SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP & AFFILIATES

Skadden

PRIVACY UPDATE

An Overview of Legislative, Regulatory and Technology Developments in the Privacy Sector

January 2013

INSIDE

LEARN MORE

If you have any questions regarding the matters discussed in this memorandum, please contact **Stuart D. Levi**, 212.735.2750, stuart.levi@skadden.com or your regular Skadden contact.

Four Times Square, New York, NY 10036
Telephone: 212.735.3000

WWW.SKADDEN.COM

Video Privacy Protection Act Amended to Allow Sharing of Online Viewing Histories Through Social Media Platforms

President Obama recently signed into law an amendment to the Video Privacy Protection Act of 1998 (VPPA)[1] that will allow users of online video streaming and rental services to share their viewing histories through social media platforms after providing a single informed, written consent to the video service. Until the amendment was passed, the VPPA prevented any automatic sharing of video viewing preferences unless video services had first obtained informed, written consent for each video shared — a prohibitively burdensome requirement.

The VPPA was passed in response to the publication of Robert Bork's video rental history during his Supreme Court confirmation hearings in 1988. The law was meant to protect an individual's privacy in choosing what films to watch — considered a mainstay of intellectual freedom under the First Amendment. The major concern among the law's supporters was that with the development of computerized data systems, "it would be relatively easy at some point to give a profile of a person and tell what they buy in a store, what kind of food they like, [and] what sort of television programs they watch … something we have to guard against."[2] Such consumer profiling is now a reality — to an extent likely unimaginable a quarter-century ago, and public fear over disclosure of private information has only intensified.

However, the language of the VPPA also prevented consumers from voluntarily sharing movie and television tastes with their friends and followers on social media — also argued to be a First Amendment right — and prevented content providers and video services from reaping the rewards of the grass roots marketing and advertising capabilities that social media can provide.

In 2011, a class action was brought against Hulu for violation of the VPPA. A California district court ruled that the VPPA, which applies to any provider of "prerecorded video cassette tapes or similar audio visual materials," covers online video streaming services as well as their brick-and-mortar video rental predecessors.[3] This case confirmed that video service providers and users would not be able to engage in the types of sharing they desired under the existing law and prompted Netflix and others to lobby aggressively for a change to the 25-year-old statute.

The amendment also contains certain safeguards that attempt to ensure viewing histories are not shared without users' informed, written consent. For example, the amendment lets service providers allow users to consent to sharing either before each video is shared or for a time period of up to two years, but requires that users be allowed to opt out at any time and to opt out of sharing certain videos on a case-by-case basis.

Despite the amendment's consent requirements, privacy advocates have voiced concern that users will fail to take advantage of opt-outs or understand social media privacy settings, and will unwittingly allow video services to share viewing history beyond the scope that users intend. There is fear that once combined with a user's social media profile, video viewing history could become a valuable commodity to be sold to advertisers and market researchers, but that the amended law does not require consent for subsequent sharing of information by social media platforms or prevent them from selling users' viewing history.

New State Laws Prohibit Employers From Requesting Social Media Passwords From Employees and Applicants

As of January 1, 2013, four states — California, Illinois, Maryland and Michigan — have enacted laws that prohibit employers from requesting personal social media log-in credentials from employees and job applicants. The laws generally prohibit employers from (1) asking an employee or applicant to disclose his or her social media username or password, (2) asking an employee or applicant to access his or her social media account while the employer observes, or (3) punishing or threatening to punish an employee or applicant who refused to comply with an illegal request. Seventeen states, including New York, New Jersey and Massachusetts, have similar measures pending.

Background

After the Associated Press reported that some employers demand access to social media accounts in March 2012, both the ACLU and Facebook — which noted that sharing or soliciting passwords violates the site's terms of use — urged that legislative action be taken to stop the practice. Legislation was proposed to add provisions to the Federal Communications Commission Process Reform Act of 2012 that would have allowed the FCC to prohibit employers from demanding confidential log-in information. However, the measure did not pass. As a result, state legislatures stepped in to prohibit the practice by employers in their states.

The state-by-state approach has resulted in a patchwork of legislation, with states adopting differing definitions of "social media" and slightly different approaches. Some states, such as California, broadly define "social media" to include any "electronic service or account" or "Internet Web site profiles or locations."[1] The pending New York law does not limit its reach to "social media" and prohibits an employer from requesting a "user name, password or other means for accessing an employee's personal account or service" through an "electronic communications device."[2]

Although the laws aim to protect employer privacy, they may pose difficulties for financial industry employers and public companies that are subject to federal securities laws that sometimes require them to supervise employees' use of social media to ensure compliance. For example, in December 2012, the SEC alleged, for the first time, violations of federal disclosure requirements based on social media communications. The statements were made by Netflix CEO Reed Hastings, who posted on Facebook in July 2012, "Netflix monthly viewing exceeded 1 billion hours for the first time ever in June." His post potentially violated Regulation Federal Disclosure (Reg-FD), which prohibits publically traded companies from disclosing material nonpublic information to some groups or individuals without making the information available to the entire marketplace.

Most states that have enacted legislation have taken special measures to alleviate this conflict for employers. The California, Maryland and Michigan laws allow employers to obtain employee social media information to conduct investigations to ensure compliance with laws or regulations. The statute pending in Delaware allows for extensive exemptions to account for securities law requirements, but no similar exemptions exist under the enacted Illinois law or the bill pending in New York. However special carve-outs may be unnecessary, as it may be argued that SEC rules and regulations preempt the state statutes to the extent that they interfere with an employer's ability to comply with the federal requirements.

Some states also have passed similar laws to prevent educational institutions from requesting social media log-in information from students and applicants.

Data Processors Can Now Use Binding Corporate Rules for Transferring Personal Data

Entities that process data for third parties now have an additional means to lawfully transfer personal data maintained by their clients based in the EU — binding corporate rules or "BCRs."[1] Historically, the use of BCRs was limited to data controllers seeking to transfer personal data from one entity to another entity in the same corporate group.[2] The Article 29 Data Protection Working Party (the Working Party) adopted the new BCRs in June 2012, and, as of January 1, 2013, data processors can officially submit their BCRs for approval.

Background

The EU Directive on Data Protection (the Directive)[3] generally prohibits the transfer of personal data to non-EU nations that do not meet the EU's standard of "adequate" privacy protection. This presents a potential impediment for data transfers to the United States, as U.S. privacy laws are not considered "adequate" for such purposes.

Historically, several options have existed for facilitating such transfers of personal data. First, a U.S.-based company and its EU counterparty can enter into the "model clauses" promulgated by the Working Party. These contractual provisions govern the means by which personal data will be transferred and processed outside the EU. However, the "model clauses" generally cannot be tailored to individual business needs or practices, and must be entered into for each data processing relationship. Alternatively, a U.S.-based entity can participate in the voluntary EU-U.S. Safe Harbor framework by self-certifying that it complies with seven specified privacy protection principles. Participants in the Safe Harbor framework are deemed to have "adequate" privacy practices and can therefore receive personal data from the EU without entering into "model clauses." The annual process for self-certifying, however, can be cumbersome and is only available to companies subject to regulatory oversight by the Federal Trade Commission or Department of Transportation.

A third option allows companies to submit BCRs, which are internal codes of conduct regarding data privacy and security, to EU Data Protection Authorities (DPAs). Once approved, personal data can be freely transferred between the companies covered by the BCRs. However, BCRs have not traditionally been an option for data processors seeking to process personal data transferred from the EU, as use of BCRs has been limited to companies seeking to transfer data amongst their affiliates.

Data Processor BCRs

The Working Party's recent adoption of data processor BCRs now extends this third option to service providers and other data processors. The requirements for the data processor BCRs are similar to those found in the existing data controller BCRs, with processor-specific requirements. For example, in addition to cooperating with the DPAs, a data processor's BCRs also must include a clear duty to cooperate and assist each applicable data controller in complying with data protection laws. In addition, the processor BCRs must be linked to, and made binding through, specific reference in the applicable services agreement. Finally, the data processor must notify each data controller in advance of any changes to its BCRs that will affect processing conditions so as to enable the controller to object to the change or terminate the relevant services agreement.

A data processor may submit its BCRs for approval by completing the application form available on the Working Party's website. The application process is the same as used for BCRs submitted by data controllers and involves submitting draft BCRs along with the application form available on the Working Party's website. A lead DPA is designated and the "mutual recognition" system is utilized to help streamline the application process.[4] Once approved, a data processor's BCRs demonstrate that it provides adequate protection of personal data and

therefore eliminates the need for including "model clauses" in each services agreement or certifying to the Safe Harbor framework.

Operating under DPA-approved BCRs could prove an attractive selling point for data processors looking to expand or maintain their client base in the EU, as EU-based data controllers may take comfort in the fact that BCRs require the service provider to cooperate with both the controller and the DPAs in privacy matters. However, some data processors may find that drafting BCRs and undergoing the DPA approval process is a potentially time-consuming and cumbersome process, and may be wary about opening up their practices to DPA oversight. Data processors ultimately will need to assess which method of transferring personal data outside of the EU best suits their business practices and the needs of their clients.

California Attorney General Issues Guidelines for Mobile App Privacy

Overview

On January 10, 2013, California Attorney General Kamala Harris issued guidelines regarding mobile app privacy entitled "Privacy on the Go: Recommendations for the Mobile Ecosystem" (Guidelines). These non-binding Guidelines recommend practices that go well beyond those required under current U.S. and California law. The Guidelines also encourage app developers and others in the mobile ecosystem to adopt best practices and consider the privacy implications of their choices "at the outset of the design process" and thereafter.

The issuance of the Guidelines represent the latest step by the attorney general to ensure that the rapid advances in the mobile space are not achieved at the cost of the right to privacy, an "inalienable right" guaranteed by the California constitution.[1] Last year, the California attorney general announced the Joint Statement of Principles — which was endorsed by Amazon, Apple, Facebook, Google, Hewlett-Packard, Microsoft and Research In Motion — to help ensure that mobile apps comply with applicable privacy laws. As of October 2012, all of the signatory companies with app stores reported that they had implemented the principles, which includes the California Online Privacy Protection Act's requirement that all apps conspicuously post a privacy policy.[2]

In July 2012, the attorney general created the Privacy Enforcement and Protection Unit, with the mission of protecting California consumers' right to privacy. Its activities include enforcing state and federal privacy laws and developing programs to educate consumers and businesses on privacy rights and best practices. The new Guidelines are a part of the unit's effort to encourage businesses to adopt best practices regarding consumer privacy.

The principles that provide the basis for the Guidelines are not new to privacy advocates — for example, advocating for the education and empowerment of consumers to make informed privacy choices, and transparency regarding the collection and use of personal data. Several aspects of the Guidelines, however, are unique and noteworthy.

First, the Guidelines are directed not only at app developers but also include recommendations for app platform providers, advertising networks, operating system developers and mobile carriers.

Second, although the Guidelines are nonbinding, they come amidst the National Telecommunications and Information Administration's (NTIA) facilitation of the multi-stakeholder process to develop an enforceable code of conduct on mobile app transparency—a process in which the Attorney General is a participant.

Third, the Guidelines introduce the concept of "surprise minimization" — *i.e.*, minimizing the likelihood that consumers will be unpleasantly surprised by "unexpected privacy practices" — as a paradigm for developers and others to adopt when making design and functionality choices. In

this way, the Guidelines attempt to strike a balance between innovative uses of personal data and the need to educate consumers about such innovations so as to allow them to make informed privacy choices. To that end, the Guidelines call for using "enhanced measures" to "alert users and give them control over data practices that are not related to an app's basic functionality or that involve sensitive information." Thus, although the Guidelines recommend limiting the collection of personal data to only that which is necessary for the app to function, they permit collection and use of personal data beyond what is necessary so long as "special notices" are delivered to consumers "in context" and "just-in-time." The Guidelines also recommend using short privacy statements to highlight potentially unexpected practices, along with privacy controls that allow users to make, review and change their in-app privacy settings.

Highlights of Recommendations

App Developers. The bulk of the recommendations in the Guidelines are directed at app developers. The recommendations lay out a process designed to ensure that privacy is considered by app developers from the start of the app design process. This process includes:

- Starting the development process with a checklist to consider the types of data the app could potentially access and collect, taking into consideration the data collection and use practices of any third-party software that is incorporated into the app;
- Identifying what personal data is necessary for the app's basic functionality and what nonessential data or "sensitive information"[3] the app may collect;
- Determining data use, sharing, retention and security practices based thereon;
- Deciding whether "special notices" or other "enhanced measures" should be implemented; and
- Drafting a privacy policy that describes the app's data practices and highlights any "enhanced measures."

The Guidelines also include recommendations regarding privacy policies; "enhanced measures" designed to implement the aforementioned "surprise minimization" approach; and privacy practices intended to align app developers' decisions with the Fair Information Practice Principles.[4]

App Platform Providers. The recommendations directed at app platform providers are intended to facilitate the development of best practices for mobile privacy in general. These recommendations include:

- Educating app developers about their obligations regarding consumer privacy;
- Educating consumers regarding privacy choices, both prior to and after downloading an app;
- Encouraging and empowering consumers to make informed decisions regarding their privacy; and
- Facilitating the policing of apps that do not comply with applicable laws or with the apps' privacy policies.

Advertising Networks. The Guidelines' recommendations directed at advertising networks principally address the fact that most consumers have no way of determining whether and how their personal data is being used by advertising networks to deliver targeted or behavioral advertising. The recommendations, which are primarily intended to increase transparency and user control over the use of personal data for advertising purposes, include:

- Providing app developers with a clear, comprehensive privacy policy that the app developers can link to and make available to users before they download or begin using the app;
- Adhering to the "surprise minimization" approach by implementing "enhanced measures" prior to accessing users' personal data;

- Not delivering ads outside the context of the app (such as adding icons to the mobile desktop or delivering adds through a browser by modifying the browser settings); and
- If ads are delivered outside the context of the app, taking extra precautions to obtain users' prior consent and clearly indicating which app is providing the ad.

Finally, the Guidelines highlight opportunities for operating systems developers and mobile carriers to collaborate with each other and with others in the mobile space to reduce security-related risks and foster an environment that respects individuals' privacy rights. These recommendations include working with device manufacturers and others to establish cross-platform standards for privacy controls, means of enabling the delivery of special privacy notices, and uniform privacy icons that consumers can recognize and rely on to inform their privacy choices. Operating system developers also are encouraged to develop global privacy settings and overrides that users can use to manage mobile apps' access to their personal data, and to develop tools for app developers to facilitate comprehensive evaluations of data collection, transmission and use.

Conclusion

These Guidelines, which describe best practices for all players in the mobile ecosystem, may have a significant impact on the mobile industry. The attorney general's recommendations send a clear message that the onus of protecting consumer privacy is not only on app developers, but also is borne by app platform providers, advertising networks, operating system developers and mobile carriers. It remains to be seen how these non-binding Guidelines will affect the mobile app industry.

Members of Congress Begin Push to Reform Computer Fraud and Abuse Act

In the wake of the recent criminal prosecution and suicide of Internet activist Aaron Swartz, federal legislators on both sides of the aisle have suggested that reform of the Computer Fraud and Abuse Act (the CFAA),[1] one law under which Swartz was charged, should be a priority in the new Congress. The CFAA prohibits hacking through a number of different suboffenses, including intentionally accessing a computer without authorization or exceeding authorized access to that computer (i) in order to obtain information,[2] (ii) so as to knowingly further a fraud,[3] or (iii) in a manner that causes damage and loss.[4] The statute also includes a private right of action for certain victims of these offenses.[5] Several in Congress are now suggesting that the set of activities that constitute unauthorized access to a computer, as well as the private right of action, may need to be revisited·

In certain cases, calls for a re-examination of the CFAA stem from the interplay between contract breaches and violations of the CFAA. Courts have found that access to a computer that violates a duty of loyalty, contractual agreement or terms of service between the user of a website or internal computer system and the owner of that system may violate the CFAA.[6] These precedents, in turn, have informed criminal jurisprudence, and some federal circuits have found that exceeding contractually limited access rights may be a criminal violation.[7] However, Internet civil rights activists have argued in recent years that this interpretation is overbroad and allows private companies to determine the scope of criminal law. A circuit split regarding the breadth of the CFAA has developed over the last year as other courts have been persuaded by this line of reasoning.[8]

The Swartz case has revitalized efforts to address this interpretative split with new statutory language clarifying that access exceeding that permitted by contractual agreement is not a CFAA violation.[9] Rep. Zoe Lofgren (D-Calif.) has introduced a draft bill that would clarify the CFAA's scope and amend a wire fraud statute by exempting violations of terms of service or other contractual agreements from criminal prosecution under both laws.[10] Members of

the Senate from both parties have supported similar amendments to the CFAA without any corresponding change to wire fraud statutes.[11] Moreover, House Judiciary Chairman Bob Goodlatte (R-Va.) also is interested in CFAA reform and recently said that his committee will "'look at [the CFAA] very carefully and see what we can do in that area,'" with an emphasis on "'what needs to [be] done to make sure that the law isn't abused.'"[12] While the language in the Lofgren and other recent proposals has largely been crafted to restrict criminal prosecutions and not civil actions, the courts have used CFAA criminal precedent to inform civil jurisprudence and vice versa.[13] As a result, any narrowing of the scope of criminal prosecutions under the CFAA may in turn narrow the scope of the private right of action available to victims of unauthorized computer access.

END NOTES

Video Privacy Protection Act Amended to Allow Sharing of Online Viewing Histories Through Social Media Platforms

1 Video Privacy Protection Act of 1998, 18 U.S.C. § 2710, *amended by* Video Privacy Protection Act Amendments Act 2012, Pub. L. No. 112-258, 2012 HR 6671.

2 S. Rep. No. 100-599, at 3 (1988), *quoted in Dirkes v. Borrough of Runnemede*, 936 F. Supp. 235, 238 (D.N.J. 1996) (quoting Senator Patrick Leahy).

3 Order Denying Defendant's Motion to Dismiss Plaintiffs' First Amended Consolidated Class Action Complaint, *In re Hulu Privacy Litigation*, No. C 11-03764 LB (N. D. Cal. Aug. 10, 2012) 2012 WL 3282960.

New State Laws Prohibit Employers From Requesting Social Media Passwords From Employees and Applicants

1 Cal. Lab. Code § 980.

2 H.R. 443, 2013 Leg., Reg. Sess. (N.Y. 2013).

Data Processors Can Now Use Binding Corporate Rules for Transferring Personal Data

1 Article 29 Data Protection Working Party, Working Document 02/2012, Setting Up a Table with the Elements and Principles to Be Found in Processor Binding Corporate Rules, WP 195 (June 6, 2012).

2 The EU Directive on Data Protection distinguishes between "data controllers," the entities controlling the manner and reasons for processing personal data, and "data processors," the entities processing personal data on behalf of data controllers.

3 Council Directive 95/46/EC, 1995 O.J. (L 281).

4 Twenty-one EU member states currently participate in the "mutual recognition" system, whereby once the lead DPA determines an applicant's BCRs satisfy all requirements, the DPAs of the other participating member states BCRs accept the lead DPA's opinion as a sufficient basis for approving the BCRs in their respective member states.

California Attorney General Issues Guidelines for Mobile App Privacy

1 California Constitution, Article I, Section 1.

2 California Business and Professions Code §§ 22575-22579.

3 "Sensitive information" is defined as "personally identifiable data about which users are likely to be concerned, such as precise geo-location; financial and medical information; passwords; stored information such as contacts, photos and videos; and children's information." "Personally identifiable data" is defined as "any data linked to a person or persistently linked to a mobile device: data that can identify a person via personal information or a device via a unique identifier."

4 As formulated by the Organization for Economic Cooperation and Development (OECD), the Fair Information Practice Principles are Openness/Transparency, Purpose Specification, Collection Limitation, Use Limitation, Individual Participation, Data Quality, Security and Accountability. See http://oecdprivacy.org/.

(continued)

Members of Congress Begin Push to Reform Computer Fraud and Abuse Act

1 18 U.S.C. § 1030.

2 18 U.S.C. § 1030(a)(2)(C).

3 18 U.S.C. § 1030(a)(4).

4 18 U.S.C. § 1030(a)(5)(C).

5 18 U.S.C. § 1030(g).

6 *See Int'l Airport Ctrs. LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001); *Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

7 *See United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010); *United States v. John*, 597 F.3d 263 (5th Cir 2010).

8 *See United States v Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc). *See also WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012) (applying *Nosal* rather than *Citrin* in rejecting a civil CFAA claim).

9 *See* Somini Sengupta, "Swartz Suicide Fuels Argument Over 1986 Computer Law," *New York Times*, Jan. 14, 2013, at http://bits.blogs.nytimes.com/2013/01/14/swartz-suicide-fuels-argument-over-1986-computer-law/.

10 *See* Discussion Draft of Lofgren Bill, http://www.lofgren.house.gov/images/stories/pdf/draft%20lofgren%20bill%20to%20exclude%20terms%20of%20service%20violations%20from%20cfaa%20%20wre%20fraud%20011513.pdf ("Discussion Draft").

11 *See* Kashmir Hill, "No, Faking Your Name On Facebook Will Not Be A Felony," *Forbes*, Sept. 16, 2011, at http://www.forbes.com/sites/kashmirhill/2011/09/16/no-faking-your-name-on-facebook-will-not-be-a-felony/.

12 Jennifer Martinez, "House Judiciary Committee to Look at Hacking Law in Wake of Swartz's Death," *The Hill*, Jan. 22, 2013, at http://thehill.com/blogs/hillicon-valley/technology/278593-goodlatte-house-judiciary-to-look-at-computer-hacking-law-in-wake-of-swartz-death.

13 *See, e.g.*, *Miller*, 687 F.3d at 204-07 (applying *Nosal*, a criminal precedent, to decide a civil case); *John*, F.3d 263 at 272 (applying *EF Cultural Travel BV*, a civil precedent, to decide a criminal case).