings Act/Regulation DD:** Like the considerations for compliance with Regulation Z, the Guidance highlights that Regulation DD also contains special advertising requirements for use of trigger terms such as "bonus" and "APY," and further notes that depository institutions can ensure compliance with the federal disclosure requirements by including a link to the additional information required to be provided to the consumer.
- **Deposit Insurance and Share Insurance:** The Guidance reminds institutions that they are required to comply with the advertising requirements for deposit insurance in non-social media advertisements and displays.

The FFIEC having finalized its Guidance, financial institutions will need to carefully review their social media policies and practices in light of the Guidance. Indeed, even companies that are not financial institutions may find the Guidance to reflect emerging best practices for minimizing risk in using social media to promote products and services.

UNCOVERING A LINE IN THE SAND: EMPLOYEE SOCIAL MEDIA USE AND THE NLRA

By Mary Race and Christine E. Lyon

If an employee calls his supervisor a "nasty motherf[**]ker" on Facebook, would the employee lose the protection that he would otherwise enjoy under the National Labor Relations Act (NLRA)? Probably not, according to National Labor Relations Board (NRLB) decisions like *Pier Sixty LLC*.

In Pier Sixty, an employee reacted to a labor dispute by posting the following message about his supervisor on Facebook: "Bob is such a NASTY MOTHER F[**]KER don't know how to talk to people!!!!! F[**]k his mother and his entire f[**]ing family!!!! What a LOSER!!!! Vote YES for the UNION!!!!!!!" Despite the obscenities, the administrative law judge decided that the employee's posting was concerted activity under the NLRA, which is activity by two or more employees that provides mutual aid or protection regarding terms or conditions of employment. This concerted activity was not egregious enough to cause the employee to lose the NLRA's protections. Accordingly, the judge ordered the employer to reinstate the employee. This decision is not an anomaly among decisions interpreting the NLRA. In fact, a number of NLRB cases have held that use of the "f-word" did not exceed the bounds of the NLRA's protection.

Certain situations, particularly egregious postings by employees on social media sites, may fall outside the protection of the NLRA, even when the postings otherwise involve concerted activity.

This has left employers wondering: Is there any limit to what an employee can post? Can postings otherwise covered by the NLRA ever go too far and cross the line into unprotected activity? In a recent decision, *Richmond District Neighborhood Center*, the NLRB demonstrated that it will draw a line in the sand, albeit a thin and distant one. Certain situations, particularly egregious postings by employees on social media sites, may fall outside the protection of the NLRA, even when the postings otherwise involve concerted activity.

Richmond District Neighborhood Center concerned a Facebook conversation between Ian Callaghan and Kenya Moore, who were both employed as teen activity leaders at the Richmond Neighborhood District Center, a non-profit organization that provides youth and family community programs. In a conversation visible only to their Facebook friends, Callaghan and Moore complained about management and discussed plans to defy the Center's rules, posting statements such as:

> "…[L]et them figure it out and they start loosin' kids I ain't help'n HAHA."
>
> "…[W]e'll take advantage, play music loud … teach kids how to graffiti up the walls…. I don't feel like being their b*tch and making it all happy-friendly middle school campy. Let's do some cool sh*t, and let them figure out the money. No more Sean. Let's f*ck it up."
>
> "HAHA we gone have hella clubs and take the kids."
>
> "[H]ahaha! F*ck em. Field trips all the time to wherever the f*ck we want!"
>
> "I'll be back to raise hell wit ya. Don't worry."

The Center fired Callaghan and Moore after another employee brought the conversation to its attention. Callaghan and Moore contended their activity was protected under the NLRA.

The administrative law judge found that the employees were engaged in concerted activity when voicing their disagreement with the Center's management. The judge concluded, however, that even though the employees' remarks constituted concerted activity, the activity was *not protected* under the NLRA. He stated: "[T]he question is whether the conduct is so egregious as to take it outside the protection of the Act, or of such character as to render the employee unfit for further service."

The Center explained that the employees' Facebook conversation was detrimental to its eligibility for grants and could raise

serious concerns for parents of the youth served by the Center. The judge agreed, finding that the conversation was not protected under the NRLA because it "jeopardized the program's funding and the safety of the youth it serves." Moreover, the conduct rendered the two employees "unfit for further service." The judge dismissed Callaghan and Moore's complaint.

Although this decision uncovers a previously obscured line in the sand with regard to protected social media activity, employers should still exercise considerable caution when responding to complaints about an employee's use of social media. Postings that are otherwise protected by the NLRA are unlikely to lose that protection merely because they are offensive, even if they use profanity. *Nonetheless*, the Richmond case reveals that conduct found to endanger an employer's funding or client safety may potentially cross the line and fall outside the wide protection of the NLRA.

Editors' Note: The original posts quoted in this article did not contain asterisks; such asterisks have been added by the authors of this article.

WEBSITE OPERATORS AWAIT FINAL GUIDANCE REGARDING COMPLIANCE WITH CALIFORNIA'S "DO-NOT-TRACK" DISCLOSURE REQUIREMENTS

By Julie O'Neill and John Delaney

Even with the publication of draft "best practices" by the California Attorney General (AG), website operators remain uncertain as to their obligations under the new do-not-track disclosure requirements of the state's Online Privacy Protection Act ("CalOPPA"), which took effect on January 1, 2014.

The new provisions require privacy policy disclosures with respect to: (1) a site operator's tracking of its visitors when they are on third-party sites (if it engages in such tracking) and (2) any "other party's" tracking of the operator's site visitors when they are on third-party sites.

In the first case only, the law requires that the operator disclose how it responds to browser do-not-track signals or other do-not-track choice mechanisms. It does not impose the same disclosure obligation with respect to "other parties"—rather, it requires only that the operator disclose whether other parties engage in such tracking.

Our sense is that the AG's office is unlikely to bring any actions for violations of the amended statute prior to issuing its final guidance.

During a December 10, 2013 call with industry representatives, consumer advocates and other interested parties, the AG's office took the position that a service provider is not the same as a site operator but instead should be treated as an "other party" for purposes of the law. (This position is consistent with the law's definition of an "operator," which appears to exclude service providers.) It follows that the site operator would not have to disclose a choice mechanism with respect to any such "other party."

As a practical matter, this should be a moot point for an operator that uses third parties that are members of the Network Advertising Initiative or Digital Advertising Alliance, as such operator should already be contractually required to disclose how site visitors may opt out of cross-site tracking for online behavioral advertising purposes. Site operators should keep in mind, however, that CalOPPA's provisions cover any type of cross-site tracking—which may also include tracking for analytics or other purposes.

On January 22, 2014, the AG's office circulated a second draft of its best practice recommendations for online tracking transparency. The draft notes that the recommendations are not intended to tell a site operator what disclosures are necessary to comply with CalOPPA. Rather, they will, "in some places offer greater privacy protections than required by . . . law" and are intended to "encourage the development of privacy best practice standards."

The AG accepted comments on its draft until January 29, 2014. We expect that the AG will issue final guidance in the coming weeks. We do not anticipate that the final version of the guidelines will be substantively different from the current draft. That said, businesses may wish to wait until the final version is published before considering any changes to their privacy policies.

Although site operators need to proceed with great caution, our sense is that the AG's office is unlikely to bring any actions for violations of the amended statute prior to issuing its final guidance. If the AG's office does bring such an action, we suspect that the action would most likely involve a "slam dunk" situation—i.e., where a site operator engages in cross-site tracking but makes absolutely no mention of do-not-track, third parties or an opt-out in its privacy policy.

Socially Aware will provide an update after the AG publishes its final best practice recommendations.

YOU MAY NOT NECESSARILY BE THE MASTER OF YOUR DOMAIN

By Naho Marcella Tajima and Gabriel Meister

The ability to associate goods and services with a specific domain name can make or break a business, so much so that companies are still willing to fork over millions to purchase domain names. And although you may consider yourself lucky to have registered a catchy domain name that drives plenty of traffic to your website, query whether the domain name is actually your property; not only do companies that provide domain name registration services frequently take the position that domain names are not property, but at least one recent case law suggests this as well.

The concept that domain names can be "owned" as intangible personal property seems reasonable on its face, particularly given the close relationship between domain names and trademarks, the latter of which historically have been considered property. Domain names frequently contain a registrant's trade name or trademark associated with the registrant's goods or services. Moreover, the Anticybersquatting Consumer Protection Act of 1999 (15 U.S. Code § 1125) permits a trademark owner to pursue an *in rem* action against a domain name that violates the mark owner's rights, and the availability of an *in rem* action implies that the Act treats domain names as property.

On the other hand, domain names and trademarks are distinguishable. For example, certain prerequisites for federal trademark registration, such as proof of the mark being used in interstate commerce to identify a specific type of good or service, do not apply to domain name registrations (which instead are registrable on a first-come, first-served basis). And although similar marks used by different companies can potentially co-exist depending on territorial and other factors, each registered domain name is unique, at least with respect to the applicable top-level domain. (Given that uniqueness, and the ability of domain names to "point" Internet users to information sources, domain names have been likened to toll-free "vanity" telephone numbers; like domain names, vanity telephone numbers that include a company's name or mark are, in a sense, tools that can help drive traffic to the company's offerings.)

Although the court in Alexandria acknowledged that a domain name can be valuable, the court reasoned that such value is subjective and therefore in itself insufficient to support an argument that domain names constitute property.

On November 7, 2013, in *Alexandria Surveys, LLC v. Alexandria Consulting Group*, the U.S. District Court for the Eastern District of Virginia held that under Virginia law, domain names, like telephone numbers, are not property. In *Alexandria*, two competitors, Alexandria Surveys LLC ("ASL") and Alexandria Consulting Group ("ACG"), each sought the rights to the domain name alexandriasurvey.com, which previously had been registered by Alexandria Surveys International ("ASI"), a debtor in bankruptcy. ASL had purchased from Cox Communications ASI's former telephone number and domain name, which had not been scheduled by the trustee in ASI's bankruptcy proceeding. ASI's estate was later reopened, and among other assets, the trustee auctioned off that same telephone number and domain name to ACG. The bankruptcy court ordered ASL to hand over the disputed assets to ACG, and ASL appealed.

The District Court, noting the absence of any on-point Fourth Circuit precedent, relied on the 2000 decision in *Network Solutions Inc. v. Umbro International, Inc. et al.*, in which the Virginia Supreme Court held that domain names are contractual rights rather than property rights subject to garnishment; that is, that they are merely "the product of a contract for services between the registrar and registrant," because they cannot exist without the provider performing services under the applicable domain name registration services agreement. Although the court in *Alexandria* acknowledged a split in authority concerning the proprietary nature of telephone numbers, the court ultimately agreed with the Virginia Supreme Court's conclusion that "Virginia does not recognize an ownership interest in . . . web addresses[,]" and held that ASI's domain names were not transferred as part of the estate. Although the court in *Alexandria* acknowledged that a domain name can be *valuable*, the court reasoned that such value is subjective and therefore in itself insufficient to support an argument that domain names constitute property.

The view that domain names are not personal property can be viewed as contrary to the Ninth Circuit's well-known 2003 ruling in *Gary Kremen v. Stephen Michael Cohen, et al.*, concerning the wrongful transfer of the highly lucrative domain name sex.com. In *Kremen*, Gary Kremen, the original registrant of sex.com, sought to recover against Network Solutions, ("NSI") under theories of breach of contract

and conversion after NSI transferred the domain name to Stephen Cohen without his authorization. Although Kremen's breach of contract claim failed for want of consideration—Kremen had registered sex.com in the mid-1990s, when NSI was issuing domain name registrations to companies and individuals free of charge—the Ninth Circuit ruled that a registrant does have a property right in a registered domain name and that the unauthorized transfer of that domain name serves as a basis for a claim of conversion. In support of this conclusion, the Ninth Circuit pointed out that domain names represent an interest that is well-defined; that domain names are subject to exclusive possession or control; and that registrants can have a legitimate claim to exclusivity over domain names.

Meanwhile, some domain name registration service providers go to great lengths to inform their customers that domain names are not property. Namecheap's registration agreement states: "You further agree that domain name registration is a service, that domain name registrations do not exist independently from services provided pursuant to this or a similar registration agreement with a registrar, and that domain name registration services do not create a property interest." And GoDaddy's registration agreement requires customers to "acknowledge and agree that by registering a domain name, you are not acquiring any property rights in that domain name."

Also keep in mind that treating domain names as property is not without potential problems. For example, as the Virginia Supreme Court pointed out in *Network Solutions*, treating domain names as property and thereby subjecting them to garnishment could open the door to garnishment of other business indicia, such as corporate names, "by serving a garnishment summons on the State Corporation Commission since the Commission registers corporate names and, in doing so, does not allow the use of indistinguishable corporate names." It is unclear how problems like these might be resolved in the future.

For now, whether domain names constitute personal property is a tough question and may depend on the jurisdiction where a claim is ultimately raised. And, from a practical standpoint, care should be taken in how domain names are treated in commercial transactions, given that domain names are frequently among a business's most important assets.

REFINING THE FIRST AMENDMENT STATUS OF SOCIAL MEDIA ACTIVITY BY GOVERNMENT EMPLOYEES

By Nathan Salminen and Aaron Rubin

The Supreme Court's 1968 decision in *Pickering v. Board of Education* allows governmental employers, including law enforcement agencies, to fire or discipline employees for disrupting operations with excessive complaining, but it prohibits governmental employers from firing or disciplining an employee for speaking out on matters of public concern as a private citizen if the employee's interest in speaking outweighs the agency's interest in maintaining efficiency. While the line between disruptively complaining and responsibly speaking out may be clear enough in theory, however, it is often difficult to draw in practice, particularly when the employees in question work in law enforcement. The most recent case to dive into this thicket is *Graziosi v. City of Greenville*, from the Northern District of Mississippi.

We previously discussed the First Amendment rights of law enforcement personnel in connection with the Eleventh Circuit case *Gresham v. City of Atlanta*. In Gresham, the plaintiff was passed over for a promotion after making a Facebook post critical of what she saw as obstruction of justice by a fellow officer. The court held that the plaintiff had spoken on a matter of public concern, but that her interest in speaking did not outweigh the government's interest in promoting efficiency. The key point was that the plaintiff had configured her Facebook post to be viewable only by her friends, which indicated that her post was not "calculated to bring an issue of public concern to the attention of persons with authority to make corrections . . . the context was more nearly one of Plaintiff's venting her frustration with her superiors."

The decision in *Graziosi* deals with the same elusive line between mere complaining on the one hand, and alerting the public to important information about the operations of government agencies on the other. A member of the Greenville Police Department, Sergeant Graziosi, made a series of public Facebook posts criticizing the chief of police for failing to send a representative to the funeral of a fellow officer. Graziosi posted these complaints first as her own Facebook status update, and then posted them on the campaign page of the local mayor. The chief of police fired Graziosi for making the posts, which the chief of police contended violated several internal police department policies that forbid public criticism and excessive complaining by officers. Graziosi filed a lawsuit alleging that her termination violated the First Amendment.

One pivotal issue in the case was whether the criticisms Graziosi posted on Facebook qualified as speaking out on a matter of public concern as a private citizen. Graziosi argued that a decision about whether or not to send police officers to a funeral is inherently a matter of public concern because it involves the spending of public funds. However, the court noted

that if anything that involved spending funds was a matter of public concern, then "almost anything" would satisfy that requirement of the *Pickering* test. Instead, the court looked to the primary motivation for speaking. The court determined that "Graziosi's comments to the Mayor, although on a sensitive subject, were more related to her own frustration of Chief Cannon's decision not to send officers to the funeral and were not made to expose unlawful conduct within the Greenville Police Department. Her posts were not intended to help the public actually evaluate the performance of the GPD." The court found that Graziosi was speaking out about a matter that was primarily internal to the police department, and hence, she was speaking not as a citizen, but as an employee, and not on a matter of public concern, but on a matter of personal concern. Therefore, her comments did not pass the threshold requirement of the *Pickering* test.

> The decision in Graziosi deals with the same elusive line between mere complaining on the one hand, and alerting the public to important information about the operations of government agencies on the other.

This decision is similar to the decision in *Gresham*, but differs in important ways. In both cases, the complaints that a law enforcement officer posted on Facebook were denied First Amendment protection because those complaints were more fairly described as venting frustrations than as attempts to get important information to the public. In both cases, the court found that although the topic of the speech was of at least some concern to the public, the speaker was primarily motivated by a desire to vent frustration. In *Gresham*, the court made this determination by considering the audience that the plaintiff spoke to; in *Graziosi*, the court made this determination by considering what the plaintiff spoke about. However, the courts applied the determination that the speaker was motivated primarily by a desire to vent at different steps in the analysis. In *Gresham*, the court found that the plaintiff's interest in complaining was less weighty than the interest of the police department in preserving efficiency. However, in *Graziosi*, the court found that the plaintiff's primary purpose of venting personal grievances defeated her claim before the weighing stage was even reached. Because the plaintiff's intent was primarily to vent frustration, she was not speaking as a private citizen or speaking on a matter of public concern, and hence would not have been eligible for First Amendment protection even if her interest had outweighed the interest of the police department.

Viewed in the light of recent high-profile situations involving governmental employees speaking out about matters of public concern contrary to applicable governmental policies, such as the leaks by Edward Snowden and Chelsea (formerly Bradley) Manning, clarifying the rules in this area is more important than ever. And the fact that so much of the relevant communication now takes place in the diverse and always-changing world of social media only increases the complexity of the issues. As a result, we can expect that the courts will continue to develop the law in this area for many years, but the outline of how the First Amendment applies to governmental employees using social media is at least beginning to take shape.

FTC EXPANDS REACH ON CONSPICUOUSNESS OF PRIVACY DISCLOSURES IN SETTLEMENT WITH ANDROID FLASHLIGHT APP

By Reed Freeman and Adam Fleisher

An FTC settlement with a mobile app over its privacy disclosures alleged to be deceptive may seem to be run-of-the-mill. After all, the FTC has been settling cases for years with companies whose data collection and use practices are allegedly not consistent with the representations those companies make in their privacy policies.

But the FTC's Complaint and Order with Goldenshores Technologies ("Goldenshores"), announced on December 5th, is a particularly noteworthy Section 5 case because the FTC's theory is that the company's alleged violation of Section 5 resulted not out of an affirmative representation regarding its app alleged to have been deceptive, but from an alleged *material omission*, and from an allegation that whatever disclosures there were *did not rise to the required level of prominence because they were in the privacy policy and EULA only*.

These types of allegations and policy determinations have heretofore been limited to spyware, and have crept into online behavioral advertising, but have generally not been part of FTC enforcement actions in other contexts. This case represents the FTC's signal to industry that material facts, especially those involving sensitive data, and especially where the facts involve collection, use or disclosure of data that may surprise ordinary users because it is out of context of the use of the service, must be disclosed not only

in a privacy policy, but also outside the privacy policy, clearly and conspicuously, prior to collection of the data.

THE APP'S COLLECTION AND USE OF "SENSITIVE DATA"

Goldenshores is the developer of the immensely popular "Brightest Flashlight Free" flashlight app (the "app") for Android devices. The FTC Complaint explains that the app can be downloaded from the Google Play application store, amongst other places. The gravamen of the FTC's Complaint stems from the allegation that while the app is operating as a flashlight (using the phone's screen and LED flash for the camera) it is also collecting and transmitting certain information from the mobile device to third parties including ad networks. This information includes precise geolocation information and persistent device identifiers that can be used to track a user's location over time.

The app ran into two problems with these alleged data collection and use practices. First, the FTC alleged that it did not adequately disclose that information including geolocation and the persistent device identifiers would be collected and shared with third parties, such as advertising networks. Second, the app did not accurately represent consumers' choices with regard to the collection, use and sharing of this information.

However, the Complaint does not start out by focusing on these collection and use practices, and the app's disclosures relating to them. Instead—and not insignificantly—it starts by describing the app's promotional page on the Google Play store. The Complaint notes that this page describes the flashlight app, but "*does not make any statements relating to the collection or use of data from users' mobile devices*" (emphasis added). Similarly, the FTC notes that the general "permission" statements that appear for all Android applications provide notice about the *collection* of sensitive information, but not about any *sharing* of sensitive information.

But these issues do not reappear in the FTC's allegations regarding the actual violations of Section 5 of the FTC Act for deceptive practices. Thus, it seems safe to assume that the FTC cited the lack of notice *prior to download* about the use and sharing of sensitive information to signal to app developers and platforms that it expects to see such disclosures.

This case represents the FTC's signal to industry that certain material facts must be disclosed not only in a privacy policy, but also outside the privacy policy, clearly and conspicuously, prior to collection of the data.

THE APP'S DISCLOSURES REGARDING SENSITIVE DATA

The FTC's allegations specifically focus on the disclosures made by the app in its privacy policy and end user license agreement ("EULA"). In short, the Complaint notes that while the app's privacy policy discloses that the app collects information relating to "your computer," it does not *specifically disclose*: (1) that sensitive information such as precise geolocation is collected; or (2) that it is transmitted to third parties. Based on this failure to disclose, the FTC alleged that the app violated Section 5 by materially misrepresenting the scope of its data collecting and sharing, specifically the collection and sharing of precise geolocation information and persistent device identifiers.

As for the EULA, the Complaint explains that after a user downloads and installs the app, the user is presented with a EULA that must be accepted to use the app. First, like the privacy policy, the FTC alleges that the EULA does not accurately and fully disclose the data and sharing practices of the app. Second, the FTC alleges that the EULA also misleads consumers by giving them the option to "refuse" its terms. As the Complaint puts it, "that choice is illusory." The problem is that the app transmits device data including precise geolocation and the persistent identifier before the user accepts—or refuses—the terms of the EULA. As a result, the EULA misrepresented that consumers had the option to "refuse" the collection of this information, because "regardless of whether consumers accept or refuse the terms of the EULA, the Brightest Flashlight App transmits . . . device data as soon as the consumer launches the application. . ."

NEW DISCLOSURES REQUIRED BY THE SETTLEMENT

For the most part, the Agreement and Consent Order is what we've come to expect from the FTC in Section 5 cases relating to data collection and use practices. Thus, for instance, Goldenshores and any apps it develops, including this Flashlight app, are barred from misrepresenting the manner in which information is collected, used, disclosed or shared.

What makes this Order unique, however, is the specificity the FTC provides with regard to the disclosures Goldenshores must make about the collection and use of precise geolocation information in its apps. The Order requires a notice that goes significantly beyond the typical boilerplate "just-in-time" opt-in notice that apps typically use to obtain consent for the collection of precise geolocation information. In this case, **the separate out-of-policy just-in-time notice and opt-in consent that the app must provide *prior* to collecting precise geolocation information must include a disclosure that informs the user:**

1. **That the application collects and transmits geolocation information;**

2. **How this information may be used;**

3. **Why the application is accessing geolocation information; and**

4. **The identity or specific categories of third parties that receive geolocation information directly or indirectly from the app.**

CONCLUSION

Thus, what looks at first to be a simple privacy policy FTC deception case is actually rather significant for three reasons. First, this is about the failure to disclose collection and use practices relating to "sensitive data," which includes precise geolocation and the device's unique identifier. Second, the FTC flagged the lack of disclosures about such collection and use practices in the app store prior to download. And third, the FTC gave very specific and detailed instructions to the app developer on how it must provide notice and choice about the collection of precise geo-location information, which could perhaps be an indication of where the FTC expects the entire industry to go in the near future.

SOCIALLY AWARE INVITES YOU TO "SOCIAL MEDIA 2014: ADDRESSING CORPORATE RISKS," THE COUNTRY'S PREMIER SOCIAL MEDIA LAW CONFERENCE

Did you know that Facebook now has *well over one billion monthly active users*? (By contrast, the entire population of the United States is 314 million people.) Or that Facebook accounts for over ten percent of all U.S. web traffic? And that *over 300 million photographs* are posted to Facebook each day? Or that Twitter users are expected to send over 146 billion tweets during 2013? And that *over six billion hours of video* are viewed each month on YouTube, almost an hour for every person on Earth?

Facebook, Foursquare, Google+, LinkedIn, Pinterest, Tumblr, Twitter, YouTube and other social media sites are transforming not only the daily lives of consumers, but also how companies interact with consumers. Indeed, even the largest, most conservative blue-chip corporations have begun to embrace social media; one study revealed that, of the Fortune Global 100, 82% had Twitter accounts; 74% had a presence on Facebook; and 79% had a YouTube channel; these numbers will only increase over time. Many marketing professionals view social media as the single greatest marketing tool to have emerged in this century.

However, along with the exciting new marketing opportunities presented by social media comes challenging new legal issues. In seeking to capitalize on the social media gold rush, is your company taking the time to identify and address the attendant legal risks? The good news is that, merely by undertaking simple, low-cost precautions, companies seeking to use social media can significantly reduce their potential liability exposure.

Please join us as leading practitioners and industry experts explore the cutting-edge legal concerns emerging from social media, and provide practical solutions and real-world insights to assist you in tackling these concerns.

What you will learn

- Social media: how it works, and why it is transforming the business world
- Drafting and updating social media policies
- User-generated content and related IP concerns
- Ensuring protection under the CDA's Safe Harbor
- Legal issues in connection with online data harvesting
- Online marketing: new opportunities, new risks
- Privacy law considerations
- Practical tips for handling real-world issues

This conference is being held in San Francisco on February 10, 2014 and in New York City on February 26, 2014; the February 10th event will be webcasted. Socially Aware co-editor John Delaney will serve as conference chair and representatives from top social media companies will be presenting at the event. For more information or to register, please visit Practicing Law Institute's website at www.pli.edu/content.