Skadden

PRIVACY & CYBERSECURITY UPDATE

JUNE 2014

CONTENTS (click on the titles below to view articles)

LEARN MORE

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on Page 11, or your regular Skadden contact.

NEW STUDIES HIGHLIGHT PRIVACY AND CYBERSECURITY RISKS AND COSTS

A number of recent studies have highlighted the risks and costs of cybersecurity attacks. According to a report from the Center for Strategic and International Studies (CSIS), cybercrime imposes a $445 billion annual cost on the global economy.[1] A number that many will find startling is that about 40 million Americans, translating into approximately 15 percent of the population, have had personal information stolen by hackers. Significantly, especially given the media focus on credit card theft, the CSIS report noted that losses from the theft of corporate intellectual property exceeded the $160 billion loss to individuals from cyber-attacks. The study serves as an important reminder that even companies that are not holding personal information are susceptible to costly attacks and that a strong cybersecurity policy, response plan and governance model is essential.

SEC COMMISSIONER ADDRESSES THE ROLE OF THE BOARD ON CYBERSECURITY MATTERS

On June 10, SEC Commissioner Luis A. Aguilar spoke at the New York Stock Exchange on "Boards of Directors, Corporate Governance and Cyber-Risks," urging directors to focus on cyber-risks and the directors' oversight obligations. Aguilar's comments come just a few weeks after an SEC roundtable that discussed the cyber-risks facing public companies and critical market participants like exchanges, broker-dealers and transfer agents.

Aguilar began his remarks by highlighting recent cyber-attacks and noting that, in contrast to other crises a company may face, cyber-attacks require a rapid response to contain the harm. In many cases, companies need to respond "within hours, if not minutes" of a cyber-attack to analyze the event, prevent further damage and initiate a response.

The commissioner next stressed the board's role in corporate governance and overseeing risk management, and its responsibility to ensure that management effectively serves the corporation and its shareholders. While noting that primary responsibility for risk management historically has belonged to management, a corporation's board is responsible for overseeing "that the corporation has established appropriate risk management programs" and "how management implements those programs." According to Aguilar, cyber-risk must be considered part of the board's overall risk oversight. Indeed, given the threat of "significant business disruptions, substantial response costs, negative publicity and lasting reputational harm," and the threat of litigation and potential liability for failing to implement adequate cybersecurity steps, the commissioner warned that "boards that choose to ignore or minimize the importance of cybersecurity oversight responsibility, do so at their own peril." Nonetheless, there has been a significant gap between the high risk of cyber-attacks and the steps that boards have taken to address those risks.

[1] The study was sponsored by security software company McAfee.

The commissioner noted that even when boards do focus on these issues they often rely too much on the personnel who implement the security measures. Board need to be proactive in these areas and understand the risks so they can properly execute their oversight responsibility.

Aguilar outlined some of the key considerations for boards with respect to their oversight responsibilities:

- Boards should consider the February 2014 Framework for Improving Critical Infrastructure Cybersecurity (Framework), released by the National Institute of Standards and Technology (NIST), which provides companies with a set of industry standards and best practices for managing their cybersecurity risks. Interestingly, Aguilar acknowledged that the Framework is voluntary guidance but noted that "some commentators have already suggested that it will likely become a baseline for best practices by companies." Statements such as this by government officials will quickly make the NIST Framework an accepted "best practices" document.
- Many boards, and even audit committees, lack the technical expertise and bandwidth necessary to evaluate cybersecurity issues. Boards might therefore consider mandatory cyber-risk education for directors or include directors with an understanding of the cybersecurity risks the company faces.
- Boards might create a risk committee, or rely on an existing risk committee, that "can foster a 'big picture' approach." Such a committee might consider improved risk reporting and monitoring for management and the board, and greater focus for the board on the adequacy of resources and overall support provided to the company's executives who are responsible for risk management.
- Boards should ensure that the company has appropriate management in the area of cyber-risk, and that they receive regular reports on these issues. This includes having a clear understanding of who at the company has primary responsibility for cybersecurity risk oversight and for ensuring the adequacy of the company's cyber-risk management practices. Aguilar also noted that, according to the evidence, "devoting full-time personnel to cybersecurity issues may help prevent and mitigate the effects of cyber-attacks."
- Boards should ensure that companies have "well-constructed and deliberate" cyber-attack rapid response plans that are consistent with best industry practices — a poorly executed plan can, in many cases, be worse than not having a plan at all. Such plans should include whether, and how, a cyber-attack will need to be disclosed internally and externally to customers and investors.

Aguilar concluded his remarks by observing that strong boards adapt to new circumstances and that cyber-attacks present a new risk to companies. Directors therefore need to take seriously their obligation to ensure companies are appropriately addressing those risks.

Return to Table of Contents

SUPREME COURT DECISION ON CELLPHONE SEARCHES PROVIDES SOME PRIVACY INSIGHTS

U.S. Supreme Court decisions regarding warrantless searches in connection with arrests usually have little relevance to companies. However, a unanimous June 25 decision by the Court regarding cellphone searches by the police provides some interesting insights as to how the Court views an individual's privacy rights in cellphones and the information such phones may contain.

The decision concerned two cases, *Riley v. California and U.S. v. Brima Wurie*. In each case, the police accessed the cellphone of an individual who had been arrested and found incriminating evidence on the phone. In *Riley*, the evidence a photo of the defendant standing by a car that had been used in a shooting; in *Brima Wurie*, the evidence was a phone number identified

as "my house" that the police subsequently searched, finding drugs and weapons. In each case, the defendant moved to suppress the evidence. The government argued in each case that their actions constituted a "warrantless search incident to a lawful arrest," which the Court has upheld in a number of cases.

The Court disagreed, finding that cellphones today introduce an entirely new level of privacy issues, and that individuals — even in the throes of an arrest — have a right to privacy in those devices. In analyzing this issue, the Court noted that there are two overriding issues that permit searches incident to an arrest: protecting the police officer (*i.e.*, to pat the arrestee down to make sure he does not have a weapon) and preventing the destruction of evidence. The government argued that a search of a cellphone could indicate whether confederates of the arrestee were headed to the scene and was therefore important to search. The Court found no actual evidence to support this theory. With respect to the destruction of evidence, the Court acknowledged that remote wiping of the phone (say, by a confederate who learns of the arrest) or automatic encryption that is triggered when the phone is locked could result in the destruction of evidence. However, again the court found no evidence that such practices are prevalent. The Court also held that police officers are unlikely to come across a phone that is unlocked (and must be searched immediately) and could address remote wiping by placing the phone in a foil bag to stop any radio signal transmissions.

The Court next turned to an arrestee's right to privacy in a cellphone. While noting that an arrestee has a reduced privacy interest, the Court found that cellphones today implicate privacy concerns that transcend physical objects that an individual may have historically had in their possession. Using a metaphor, the Court reasoned that cellphones are akin to an individual carrying around a large trunk (which would require a search warrant before it could be examined) as opposed to a small object in a pocket (which would not require a warrant). The Court proceeded to highlight a number of key aspects of cellphones that make them subject to a higher level of privacy protection:

- Nearly three-quarters of smartphone users report being within five feet of their phones most of the time, with 12 percent admitting that they even use their phones in the shower.
- Many of the more than 90 percent of American adults who own a cellphone keep on their person a digital record of nearly every aspect of their lives — from the mundane to the intimate.
- The average smartphone user has installed 33 apps, which together can form a revealing montage of the user's life.
- A cellphone collects in one place many distinct types of information — addresses, notes, prescriptions, bank statements, videos — that reveal much more in combination than any isolated record.
- A cellphone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations and descriptions.
- The data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.

The Court also noted that it was not merely the amount of data that distinguishes cellphones, but also the quality of that data. The Court cited as an example that Internet search and browsing history can be found on an Internet-enabled phone and could "reveal an individual's private interests or concerns — perhaps a search for certain symptoms of disease, coupled

with frequent visits to WebMD. Data on a cellphone can also reveal where a person has been. Historic location information is standard feature on many smartphones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building."

Of equal importance, the Court highlighted the reality that data accessible through a cellphone is not stored on the device itself. Rather, because of cloud computing, a search of a cellphone actually constitutes a search of many other systems. Such a search, according to the Court, far exceeds the scope of a "search incident to an arrest." While the government had conceded that a search of materials stored on the cloud would not be appropriate, the Court correctly observed that law enforcement officials would have no way of knowing whether information they are accessing is stored on the cloud or on the device.

In conclusion, the Court noted that modern call phones are "not just another technological convenience, but hold for many Americans 'the privacies of life.'"

The Court's ruling, although in the context of a Fourth Amendment issue regarding searches incident to an arrest, contains some important insights into the Court's views on privacy. The Court acknowledged that searching a device in today's environment might really mean improperly searching multiple other devices because of cloud computing. This reality might impose a limit on other types of searches in the future.

Return to Table of Contents

DECISION IN HULU CASE CREATES SUBSTANTIAL CLASS CERTIFICATION HURDLES UNDER VPPA

After three years of litigation and with potentially billions of dollars in automatic statutory class damages on the line, a California district court denied class certification in *In re Hulu Privacy Litigation*, C 11-03764 LB (N.D. Cal. Aug 10, 2012), without prejudice to renewal of the motion at a later time. As discussed below, the court's ruling arms defendants with multiple tools to defeat class certification in any privacy class action where alleged personally identifiable information (PII) can be altered or deleted by the user, depending on how he or she interacts with the Internet.

BACKGROUND

Plaintiffs claimed that Hulu violated the VPPA by knowingly transmitting users' PII to Facebook in the form of a Facebook cookie that identified the user on Facebook and a URL that identified the user's video viewing selection. Having survived summary judgment with respect to the claims asserting unlawful disclosures to Facebook,[2] plaintiffs moved for class certification on the ground that common issues among class members predominated over any individual issues and, therefore, class action was superior to adjudication on an individual basis.

To increase their chances of certification, plaintiffs alleged that code written by Hulu to load the Facebook "Like" button on each Hulu.com video streaming page (called a "watch page") also sent Facebook (1) the watch page's URL, which contained the name of the video watched, and (2) a "c_user" cookie created by Facebook that contained the Hulu user's Facebook ID, which specifically identified the Hulu user on Facebook. Plaintiffs argued that these two pieces of data together "identif[ied] a person as having requested or obtained specific video materials" in violation of the VPPA. Plaintiffs sought to certify a class of registered Hulu

[2] In an April 28, 2014, ruling, the court dismissed claims with respect to certain transmissions from Hulu to comScore and, thus, those claims were not the subject of plaintiffs' motion for class certification.

users from April 21, 2010, through June 7, 2010, who also used Facebook and "who at least once during the class period watched a video on hulu.com having used the same computer and web browser to log into Facebook in the previous four weeks using default settings."

Hulu argued that the requisite commonality of legal and factual issues was absent and, in the alternative, individual issues predominated over common issues because Facebook's c_user cookie would not be transmitted during a Hulu session if the user unchecked the "Keep Me Logged In" box when logging into Facebook, manually cleared cookies between logging out of Facebook and using Hulu, or used browser settings or other tools, such as ad blockers, to block cookies. Under these circumstances, Hulu argued, only the Hulu watch page URL would be sent to Facebook and no VPPA violation would occur. Hulu also argued, among other things, that the proposed class was not ascertainable, as required by Rule 23(a).

THE COURT'S DECISION

The court denied class certification, holding that because Hulu only transmitted the c_user in some instances, common questions of law or fact did not predominate over individual ones. Further, even if the class definition could be modified to include only those users whose personally identifiable information was transmitted, it would be impossible to objectively ascertain whether an individual belonged to the class.

ASCERTAINABLE AND DEFINITE CLASS

The court held that the proposed class was not sufficiently definite because it was not possible to determine objectively whether a given individual qualified for class membership. While the court could determine the universe of users who subscribe to both Facebook and Hulu by cross-referencing email addresses, the only way to identify the subset of users whose PII was actually transmitted to Facebook would be to have the users self-report through the submission of affidavits or otherwise whether they (1) were logged into Facebook, (2) cleared their cookies, or (3) used ad-blocking software.

While recognizing that in some circumstances self-reporting may be sufficient, the court held that it was not an appropriate method of ascertaining class membership in this context. Many users might not accurately remember uneventful aspects of their web-browsing history. Furthermore, because the liquidated damages per class member would be relatively high ($2,500 per violation) and because it would be difficult to objectively verify potential members' reports, some users might be incented to provide false affidavits. Thus, the court denied class certification on the ground that the proposed class was not ascertainable. The court did so without prejudice, noting that it could not tell on the record before it "[w]hether these issues could be resolved by narrowing the class definition, by defining subclasses, by reference to objective criteria, by a damages analysis that addresses pecuniary incentives, or otherwise." The court also noted in connection with its predominance analysis "that even the court's best guess at subclassing would not address the issues about ascertainability and identify the class members."

COMMON/PREDOMINANT QUESTIONS OF LAW OR FACT

The court held that plaintiffs' claims shared common questions of law or fact sufficient to satisfy Rule 23(a)(2) of the Federal Rules of Civil Procedure because they would require the court to decide on a class-wide basis: (1) whether the c_user cookie "identifies a person" under the VPPA, (2) whether the watch page URL identifies "specific video materials or services" under the VPPA, and (3) whether Hulu obtained users' "informed, written consent" to disclose their information. However, the court held that common issues did not predominate over individual issues because the court would be required to determine on an individualized basis whether a user's c_user cookie existed at the time of the user's viewing of videos on Hulu. For example, it may have been deleted by the user or blocked by ad blocking software installed by the user.

If no c_user cookie existed or was transmitted to Facebook, then no VPPA violation occurred. These individual issues were thus central to the disposition of the class claims and predominated over any common issues of law or fact.[3]

Hulu also argued that its defense of consent raised individual issues because some putative class members may have consented to the disclosure either by (1) logging into Facebook and thereby accepting Facebooks' general privacy policy or (2) independently posting on Facebook about videos they had watched. The court disagreed, holding that neither of these behaviors constituted consent and were therefore irrelevant to adjudication of plaintiffs' claims. The court noted that whether a class member voluntarily revealed his video viewing choices by posting them on Facebook would not change the allegedly unlawful disclosure of PII under the VPPA by Hulu.

DUE PROCESS CHALLENGE

The court also discussed, without ruling upon (because the court had already denied certification on other grounds), Hulu's constitutional challenge to class certification under the Due Process clause. The VPPA provides that "aggrieved" persons may be awarded "not less than liquidated damages in an amount of $2,500" (18 U.S.C. § 2710(C)(2)) without regard to the absence or presence of actual financial harm. The court recognized as a "legitimate concern" that this minimum statutory damage could result in "a devastatingly large damages award, out of proportion to the actual harm suffered by members of the plaintiff class," and that such a result "may raise Due Process issues." Furthermore, the court noted that "[t]he aggregation of statutory damages claims potentially distorts the purpose of both statutory damages and class actions." The court surveyed cases decided outside the VPPA context that took varying approaches to "the calamitous damages problem," including allowing a class action to proceed and then invoking the Due Process clause to cap damages. In refusing to reach the issue, the court noted that "likely it is one best addressed after a class is certified."

IMPACT OF COURT'S DECISION

The court's ruling will arm defendants with arguments to attack class certification in any privacy case where the PII at issue is packaged in transitory data that could be altered or deleted by the user. In addition, the court acknowledged the Due Process implications of certifying a class where statutory "per violation" damages are high. Although the court felt that this was an issue best left for a later stage in the proceeding, defendants in privacy class actions with high statutory damages would be wise to press the issue at the class certification stage.

Return to Table of Contents

INSURER SEEKS DECLARATION THAT THEFT OF CONSUMER PAYMENT CARD INFORMATION IS NOT COVERED BY COMMERCIAL GENERAL LIABILITY POLICY

On June 18, 2014, Safety National Casualty Corporation filed suit against Michaels Stores, Inc., the nation's largest arts and crafts retailer, in the U.S. District Court for the Northern District of Texas (No. 3:14-cv-02223-L), seeking a declaration that Safety National has no duty to defend or indemnify Michaels in connection with a data breach that compromised millions of customers' credit and debit card information.

According to the complaint, Safety National issued an occurrence-based commercial general liability (CGL) policy to Michaels and its subsidiaries for the period June 1, 2013, to June 1,

[3] Hulu offered a couple of additional factual differences between potential class members' claims: some registered for Hulu with a pseudonym, rather than their legal name. Others allowed someone else to use their Hulu accounts. The court held that because none of these differences affected the elements or defenses of the VPPA claim, they were irrelevant to the predominance inquiry.

2014. As with most CGL policies, the Safety National policy grants Michaels coverage for "bodily injury" and "property damage" (Coverage A) and "personal and advertising injury" (Coverage B), subject to the policy's terms, conditions and exclusions.

The underlying consolidated complaint brought by individuals whose data was allegedly compromised contains two counts — the first for breach of implied contract, the second for violation of certain states' consumer protection statutes — both of which are premised on the allegation that Michaels "fail[ed] to take reasonable measures to safeguard [customers'] financial data" and "failed to follow industry best practices concerning data theft." The complaint seeks certification of nationwide (count one) and multistate (count two) classes in addition to compensatory, punitive and statutory damages; individualized notice to all class members; fees, costs and interest.

According to Safety National's complaint, the company rejected Michael's demand for coverage under the CGL policy because the claims in the underlying putative class actions fail "to allege[] 'bodily injury' or 'property damage' or 'personal or advertising injury,'" a prerequisite to triggering Coverage A or B under the policy. Moreover, Safety National raises the prospect that policy exclusions, including for "expected or intended injury" and "damage to property in Michael's possession, custody or control," may separately bar coverage.

Although Safety National does not elaborate on its no-coverage position, this lawsuit further illustrates what appears to be the now uniform position among insurers that traditional insurance policies do not cover cyber/data-breach losses. To date, the case law regarding insurance coverage for such claims under "non-cyber" policies has been mixed. In addition, an ever increasing number of insurers are adding express exclusions to their traditional policies in this regard or subjecting them to relatively small sublimits. At the same time, however, numerous of these same insurers are offering "cyber"-specific coverage on a standalone basis or as an enhancement to existing policies. Now, more than ever, it is important that insureds fully understand their cyber-related exposure and have a clear picture of what insurance coverage they may or may not have in place to respond to such incidents.

Return to Table of Contents

US-EU SAFE HARBOR: CHANGE IN ARBITRATION FEES

Self-certification to the U.S.-EU Safe Harbor is one of the methods that allows U.S. companies to satisfy the "adequacy" requirement for transborder data flows from the EU to the U.S. under the EU Data Directive. The enforcement principle of the Safe Harbor requires that companies that certify to the Safe Harbor must establish an independent recourse mechanism that consumers may use to address any unresolved complaints and that each company should include an appropriate reference to such mechanism in its privacy policy.

In June, the Department of Commerce sent warning letters to a number of companies that had selected the International Centre for Dispute Resolution/American Arbitration Association as the organization to be used as their independent recourse mechanism. The ICDR/AAA recently changed its Safe Harbor-related dispute resolution program and instituted an upfront/annual administration fee. After being notified of this change by ICDR/AAA, the Department of Commerce warned these companies that they must immediately either contact ICDR/AAA, sign up for the program and pay the fee or select another dispute resolution provider in order to retain the benefits of certification under the Safe Harbor. If a company selects another dispute resolution provider, it must remove all references to ICDR/AAA in its privacy policy and notify the Department of Commerce.

While it is not clear why ICDR/AAA has instituted this new administration fee, the European Commission issued a report in November that called for heightened scrutiny of data handling by U.S. companies. In its report, the commission recommended that the Department of Commerce and the FTC monitor alternative dispute resolution providers more systematically

and that participation fees for any dispute resolution be made more affordable. Seemingly in line with that recommendation, the Department of Commerce noted in its warning letter that although there were no annual fees in the past, "the fees that would have been charged were higher than what is now being charged on an annual basis." This development highlights once again that companies relying on the Safe Harbor must be especially diligent with their compliance, especially at a time when Safe Harbor compliance is coming under increased scrutiny.

Return to Table of Contents

LATEST DEVELOPMENTS IN WYNDHAM HOTEL CASE

KEY ISSUES CERTIFIED TO THE THIRD COURT

A New Jersey district court judge has certified to the Third Court the key questions in the ongoing battle between Wyndham Hotels and the FTC over the company's cybersecurity practices.

As we previously reported, a New Jersey district court denied Wyndham Hotels and Resorts, LLC's motion to dismiss an FTC enforcement action alleging that Wyndham had violated Section 5 of the Federal Trade Commission Act as a result of a cybersecurity attack on Wyndham that resulted in the theft of over 600,000 credit card numbers. Judge Esther Salas' April 7 decision in *FTC v. Wyndham Worldwide Corporation, et al.,* addressed the scope of the FTC's authority over cybersecurity at a time when the FTC is taking a greater enforcement role in such incidents and privacy more generally. Wyndham had argued, in part, that to satisfy fair notice and due process principles, the FTC was required to publish formal rules, regulations or other guidelines regarding appropriate data security practices before it could file a Section 5 unfairness claim. Judge Salas disagreed, holding that the FTC had discretion to proceed by rulemaking or by individual adjudication, especially in areas that were not reasonably foreseeable like cybersecurity.

Wydham sought interlocutory review of that order, and Judge Salas has now certified to the Third Circuit the questions of whether the FTC can bring an unfairness claim involving data security under Section 5 of the FTC Act and, if so, whether the FTC must formally promulgate regulations before bringing such a claim. In her decision, Judge Salas acknowledged "the nationwide significance of the issues in the action, which indisputably affect consumers and businesses in a climate where we collectively struggle to maintain privacy while enjoying the benefits of the digital age." Judge Salas also noted that, given the novelty of liability issues relating to data-security breaches, "reasonable jurists may differ over the court's resolution of the two legal issues in question."

DISTRICT COURT REFUSES TO DISMISS WYNDHAM WORLDWIDE FROM CASE

The FTC's case against Wyndham was brought against Wyndham Hotel & Resorts LLP (Wyndham Hotel) as well as Wyndham Worldwide Corp. and two of its subsidiaries (Wyndham Worldwide). In addition to the motion challenging the FTC's authority, Wyndham Worldwide asserted that it should be dismissed from the suit because any security lapses had taken place through Wyndham Hotel and the FTC had failed to allege direct or derivative liability against Wyndham Worldwide. Judge Salas disagreed, concluding that the FTC had, in fact, sufficiently alleged that Wyndham Worldwide might also be to blame for not providing adequate security on the corporate servers, thereby leading to multiple security breaches at Wyndham Hotel properties. The court highlighted, among other matters, that the FTC had alleged common control amongst the different Wyndham entities, a sharing of office space and a lack of distinction between the defendants. The court cautioned that her ruling merely meant that the FTC had properly framed a complaint against all of the Wyndham entities, but the evidence might reveal that the non-Wyndham Hotel entities had no role in the breach.

Return to Table of Contents

NEW FFIEC CYBERSECURITY WEBSITE

In a nod to the growing importance of sharing cybersecurity information and the increasing role of regulators in this space, the Federal Financial Institutions Examination Council (FFIEC) has launched a website to serve as a "central repository" for cybersecurity information. The site, available at www.ffiec.gov/cybersecurity.htm, is mostly informational in nature, providing links to cybersecurity-related information from FFIEC's six member agencies: the Federal Reserve, the Federal Deposit Insurance Corporation, the National Credit Union Administration; the Office of the Comptroller of the Currency; the Consumer Financial Protection Bureau; and the State Liaison Committee.

In its press release announcing the new initiative, the FFIEC noted that its members are "taking a number of steps to raise awareness of cybersecurity risks at financial institutions and the need to identify, assess, and mitigate these risks in light of the increasing volume and sophistication of cyber threats that pose risks to all industries in our society." The website follows an FFIEC pilot cybersecurity testing program that state and federal regulators will complete during regularly scheduled examinations at more than 500 community financial institutions.

Return to Table of Contents

ITALY ISSUES NEW RULES RELATING TO COOKIES

Italy's Data Protection Authority (the Garante) recently issued new requirements for websites regarding their use of cookies. The Garante's rules outline a two-tiered system, under which websites must publish a prominent banner on the home page and link to a longer body of explanatory text to notify users about the presence and use of cookies and the users' cookie-related rights.[4]

The new rules bring Italy into compliance with the EU's amended e-Privacy Directive.5 They also effectuate various sections of Italy's Personal Data Protection Code, which required the Garante to ensure that websites only store most user information or access a user's stored information after the user gives informed consent.[6]

The new rules distinguish between "technical" and "profiling" cookies, and between website "publishers" and "third parties." Technical cookies are cookies that exist for the sole purpose of transmitting communications, such as a cookie that facilitates a user's navigation of a website. Under the new rules, websites can install technical cookies without obtaining prior consent from users, but they need to disclose to users that these cookies are being used. Technical cookies also include those cookies that allow first-party website operators to aggregate analytics data about website visits. Italy's position on this stands in contrast to that of the EU's Article 29 Data Protection Working Party, which said in a 2012 opinion that analytics cookies do not count as technical cookies.[7]

In contrast, profiling cookies are cookies that track a user's preferences for the purpose of delivering targeted advertisements. These cookies can only be installed on users' devices with the users' prior consent.

---

[4] "Simplified Arrangements to Provide and Obtain Consent Regarding Cookies" (May 8, 2014), *available at* http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3167654.

[5] *See* EU Directive 2009/136/EC § 5(3) (Nov. 25, 2009), available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009L0136.

[6] Personal Data Protection Code, Legislative Decree n. 196 §§ 13, 122, 154 (June 30, 2003) (It.), *available at* http://194.242.234.211/documents/10160/2012405/DataProtectionCode-2003.pdf. The code carves out an exception for information collected for the exclusive purpose of "carrying out the transmission of a communication" or information that is "strictly necessary" in order for a provider to furnish a service specifically requested by a user. The new rules maintain this exception.

[7] Opinion 04/2012 on Cookie Consent Exemption, 00879/12/EN, WP 194 § 4.3, Article 29 Data Protection Working Party (June 7, 2012), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf.

REQUIREMENTS UNDER THE NEW RULES

Websites must include a prominent banner on the landing page and a hyperlink to a lengthier "extended" notice page. The banner must be sufficiently disruptive as to create a "perceptible discontinuity" in the user's experience — *i.e.,* there can be no way for the user to ignore the banner and still access the site. The banner must: (1) inform users whether the website uses profiling cookies, (2) reveal the existence of third-party cookies if the website allows third parties to send such cookies (3) provide a link to an extended notice page and an announcement that the user will have an opportunity on the extended-notice page to refuse consent to the placement of cookies, and (4) inform users that continued use of the website signifies the user's consent to the placement of cookies. Once users view this banner, they can click on the webpage "underneath" the banner and gain access to the rest of the website or link to the extended notice.

The extended notice needs to inform users that the website uses technical cookies as well as profiling cookies (if applicable), allow users to select and deselect which individual cookies they do and do not want the website to place, and advise users of their ability to change their browser settings to reflect their cookie preferences. On the extended notice, the website must provide links to the third parties' own consent forms and information notices, or to the websites of any intermediaries if the publisher is not in direct contact with the third parties that installed the cookies via the website. This reflects the Garante's vision of a relationship that puts minimal onus on the publisher for the conduct of third parties.

Although users are not required to signify consent by clicking on a box, the fact that the website can only be viewed after the "cookie banner" is seen manifests the consent of the user. The new rules give website publishers the freedom to rely on "other mechanisms" to obtain consent so long as those mechanisms sufficiently comply with Italy's Personal Data Protection Code. However, the banner system is specifically approved by Italy, so website publishers that use it will know that their system meets Italy's requirements.

PRACTICE POINTS

The new rules were officially published on June 3, 2014, and websites have one year from that date to adopt the new system. The Garante also reminds website operators that the failure to provide to users the information spelled out in the new rules, the failure to notify the Garante when a website uses certain types of cookies, and the installation of cookies on users' terminal equipment without user consent all carry hefty administrative fines.[8]

Interestingly, the Garante's rules make no reference to mobile applications or to mobile-tracking analogs of cookies. However, Italy's Personal Data Protection Code prohibits storage of information on the "terminal equipment" of a user without user consent. Since either a website or mobile-app manager could place and access user information, the Code itself would seem to apply to both. Developers of mobile apps should be alert for any further clarification of their obligations under the new rules. Similarly, at this time, Italy's rules only address cookies and not other forms of web tracking. Whether future regulations will address tools like web beacons remains to be seen.

---

[8] Simplified Arrangements at Preamble § 7.

Return to Table of Contents

SKADDEN CONTACTS

STUART D. LEVI
Partner / New York
212.735.2750
stuart.levi@skadden.com

TIMOTHY A. MILLER
Partner / Palo Alto
650.470.4620
timothy.miller@skadden.com

TIMOTHY G. REYNOLDS
Partner / New York
212.735.2316
timothy.reynolds@skadden.com

JAMES S. TALBOT
Counsel / New York
212.735.4133
james.talbot@skadden.com

This communication is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This communication is considered advertising under applicable state laws.

Skadden, Arps, Slate, Meagher & Flom LLP
Four Times Square
New York, NY 10036
212.735.3000