

EYE ON PRIVACY

NOVEMBER 2013

WELCOME

While Congress struggles to simply keep the federal government running, states have taken the lead in passing new privacy legislation affecting businesses large and small. California, in particular, recently passed laws enacting a number of new requirements, some set to take effect on January 1. The state is no stranger to being at the forefront of privacy legislation, as its laws regarding the mandatory posting of privacy policies and reporting of data breaches paved the way for similar laws across the country. Now, new laws involving "Do Not Track," children's privacy and advertising, and an expansion of data breach notification requirements are set to impact any organization that interacts with California consumers, and seem likely to start a new wave of similar legislation in other states. In this issue of *Eye on Privacy*, we break down these new laws and discuss their requirements. We also take a look at recent developments regarding timing requirements for breach notifications, a recent data breach case dismissed on standing issues, and an ECPA case involving advertising issues.

We continue to also provide information on significant privacy developments through webinars, speaking engagements, and affiliated programs. Please check out the Events page on wsg.com for further details.

As always, please feel free to e-mail us at PrivacyAlerts@wsg.com if there are any future topics you'd like to see here.



Lydia Parnes

Lydia Parnes
Partner, Washington, D.C.
lparnes@wsg.com

CALIFORNIA AMENDS CALOPPA TO REQUIRE DO-NOT-TRACK DISCLOSURES



Lydia Parnes
Partner, Washington, D.C.
lparnes@wsg.com



Tracy Shapiro
Of Counsel, San Francisco
tshapiro@wsg.com



Sara Rowe
Associate, Palo Alto
rowe@wsg.com



Eddie Holman
Associate, Washington, D.C.
eholman@wsg.com

California Governor Jerry Brown recently signed into law A.B. 370,¹ which amends the California Online Privacy Protection Act² (CalOPPA) to require certain operators of websites and other online services to disclose how they respond when a visitor's web browser sends a "Do Not Track" signal. The bill also requires operators to disclose the data collection practices of certain third parties operating on the website or online service. Because this law affects every person or company that operates a website or online service that collects personally identifiable information from California

consumers, it impacts companies beyond California's borders. The law takes effect on January 1, 2014.

Background

"Do Not Track" (DNT) was originally proposed to provide an easy mechanism for consumers to opt out of online tracking. The Federal Trade Commission (FTC) initially endorsed the concept of a universal browser-based DNT signal in its 2010 preliminary staff report on privacy, *Protecting*

Continued on page 2...

IN THIS ISSUE

California Amends CalOPPA to Require Do-Not-Track DisclosuresPage 1-3

California's Social Media "Eraser" Bill Becomes LawPage 4-6

California Extends Security Breach Notification Requirements to Online Account CredentialsPage 7-8

Breach Notification: Timing Is EverythingPage 9-11

Barnes & Noble Dodges Suit over PIN Pad Data BreachPage 12-13

Illinois Federal Judge Dismisses Consumers' Data Collection Suit Against ISP WideOpen WestPage 14-15

¹http://leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB370.

² CA Bus. & Prof. Code §22575.

CALIFORNIA AMENDS CALOPPA . . . (continued from page 1)

Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (December 2010).³ In response, several browser vendors developed tools that consumers can use to signal that they do not want to be tracked. The browser signal does not technically prevent the tracking of information; rather, it communicates the DNT signal and the onus is on the operator of a commercial website or online service to respond to that signal, if it so chooses. Because the collection of data is necessary for basic functioning of the Internet, the challenge is interpreting what the signal means (i.e., when an operator sees the DNT

A.B. 370 imposes disclosure obligations by amending CalOPPA, which currently requires website operators that collect personally identifiable information to conspicuously post—and comply with—a privacy policy

signal, what data may it continue to collect and what uses of that data are permitted?). In 2011, the World Wide Web Consortium (W3C), a voluntary, collaborative body that sets technical standards for the Internet, formed a Tracking Protection Working Group to set standards for DNT. The group, which consists of industry members, advocacy groups, and academic experts, has suffered from internal dissension and turnovers in leadership, and as of yet has been unable to reach a consensus on how the DNT signal is to be interpreted.

³<http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>.

⁴<http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579>.

A.B. 370 imposes disclosure obligations by amending CalOPPA, which currently requires website operators that collect personally identifiable information (PII) to conspicuously post—and comply with—a privacy policy.⁴ CalOPPA further requires that the privacy policy identify the categories of PII that the operator collects, as well as the third parties with whom the operator shares the information.

The new bill includes two additional requirements. Under the new law, an operator also must:

1. “disclose how the operator responds to Web browser do not track signals or other mechanisms that provide consumers the ability to exercise choice regarding the collection of personally identifiable information about an individual consumer’s online activities over time and across third-party Web sites or online services, if the operator engages in that collection,” and
2. “disclose whether other parties may collect personally identifiable information about an individual consumer’s online activities over time and across different Web sites when a consumer uses the operator’s Web site or service.”

CalOPPA defines PII as “individually identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form,” including any of the following:

- Name
- Physical or email address
- Telephone or Social Security number

While A.B. 370 does not impose substantive provisions requiring companies to honor DNT signals or set standards regarding what honoring DNT entails, the bill is the California Legislature’s attempt to provide consumers with transparency, if not choice, regarding DNT

- Any other identifier that permits the physical or online contacting of a specific individual
- Information concerning a user that the website or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described in this section

Implications

While A.B. 370 does not impose substantive provisions requiring companies to honor DNT signals or set standards regarding what honoring DNT entails, the bill is the California Legislature’s attempt to provide consumers with transparency, if not choice, regarding DNT. Such transparency may have the effect of encouraging companies to honor DNT signals, as they may feel more pressure now that they have to explain their policies to consumers.

Do I Need to Comply, and How Do I Comply?

The new amendment requires operators of websites and other online services that collect PII about an individual's online activities over time and across third-party sites or services to disclose how they honor DNT signals or other mechanisms that provide consumers with choice regarding cross-site tracking.⁵ This disclosure requirement applies only to operators of online services that themselves collect such PII across sites; it does not affect those that only collect PII on their own sites.

California Attorney General Kamala Harris views CalOPPA's definition of PII to be sufficiently broad to encompass cross-site data linked to a device via a persistent identifier, even if the data is collected anonymously.⁶ Moreover, the legislative history of the amendment suggests that this is precisely the type of online tracking that the legislature intended to address.⁷ If challenged, a court may ultimately disagree with this expansive interpretation of CalOPPA.⁸ Nevertheless, companies will incur the risk of an enforcement action if they do not follow the statute with regard to the collection of persistent identifiers.

To comply with the law, operators first must determine whether and how they honor DNT

browser signals or alternative consumer choice mechanisms, if at all, and then must clearly communicate this to consumers through their privacy policy. While it isn't

Those who fail to comply with CalOPPA will be in violation of the statute if they do not post a compliant privacy policy within 30 days of being notified of noncompliance

clear whether the law requires operators to do more than state whether they honor the DNT signal or other choice mechanism, as a practical matter, companies should specify how they respond to the signal rather than simply assert that they honor it. Because there is no accepted definition of what it means to honor DNT, operators should exercise caution in the representations that they make. If an operator represents that it honors the DNT signal without a sufficient

explanation of what that entails (e.g., that it ceases to collect certain information, or continues to collect the same information but ceases to make certain uses of the data), the operator risks violating the statute or being subject to a claim for deception.

The new amendment also requires operators to disclose whether third parties may collect PII about a consumer's online activities over time and across different websites when a consumer uses the operator's website or service. This disclosure requirement applies to all websites and online services. Websites and online services that do not currently make such a disclosure will need to revise their privacy policies.

What Happens If I Don't Comply?


Those who fail to comply with CalOPPA will be in violation of the statute if they do not post a compliant privacy policy within 30 days of being notified of noncompliance. While CalOPPA does not provide for a private right of action, the California attorney general can bring enforcement actions under the law. Violations of CalOPPA may result in penalties of \$2,500 per violation. For apps, Attorney General Harris has asserted that each app download constitutes a violation.

⁵Although the law only refers to websites and other online services, California Attorney General Harris has taken the position that CalOPPA applies to mobile applications as well. See *Privacy on the Go: Recommendations for the Mobile Ecosystem* (January 10, 2013), available at http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf; See *People v. Delta Air Lines Inc.*, No. CGC 12-526741 (Cal. Super. Ct. Feb. 11, 2013) (dismissed on other grounds).

⁶*Privacy on the Go: Recommendations for the Mobile Ecosystem* (January 10, 2013), available at http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf (defining personally identifiable data 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. Included are user-entered data, as well as automatically collected data.")

⁷See, e.g., Senate Judiciary Analysis (June 24, 2013), available at <http://leginfo.legislature.ca.gov/faces/billHistoryClient.xhtml#>.

⁸In its defense of an enforcement action filed by Attorney General Kamala Harris's office for Delta's alleged failure to comply with CalOPPA, Delta argued that its app did not contact specific individuals and thus did not collect "personally identifiable data" under CalOPPA. Delta argued that "a piece of information collected from a consumer does not become PII simply because the State holds that opinion." Def. Delta Air Lines, Inc.'s Reply in Support of Demurrer at 9, *People v. Delta Air Lines Inc.*, No. CGC 12-526741 (Cal. Super. Ct. Feb. 11, 2013) (dismissed on other grounds).



Wilson Sonsini Goodrich & Rosati has a global network of experienced privacy attorneys with whom we have worked extensively. We can assist you with privacy issues in any country, interfacing with local counsel and coordinating the project on your behalf.

CALIFORNIA'S SOCIAL MEDIA "ERASER" BILL BECOMES LAW



Gerard Stegmaier
Of Counsel, Washington, D.C.
gstegmaier@wsgr.com



Emily Schlesinger
Associate, Seattle
eschlesinger@wsgr.com

The clock has begun ticking for operators of some websites, services, and applications to start thinking about how to enable minors to remove information they have posted online. Effective January 1, 2015, certain operators must comply with S.B. 568, commonly known as the "Eraser" bill, which makes California the first state in the country to require select

S.B. 568 is intended to protect teenagers from the potentially negative impact of content they regret having posted online, and to shield them from advertising and marketing efforts geared at selling minors products that could harm them

operators to allow minors to either personally remove or request and obtain removal of online content they have posted. S.B. 568 also prohibits the advertising and

marketing of specific categories of age-restricted products to minors.

S.B. 568 adds Chapter 22.1, entitled "Privacy Rights for California Minors in the Digital World," to the California Business & Professions Code. Section 22580 prohibits operators of websites, services, or applications "directed to minors" from marketing or advertising certain categories of products that minors would not legally be able to purchase, and prevents them from "knowingly" using, disclosing, or compiling minors' personal information for marketing or advertising, or allowing a third party to do so.¹ Section 22581 obligates these operators to establish a mechanism through which minors can either delete or request removal of online content. It also requires the provision of clear instructions about operators' removal process.

Affected businesses may see a surge in class action litigation, as claimants may seek injunctive relief and civil penalties of up to \$2,500 per violation.²

Aimed at Protecting California's Teenagers

S.B. 568 targets "operators" of an Internet website, online service, online application, or mobile application "directed to minors." The law also applies to operators with "actual knowledge" that a minor is using its site, service, or application. Under the law, "minors" are California residents under age 18.³ "Operators" are defined as "any person or entity that owns an Internet Web site, online service, online application, or mobile application," not including any "third party that operates, hosts, or manages, but does not own, an Internet Web site, online service, online application, or mobile application on the owner's behalf or processes information on the owner's

behalf."⁴ "Directed to minors" is broadly defined to mean "created primarily for the purpose of reaching an audience that is predominantly comprised of minors, and is not intended for a more general audience comprised of adults."⁵

As the California legislature has repeatedly stressed, S.B. 568 is intended to protect teenagers from the potentially negative impact of content they regret having posted online, and to shield them from advertising and marketing efforts geared at selling minors products that could harm them. Legislators and lobbyists supporting the bill argue that its protective features simply expand on the safeguards federal law already affords children under 13 and their parents in the Children's Online Privacy Protection Act (COPPA). For instance, the "directed to minors" language mirrors the language in COPPA targeting sites "directed to children."⁶ However, it is unquestionably more difficult to draw a bright line between content aimed at teenagers and content focused on an older audience than it is to distinguish between sites geared toward children and sites meant for adults. Thus, where the lines drawn by COPPA are fairly clear cut in many respects, S.B. 568 could potentially apply to *any* online site, service, or application popular with teenagers and young adults, regardless of the intended audience. In addition, although COPPA is limited strictly to a child's "personal information," S.B. 568 sweeps much more broadly, applying to *all* "content and information" submitted by a minor.

Section 22581: The "Eraser" Law

Major sites, such as Facebook and Twitter, already allow users to remove content themselves, but Section 22581 aims to apply that privacy standard across the digital world. Under the statute, when a registered

¹ See Cal. Bus. & Prof. Code §§ 22580(b)(1), (c) (eff. Jan. 1, 2015).

² *Id.* at § 17200, *et seq.*

³ *Id.* at § 22580(d).

⁴ *Id.* at § 22580(e).

⁵ *Id.* at § 22580(e).

⁶ 15 U.S.C. § 6501(10)(a) (defining "directed to children").

Although COPPA is limited strictly to a child's "personal information," S.B. 568 sweeps much more broadly, applying to all "content and information" submitted by a minor

user who is a California resident under age 18 posts content or information on a regulated website, service, or application, and later wants it deleted, an operator must either allow the minor to remove the content or, "if the operator prefers," request and obtain the content's removal itself.⁷ The law further requires operators to notify minors of their right to deletion by providing "clear instructions" of the operator's chosen method of removal, while also explaining that such deletion "does not ensure complete or comprehensive removal of the content or information."⁸ In particular, an operator is not required to delete submitted content from its servers, and need not take down posts from other users who republish the content submitted by the minor.

Notable Exceptions

Section 22581 lists several circumstances in which the law is inapplicable, including situations in which:

- other state or federal law requires that the site or service maintain the content or information;⁹
- the content or information in question is submitted by a third party other than the minor;¹⁰
- the content is republished or resubmitted by a third party;¹¹
- the operator anonymizes the content by ensuring that it cannot be used to individually identify the minor;¹² or
- the minor "has received compensation or other consideration" for providing the content (though "consideration" is not defined).¹³

Moreover, although the law requires operators' removal of content from public sites, it expressly allows their retention of any related data on their servers.¹⁴

Section 22580: Restrictions on Marketing to Minors

In addition to providing a virtual "eraser" for California minors, S.B. 568 limits the types of goods and services that can be advertised or marketed to minors online.¹⁵ Section 22580 provides that operators of websites, online services, online applications, or mobile applications "directed to minors" shall not market or advertise any of the listed prohibited products,¹⁶ which include alcohol, firearms, tanning services, and tobacco, as well as numerous other potentially harmful or destructive products.¹⁷ "Marketing and advertising" is specifically defined as "in exchange for monetary compensation, to make a communication to one or more individuals, or to arrange for the

dissemination to the public of a communication, about a product or service, the primary purpose of which is to encourage recipients of the communication to purchase or use the product or service."¹⁸ The law also prohibits operators of sites, services, and applications from marketing or advertising a product or service to a minor if they are targeting the minor based on his or her personally identifiable information, including "the minor's profile, activity, address," or "IP address and product identification numbers for the operation of a service."¹⁹

As is the case with Section 22581, under Section 22580's vague provision defining what it means to be "directed to minors,"²⁰ any operators whose sites, services, or applications are popular with minors would be uncertain about their obligations under the law. Also, the "marketing and advertising restrictions" do not apply to "incidental placement of products or services embedded in content" if it is not distributed "primarily for the purposes of marketing and advertising" those products.²¹ But the phrases "incidental placement" and "primarily for the purposes of marketing and advertising" leave significant room for interpretation, making it even harder for an operator to know when it may be crossing a line.

Notably, Section 22580 also specifies that operators will be "deemed in compliance" as long as they "take reasonable actions in good faith designed to avoid" marketing or advertising in ways that would violate the law.²² Although the statute states that it "shall not be construed to require" operators to "collect or retain age information" about its users,²³ "good faith" would require operators to find a reliable way to distinguish their registered users on the

⁷ *Id.* at § 22581(a)(1).

⁸ *Id.* at § 22581(a)(4).

⁹ Cal. Bus. & Prof. Code § 22581(b)(1)

¹⁰ *Id.* at § 22581(2).

¹¹ *Id.*

¹² *Id.* at §§ 22581(b)(4) & (b)(5).

¹³ *Id.*

¹⁴ *Id.* at § 22581(d).

¹⁵ *See id.* at § 22580.

¹⁶ *Id.* at §§ 22580(a) & (b)(1).

¹⁷ *Id.* at § 22581(i).

¹⁸ *Id.* at § 22580(k).

¹⁹ *Id.* at § 22580(b)(1).

²⁰ *Id.* at § 22580(e).

²¹ *Id.* at § 22580(j).

²² *Id.* at § 22580(b)(2).

²³ *Id.* at § 22580(g).

Continued on page 6...

basis of age, effectively making the collection of at least some of users' personal information unavoidable.

Criticism and Challenges

The law is already under fire for its myriad ambiguities. In addition to some of the uncertainties laid out above, S.B. 568 does not specify what qualifies as "content and information," nor does it clarify whether "personal information" would include persistent identifiers, indicate a method of deletion, or include details about how

By forcing operators to remove any and all "content or information" upon a minor's request, the law disregards operators' First Amendment interests, and may even amount to compelled speech

operators should receive and evaluate minors' requests for removal. Additionally, it does not explain when a website, service, or app is construed as "created primarily for the purpose of reaching"²⁴ teens rather than adults, or discuss how "actual knowledge" would be obtained by an online service directed to a general audience, especially given that the law does not require the collection of users' age information.²⁵ The law is also silent about whether individuals over 18 could seek to delete years-old content that they posted when they were still minors, or whether the right to request

deletion of content expires when the minor reaches age 18.

Other critics have argued that the law ignores important constitutional concerns. For instance, by forcing operators to remove any and all "content or information" upon a minor's request, the law disregards operators' First Amendment interests, and may even amount to compelled speech. Further, because marketing or advertising information is considered protected speech under the First Amendment, minors have a right to receive such information. Finally, the law may be subject to viable challenges on dormant commerce clause grounds since websites and applications typically cannot recognize or honor California's state borders.

Ways to Ensure Compliance by January 1, 2015

Despite the evident lack of clarity, violations of either section of S.B. 568 could bring stiff penalties. However, the following actions may help operators of sites, services, or applications appealing to an audience that includes a large number of minors—as well as advertisers who know that they are marketing or advertising on such sites, services, or applications—to ensure compliance by January 1, 2015:

- Develop a full understanding of the types of any information the site, service, or application collects, how it is stored, and where it is stored.
- Compare and evaluate the trade-offs between using automated options that would allow minors the ability to delete content themselves, and employing methods that would require the operator itself to field and execute deletion requests.
- Consider how long it may take to separate out a minor's information and potentially delete it, and the time it may

Despite the evident lack of clarity, violations of either section of S.B. 568 could bring stiff penalties

take to allow for or carry out a request for deletion.

- Develop internal and external policies to respond to minors' requests for deletion, and any necessary steps to complete the removal process.
- Work with counsel to draft a policy clearly instructing registered users about their rights under the law, as well as the website, service, or application's chosen deletion process, and determine how best to publicize that notice.
- To try to eliminate the applicability of the deletion requirement, operators should consider anonymizing the content or information posted by minors who are registered users so that a minor could not be individually identified, or offering minors nominal compensation or other consideration in exchange for their content.
- Sites, services, and applications selling the identified prohibited goods or services should ensure that any marketing or advertising practices they use target only adults, and that they adequately notify all third-party advertisers and marketers that they must plan accordingly.

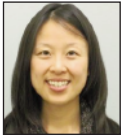
²⁴ *Id.*

²⁵ *Id.* at § 22580(g) & 22581(e).

CALIFORNIA EXTENDS SECURITY BREACH NOTIFICATION REQUIREMENTS TO ONLINE ACCOUNT CREDENTIALS



Matthew Staples
Associate, Seattle
mstaples@wsgr.com



Sharon Lee
Associate, Palo Alto
shlee@wsgr.com

California, which enacted the pioneering security breach notification law in 2002, again has taken the lead in security breach notification legislation. In an effort to protect consumers against unauthorized access to their online accounts, California has extended its security breach notification law to cover individuals' online account credentials (i.e., a user name or email address, in combination with a password or security question and answer, that would permit access to an online account) in amendments that will take effect on January 1, 2014.¹ This article discusses California's existing security breach notification obligations, as well as the changes provided for in these amendments.

California's Existing Security Breach Notification Law

Prior to its most recent amendments,² California's security breach notification statute covered "personal information," defined as an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- (1) Social Security number;

Under the law, any person or business that owns or licenses computerized data that includes personal information belonging to a California resident must notify that California resident in the event his or her personal information is, or is reasonably believed to be, acquired by an unauthorized person

- (2) driver's license number or California identification card number;
- (3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;
- (4) medical information;³ or
- (5) health insurance information.⁴

Under the law, any person or business that owns or licenses computerized data that

includes personal information belonging to a California resident must notify that California resident in the event his or her personal information is, or is reasonably believed to be, acquired by an unauthorized person.⁵ Additionally, any entity maintaining computerized data that is not owned by that person or business and that includes personal information of a California resident must notify the owner or licensee of that personal information upon discovering any such event.⁶ All notifications under the law must be in plain language and must include the following details:

- (1) the name and contact information of the reporting person or business;
- (2) a list of the types of personal information that were or are reasonably believed to have been subject to the breach;
- (3) if possible to determine at the time notice is provided, (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred;
- (4) the date of the notification;
- (5) whether notification was delayed by a law enforcement investigation, if possible to determine at the time notice is provided;
- (6) a general description of the breach incident, if possible to determine at the time notice is provided; and
- (7) the toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a Social Security number or a driver's license or California identification card number.⁷

¹The legislation, Senate Bill No. 46 (SB46), applies to Sections 1798.29 and 1798.82 of the California Civil Code. See http://leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB46. Section 1798.29 applies to California state agencies, while Section 1798.82 applies to private persons and businesses. This article focuses on the amendments to Section 1798.82.

²California's security breach notification legislation has been amended on two previous occasions, as discussed in WSGR Alerts available at http://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/clientalert_securitybreach.htm and <http://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert-security-breach-notification.htm>.

³"Medical information" is defined as "any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional." Cal. Civ. Code § 1798.82(h).

⁴"Health insurance information" is defined as "an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records." Cal. Civ. Code § 1798.82(h).

⁵Cal. Civ. Code § 1798.82(a).

⁶Cal. Civ. Code § 1798.82(b).

⁷The notification must include the toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a Social Security number or California identification card number. Cal. Civ. Code § 1798.82(d).

Continued on page 8...

CALIFORNIA EXTENDS SECURITY BREACH NOTIFICATION . . . (continued from page 7)

California's security breach notification law has permitted notification by one of the following methods:

- (1) written notice;
- (2) electronic notice;⁹ or
- (3) if the person or business demonstrates that the cost of providing notice would exceed \$250,000, that the affected class of persons exceeds 500,000, or that the entity does not have sufficient contact information, the person or business may provide substitute notice consisting of email notice (when the person or business has an email address for the affected person), conspicuous notice on the person or business's website (if one exists), and notification to major statewide media.⁹

Recent Amendments Covering Online Account Credentials

California's recent amendments to its security breach notification law expand the set of "personal information" covered by the law to online account credentials—that is, a user name or email address, in combination with a password or security question and answer that would permit access to an online account.

The amendments also provide entities with an optional method to provide security breach notification if the breach does not involve any personal information, as defined by the law, of California residents other than online account credentials. In such an event, a person or business may elect to provide required security breach notification under the law in a form that directs the person whose online credentials were breached to promptly change his or her password and security question or security answer, as applicable, or to take other steps appropriate to protect that person's online account with that entity and all other online accounts for which that person uses the same credentials.

This notice method is optional, and a person or business required to provide notification instead may choose to use one of the other notice methods permitted under the law.

The amended statute also provides that if the online account credentials that were breached were for an email account furnished by the person or business that suffered the breach, that person or business must not provide notice of the breach to the compromised email account. Rather, that person or business may use one of the other notification methods permitted under the law, or may provide clear and conspicuous notice delivered to the affected California resident online when that resident is connected to his or her email account from an IP address or online location from which that person or business knows the resident customarily accesses his or her email account.

Implications

California's amendments may have a significant impact on licensees and holders of online account credentials belonging to California residents. Any widely available online service will have California users, which means that nearly all providers of online services will need to be cognizant of California's amendments taking effect on January 1, 2014.

Additionally, it is possible that other states may follow California's lead and extend the scope of their own security breach notification statutes. When California passed its pioneering state security breach notification legislation in 2002, dozens of states followed suit with similar laws in the years thereafter. By the end of the decade, nearly all states, as well as the District of Columbia, Puerto Rico, and the U.S. Virgin Islands, had enacted legislation providing for required security breach notification. States following California's lead on this latest

development would further complicate an already complex patchwork of state laws that must be considered by entities that suffer data security incidents. In addition,

Any widely available online service will have California users, which means that nearly all providers of online services will need to be cognizant of California's amendments taking effect on January 1, 2014

California's amendments, and any similar amendments by other states, may provide further impetus for federal data breach notification legislation. Under some proposals, such federal legislation would preempt state law and help simplify the process of notifying consumers in the event of a data security breach. Federal data breach notification legislation has been proposed on several occasions in recent years, but has yet to be passed.

Only time will tell whether other states will follow California's lead on this issue and whether federal legislation will garner sufficient support for passage. In the interim, all entities maintaining online account credentials of California residents should be aware of this expansion of California's security breach notification statute and should consider appropriate modifications to their data security incident-handling procedures.

⁹The electronic notice must be consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code. Cal. Civ. Code § 1798.82(j)(2).

⁹Cal. Civ. Code § 1798.82(j).

BREACH NOTIFICATION: TIMING IS EVERYTHING



Wendell Bartnick

Associate, Washington, D.C.
wbartnick@wsgr.com



Joe Molosky

Associate, Washington, D.C.
jmolosky@wsgr.com

A data security incident can be daunting for an organization, quickly spurring it into full-blown crisis mode. Once an incident is discovered, IT and security personnel may work around the clock to attempt to identify and fix security vulnerabilities, assess and mitigate any damage from the incident, and report their findings and efforts to senior management. The organization's attorneys may review the incident from a legal risk perspective and engage experienced outside counsel and forensics firms to better assess how the organization should respond to the incident in light of its legal and contractual obligations. The communications and customer service teams may need to respond to customer inquiries about system performance and strange system behavior, while IT personnel are following emergency protocols to attempt to strengthen system security and investigate the incident. In addition, the communications team may be involved in any required data breach notifications. Finally, senior management will need to analyze technical details and legal advice to make organizational decisions that may significantly affect the organization's customers, reputation, and bottom line.

Organizations may be unaware that state breach notification statutes create time pressure following the discovery of an incident. Virtually every state in the United States has a breach notification statute. Such statutes define the term "breach" and specify who should be notified in the event

of a breach, when such notifications should be made, and what details must be included in the notifications. Typically, state regulators and/or affected individuals have the ability to sue organizations that fail to comply with the statutes.

Most state statutes require organizations to notify affected individuals and, in some cases, state regulators in the "most expedient time possible" and "without unreasonable delay" after becoming aware of a breach. However, several states have prescribed specific timing requirements, including Florida, Ohio, and Wisconsin (notice to affected individuals within 45 days),¹ as well as Vermont (notice to the state attorney general within 14 days and affected individuals within 45 days).²

Given the lack of success that plaintiffs have had in data breach lawsuits to date, plaintiffs may begin using the additional theory of notification delays in class actions more frequently

Until recently, organizations victimized by an incident have not been subject to much litigation with claims from notification delays. Instead, regulators and affected individuals have focused on the effects of the breaches themselves. However, given the

lack of success that plaintiffs have had in data breach lawsuits to date, plaintiffs may begin using the additional theory of notification delays in class actions more frequently. State regulators also may enforce their statutes more aggressively. Three recent cases demonstrate that organizations should be aware of their breach notification requirements—particularly the timing requirements—and be prepared to comply with them.

Notification Delay Lawsuits

Barnes & Noble (B&N)

A group of criminals stole customer credit and debit card information from sixty-three B&N stores across nine states. The criminals tampered with card readers located at the stores to capture the information. Six weeks after discovering the malicious activity, B&N announced the breach to the media and posted a notice on its website. B&N allegedly did not notify any of the affected customers directly, because it did not know which customers were affected. Customers brought a class action against B&N asserting several claims based on a failure to properly safeguard credit and debit card information. They also claimed that B&N violated Illinois's breach notification statute due to its "untimely and inadequate notification of the security breach[.]"³

The court dismissed the customers' claims regarding notification delays, as well as all of their other claims. First, the customers claimed that the delay or inadequacy of the notification increased their risk of identity theft or fraud. The court rejected this argument, relying on a recent Supreme Court case holding that for plaintiffs to have standing to bring a claim, they must have been actually harmed or "a threatened injury must be certainly impending."⁴ The court

¹ Fla. Stat. §817.5681(1)(b); Ohio Rev. Code § 1349.19(B)(2); 9 V.S.A. § 2435(b)(1)&(3)(A)(i); Wis. Stat. § 134.98(3)(a).

² 9 V.S.A. § 2435(b)(1)&(3)(A)(i).

³ *In re Barnes & Noble Pin Pad*, No. 12-cv-8617, 2013 U.S. Dist. LEXIS 125730, at *4 (N.D. Ill. Sept. 3, 2013).

⁴ *Clapper v. Amnesty Int'l USA*, 568 U.S. ____, 133 S. Ct. 1138, 1143 (2013). Please see our *Eye on Privacy* article discussing the case at <http://www.wsgr.com/publications/PDFSearch/eye-on-privacy/May2013/index.html#4>.

Continued on page 10...

BREACH NOTIFICATION: TIMING IS EVERYTHING *(continued from page 9)*

held that “merely alleging injury from an increased risk of identity theft or fraud is insufficient to establish standing,”⁵ because the injury was not certainly impending.

Second, the customers claimed that a violation of the Illinois breach notification statute by itself constituted actual injury sufficient to convey standing. The customers argued that B&N violated the statute through its failure to provide direct notice. The court rejected this argument due to the clear language in the statute. The Illinois breach notification statute states that “any person who suffers actual damages as a result of a violation” may sue under the statute.⁶ Moreover, a violation of a statute alone, without an injury, generally is insufficient to confer standing.⁷ The court concluded that the customers failed to allege actual damages, so they could not bring a claim under the statute.

After rejecting all the other claims, the court dismissed the lawsuit.⁸ B&N allegedly did not provide direct notice to individuals following a data breach. Yet, potentially affected individuals were unable to successfully sue B&N for any violations of the Illinois breach notification statute.

Natural Provisions

Natural Provisions, a small health food store in Vermont, faced an investigation by state regulators after criminals stole customer credit card information from the company. After the police department notified Natural Provisions of the possible breach, the company allegedly did not take any action to fix the vulnerability for more than a month. The store also allegedly did not notify its customers or the Vermont attorney general within 45 days of the breach’s discovery.

The Vermont attorney general concluded that these actions violated Vermont’s breach notification statute, which requires notifying affected individuals within 45 days and notifying the Vermont attorney general within 14 days of the discovery of a breach.⁹ State regulators may not face the same standing requirements as plaintiffs in class actions, so their investigations and lawsuits seem to be more effective at present. Natural Provisions reached a settlement with

Organizations should provide notifications only after careful consideration of the incident and the applicable breach notification statutes

the Vermont attorney general under which it agreed to pay a civil penalty, implement and maintain a comprehensive information security program, and implement specific data security safeguards.¹⁰ In this case, a company’s failure to comply with the breach notification statute resulted in successful government enforcement.

Citibank

Citibank recently reached settlements with attorneys general from California and Connecticut due to delayed breach notification. Citibank’s online banking system had a vulnerability that allowed criminals to access account information for more than

360,000 customers. Citibank allegedly knew about the vulnerability and failed to patch it for almost three years, and allegedly did not finish notifying affected consumers until 32 days after discovering the breach. The Connecticut attorney general determined that the timing of the notice was not without “unreasonable delay,” as required by Connecticut’s breach notification statute.¹¹ Likewise, the California attorney general concluded that Citibank “failed to expediently notify its California resident customers.”¹² In both settlements, Citibank agreed to pay a civil penalty and provide free credit monitoring services to the affected residents.

Data Breach Response

The above cases demonstrate that state regulators and affected individuals are becoming more aggressive in ensuring that organizations provide breach notifications in a timely manner and within any legally mandated timelines. It appears state regulators may currently be more successful at enforcing the statutes than private citizens due to issues of standing. However, both regulators and affected individuals remain sources of costly litigation. Organizations should not take these cases to mean that they should hurriedly notify affected individuals in the event of any security incident, though. On the contrary, organizations should provide notifications only after careful consideration of the incident and the applicable breach notification statutes.

Typically, and with good reason, organizations will not provide notifications unless they are required to do so. Such notifications are costly. The Ponemon Institute’s *2013 Cost of a Data Breach Study* found that, on average, a breach costs \$188

⁵ *In re Barnes & Noble Pin Pad*, 2013 U.S. Dist. LEXIS at *8.

⁶ 815 ILCS 505/10a.

⁷ *In re Barnes & Noble Pin Pad*, 2013 U.S. Dist. LEXIS at *9.

⁸ See a more detailed analysis of the B&N case in an article in this issue of *Eye on Privacy* entitled “Barnes & Noble Dodges Suit over PIN Pad Data Breach.”

⁹ V.S.A. § 2435(b)(1)&(3)(A)(i).

¹⁰ Assurance of Discontinuance at 3, *In re: Natural Provisions, Inc.*, No. 522-9-13-wncv (Vt. Super. Ct. Sept. 5, 2013).

¹¹ Complaint at 4, *Connecticut v. Citibank, N.A.*, No. HHD-CV12-6044810-S (Conn. Super. Ct. Aug. 29, 2013); CT Gen. Stat. § 36a-701b(b).

¹² Complaint at 4, *People of California v. Citibank, N.A.*, No. RG13693591 (Cal. Super. Ct. Aug. 29, 2013); Cal. Bus. & Prof. Code § 1798.82.

BREACH NOTIFICATION: TIMING IS EVERYTHING *(continued from page 10)*

per record.¹³ According to the study, the average breach affects 28,765 records, leading to costs exceeding \$5 million.¹⁴ The Ponemon Institute estimates that the average costs of notification alone amount to more than \$550,000.¹⁵ The factors considered by the study include the strength of the organization's policies and procedures, the type of breach, and the quality of staff involved in the remediation.¹⁶ Of the seven factors noted in the study, one factor fully under the organization's control after the incident directly affected the cost of a breach: the speed of notification. The study also found that if the organization notified data breach victims within 30 days of discovering the breach, the cost of the breach increased by \$37 per record, or over \$1 million on average.¹⁷

Senior management inexperienced with breaches might believe that once a security breach is discovered, notification is inevitable and should be made, especially with the specter of breach notification statute violations. However, the Ponemon Institute's numbers show that organizations should not give in to the temptation of notifying affected individuals too quickly without sufficient understanding of the incident.

Experience shows that many security incidents look much worse initially than they do after a thorough forensic review of the incident. Therefore, it is likely in an organization's best interest to wait until it has thoroughly investigated an incident before it concludes that a breach has occurred. In addition, some breach

notification statutes have a narrow definition of "breach" that may not include the security incident that occurred. For example, some statutes state that a breach occurs only if data is "accessed" or "acquired" by an unauthorized person. Access or acquisition may not have occurred during an incident, and this is only apparent after thorough investigation. Most states do not require notification when encrypted data was involved. Therefore, properly analyzing the circumstances of the incident under the applicable statutes is an important step to take before notifying regulators and affected individuals.

Organizations will likely never have all of the knowledge they want before they need to make the decision of whether to notify regulators and affected individuals. So, how can organizations properly deal with security incidents quickly, but with good judgment? One effective method is for organizations to draft, implement, and regularly test an incident response policy before an incident occurs. The Ponemon Institute's research shows that having a quality incident response plan in place at the time of the breach is worth \$42 per record, or over \$1.2 million on average. Incident response policies tend to be more effective if they are drafted and implemented with the help of outside experts. Incident response policies include detailed instructions for:

- identifying suspected incidents;
- responding to suspected security incidents from an IT perspective;

- bringing in outside legal and forensics experts;
- mitigating any damage from a security incident;
- documenting the security incident;
- reporting the response efforts;
- assessing the legal and business risks from a security incident; and
- determining any breach notification obligations under applicable law or contracts.

Having a quality incident response plan in place at the time of the breach is worth \$42 per record, or over \$1.2 million on average

Following such a policy helps ensure that the organization methodically takes the proper steps during a crisis situation once an incident occurs. In doing so, organizations will be able to more quickly assess the incident so that they can provide notice in a timely, cost-effective manner when required.

¹³ *2013 Cost of a Data Breach Study: United States*, Ponemon Institute (May 2013).

¹⁴ *Id.*

¹⁵ For estimating the notification costs, the Ponemon Institute considered the costs of creating contact databases, "determination of all regulatory requirements, engagement of outside experts, postal expenditures, secondary contacts to mail or email bounce-backs, and inbound communication set-up."

¹⁶ *Id.* at 8.

¹⁷ *Id.*

Tip

Are you familiar with HIPAA risk assessments? If not, don't forget that the new HIPAA rule—which went into effect on September 23—imposes new requirements on many businesses that handle health information.

BARNES & NOBLE DODGES SUIT OVER PIN PAD DATA BREACH



Wendell Bartnick

Associate, Washington, D.C.
wbartnick@wsgr.com

A trial court in the Seventh Circuit recently dismissed a data breach class action case against Barnes & Noble (B&N) due to the plaintiffs' failure to allege actual or imminent injuries.¹ This is one of the first data breach cases following the U.S. Supreme Court's recent decision about pleading actual damages in *Clapper v. Amnesty Int'l USA*.² The trial court relied on *Clapper* to dismiss the case rather than follow Seventh Circuit precedent, which may have allowed the case to continue. *Clapper* appears to provide defendants with a strong defense in data breach cases.

Barnes & Noble Data Breach

According to the complaint, B&N was the victim of criminal actors hacking into the credit and debit card readers at several of its stores. The hackers collected credit and debit card data from B&N customers. Approximately six weeks after the breach discovery, B&N notified the media and posted notice on its website. The company allegedly did not provide direct notice to customers because it did not know which customers were affected.

The Plaintiffs' Claims

The plaintiffs sued on behalf of all customers who made in-store credit and debit card purchases during the time period the hackers may have had unauthorized access to the card readers. The plaintiffs made the following claims:

- B&N allegedly breached implied contracts formed with its customers when it collected financial information from them. The plaintiffs allege that the contracts require B&N to reasonably safeguard this information.
- B&N allegedly violated federal and state consumer protection laws when it failed to properly implement adequate, commercially reasonable measures to protect financial information.
- B&N allegedly violated the state breach notification statute in Illinois when it failed to immediately notify affected customers of the breach.
- the inaccessibility to the credit card of one plaintiff whose card was cancelled following an unauthorized charge;
- inherent harm from invasion of privacy;
- inherent harm from improper disclosure of personal information; and
- overpayment for products, which incorporated the costs of data security.

The plaintiffs asserted a series of harms resulting from B&N's alleged activities. They alleged that they made purchases at the B&N stores affected by the breach during the time the breach occurred and that therefore the court should infer that their financial information was stolen as part of the breach. The plaintiffs alleged that as a result they were subject to:

- increased risk of identity theft, fraud, and other misuse;
- out-of-pocket costs and the value of time for identity theft prevention and replacement of cards and PIN numbers;
- inherent injuries from a violation of a breach notification statute;
- deprivation of the value of their personal information;
- anxiety;

Federal Court Jurisdiction

Federal courts have jurisdiction over cases only when the plaintiff has standing to sue. Therefore, courts will dismiss a case when the plaintiff does not meet the requirements for standing. For standing to exist, the plaintiffs' injury must be "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling."³

Courts have not reached consensus on whether the frequently alleged injuries from data breaches meet standing requirements. Both the Seventh Circuit and the Ninth Circuit have concluded that an increased risk of identity theft caused by a data breach is sufficient to confer standing.⁴ Other courts have not found standing in data breach cases.⁵ The Supreme Court's recent decision in *Clapper* calls into question the precedent in the Seventh and Ninth Circuits, as it clarified what an "actual or imminent" injury is.

In *Clapper*, the Supreme Court clarified that to find standing based on a threat of future harm, the "threatened injury must be *certainly impending* to constitute injury in

¹ *In re Barnes & Noble Pin Pad*, No. 12-cv-8617, 2013 U.S. Dist. LEXIS 125730 (N.D. Ill. Sept. 3, 2013).

² *Clapper v. Amnesty Int'l USA*, 568 U.S. ____, 133 S. Ct. 1138 (2013). See the *Eye on Privacy* article discussing *Clapper v. Amnesty Int'l USA* at <http://www.wsgr.com/publications/PDFSearch/eye-on-privacy/May2013/index.html#4>.

³ *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. ____, 130 S.Ct. 2743, 2752 (2010).

⁴ *Krottner v. Starbucks Corp.*, Nos. 09-35823 and 35824 (9th Cir., Dec. 14, 2010); *Pisciotta v. Old National Bancorp*, 499 F.3d 629, 634 (7th Cir. 2007). See the WSGR Alert discussing the *Krottner* case in the Ninth Circuit at http://www.wsgr.com/wsgr/Display.aspx?SectionName=publications/pdfsearch/wsgralert_Krottner_v_Starbucks.htm.

⁵ *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011); *Whitaker v. Health Net of California, Inc.*, No. CIV S-11-0910 KJMDAD, 2012 WL 174961, at *2 (E.D. Cal. Jan. 20, 2012); *Low v. LinkedIn Corp.*, No. 11-CV-01468-LHK, 2011 WL 5509848, at *4 (N.D. Cal. Nov. 11, 2011).

fact.” Allegations of possible future injury are inadequate. The Supreme Court also stated that it has found standing based on the existence of a “substantial risk” of future injury that reasonably prompts a plaintiff to incur costs to avoid or mitigate that harm.

The Supreme Court’s recent decision in *Clapper* calls into question the precedent in the Seventh and Ninth Circuits, as it clarified what an “actual or imminent” injury is

However, plaintiffs “cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.” Plaintiffs frequently have been unable to successfully allege that harm is “certainly impending” following a data breach. The case against B&N was no different.

Federal Court Grants Barnes & Noble’s Motion to Dismiss

B&N filed a motion to dismiss, alleging that the plaintiffs did not have standing. The court agreed and dismissed the case, concluding that none of the alleged injuries claimed by the plaintiffs constituted actual or imminent injury sufficient to confer standing.

General Increased Risk of Identity Theft Is Not an Injury Sufficient for Standing. Relying on *Clapper*, the court concluded that

an increased risk of identity theft or fraud was insufficient to establish standing, because the plaintiffs failed to plead that they suffered a “certainly impending” injury or a “substantial risk” of an injury. Seventh Circuit precedent indicated that increased risk of identity theft or fraud could be sufficient for standing purposes, but the court relied on the Supreme Court case to hold otherwise. Likewise, the court concluded that the cost and time spent to mitigate any increased risk of identity theft are insufficient injuries when harm is not imminent.

Notification Delays Are Not Injuries Sufficient for Standing Without Actual Injuries. The court held that delays in notifying affected customers, even when the delays may have violated the Illinois breach notification statute, are not enough to establish standing without actual resulting injuries. The Illinois breach notification statute explicitly requires “actual injury” before affected individuals have a claim, and a statutory violation alone is generally not enough to confer standing.

Deprivation of Value of Personal Information Is Not an Injury Sufficient for Standing Without Allegations that Personal Information Could Be Sold for Value. The court rejected the claims that the data breach deprived the plaintiffs of the value of their personal information. The court stated that the plaintiffs must allege that they sold or could sell their personal information for value.

General Anxiety from a Data Breach Is Not an Injury Sufficient for Standing. The court determined that anxiety and emotional distress are insufficient to establish standing, especially where, as in this case, there is no imminent threat the information will be used in a malicious way.

Lag Time in Receiving Replacement Credit Card Is Not an Injury Sufficient for Standing. The court concluded that a time lag in

receiving a replacement credit card following a fraudulent charge is not an actual injury. Instead, the court stated that plaintiffs must have had an unreimbursed charge on the credit card to suffer an actual injury. Here, the plaintiff did not have any unreimbursed charges.

Plaintiffs Failed to Show Their Data Was Compromised. The court also denied the claims for improper disclosure of personal information and invasion of privacy. It refused to make the inference that the plaintiffs’ data was compromised as part of the breach. The court explained that making a purchase from a store that had a data breach is too tenuous to support a reasonable inference that the plaintiffs’ information was involved. Ultimately B&N benefited from its inability to accurately determine which customers were affected, because the plaintiffs were unable to plead that their data was in fact compromised.

Plaintiffs Failed to Show They Paid Higher Prices to Pay for B&N’s Data Security. The court concluded that the plaintiffs failed to allege that they paid higher prices at B&N when they pay with credit or debit cards to account for data security. Therefore, there was no proper allegation that the plaintiffs overpaid for B&N goods to pay for data security measures that did not prevent this breach.

Conclusion

The dismissal of the *B&N* case shows that the recent Supreme Court ruling in *Clapper* appears to be a strong defense for data breach defendants. In the *B&N* case, the trial court seemed to ignore Seventh Circuit precedent to dismiss the case. Time will tell whether the Seventh and Ninth Circuits will attempt to distinguish *Clapper* in data breach cases, and whether plaintiffs will be able to successfully plead that an injury is “certainly impending” following data breaches.

ILLINOIS FEDERAL JUDGE DISMISSES CONSUMERS' DATA COLLECTION SUIT AGAINST ISP WIDEOPEN WEST



Emily Schlesinger
Associate, Seattle
eschlesinger@wsgr.com

On September 27, 2013, Illinois federal judge Edmond Chang ruled that Internet service provider (ISP) WideOpen West Finance LLC (WOW) did not violate privacy laws by allowing third-party advertising company NebuAd, Inc. to gather information concerning the websites visited by WOW customers.¹ Judge Chang held that a company does not violate the Electronic Communications Privacy Act (ECPA)² when it allows a third party to access users' anonymous data but does not itself acquire the contents of that data. The decision also reaffirmed the principle that a company does not violate the ECPA if it accesses the contents of Internet transmissions to which it already had access in the ordinary course of its business.

The decision is noteworthy for online advertisers, advertising firms, web publishers, and website hosts because it suggests significant limitations on the potential liability of such companies for violations of the ECPA committed by third-party business partners.

Litigation Background

The parties' dispute had raged for several years. In 2007 and 2008, WOW and several other small to mid-sized ISPs across the

country partnered with NebuAd to license and install NebuAd devices inside each of their broadband network facility locations. According to the named plaintiffs, two WOW customers, in exchange for monthly payments from NebuAd, WOW diverted all aspects of its customers' Internet traffic to the devices, and allowed NebuAd to access

In 2009, a number of plaintiffs sued WOW, NebuAd, and five other ISPs that had partnered with NebuAd in federal district courts across the country, making similar allegations.³ All of the ISPs have fought the claims, but now defunct NebuAd settled the litigation in 2011 for \$2.4 million. The WOW decision follows the dismissals of all but one of the ISP suits.

The decision is noteworthy for online advertisers, advertising firms, web publishers, and website hosts because it suggests significant limitations on the potential liability of such companies for violations of the ECPA committed by third-party business partners

and analyze the information to serve customers with targeted advertisements without their knowledge or consent.

Plaintiffs' Claims Against WOW

The plaintiffs alleged that WOW improperly intercepted their communications relating to personal and sensitive matters by capturing those communications, which NebuAd then scraped for content such as search queries and page requests for health and financial information, visits to political and religious websites, and travel plans to use in its targeted advertising efforts.⁴ The plaintiffs also claimed that they never received notice of the nature and dimensions of WOW's partnership with NebuAd, and never gave their consent.⁵

The plaintiffs initially brought common law intrusion, trespass, and unjust enrichment claims, as well as claims that WOW had violated the Computer Fraud and Abuse Act⁶ and the Illinois Criminal Code. Everything but the ECPA claims was knocked out in March 2012, when the court found them subject to arbitration under the parties' agreement,⁷ and the plaintiffs filed a second amended complaint.⁸

¹ See Sept. 27, 2013 Memorandum Opinion and Order, *Valentine v. WideOpen West Finance LLC*, No. 09 C 7653 (N.D. Ill. Sept. 27, 2013) [Doc. No. 186] (hereinafter, "September 2013 Dismissal Order"), available at http://scholar.google.com/scholar_case?case=391451202472831530&q=%22WOW%22&hl=en&as_sdt=4,332 (last visited Oct. 18, 2013).

² 18 U.S.C. Chapter 119.

³ The lawsuit originated from a proposed class action filed in United States District Court for the Northern District of California in November 2008. The plaintiffs sued WOW and five other ISPs that had contracted with NebuAd, claiming they had each violated the ECPA by installing hardware on their network facilities that then intercepted the plaintiffs' online communications. The suit was dismissed for lack of jurisdiction in October 2009, forcing the plaintiffs to file actions against the six individual ISPs in various federal courts around the country. See *Valentine v. NebuAd, Inc.*, No. 08-5113, 2009 WL 8186140, at *1 (N.D. Cal. Oct. 6, 2009).

⁴ Second Amended Class Action Complaint, *Valentine v. WideOpen West Finance LLC*, No. 09 C 7653 (N.D. Ill. May 25, 2012) [Doc. No. 135] (hereinafter "Second Amended Complaint").

⁵ Although defendant WOW also argued that dismissal was appropriate because plaintiffs had "consented" to the alleged misconduct in their terms of service, the court held that dismissal on the basis of consent was inappropriate at this stage of the proceedings because it could not take judicial notice of the plaintiffs' alleged consent. See *Valentine v. WideOpen West Finance LLC*, No. 09 C 7653 (N.D. Ill. Dec. 20, 2012) [Doc. No. 157] (hereinafter "December 20, 2012 Order") at 13, available at http://scholar.google.com/scholar_case?case=5222736126937836783&q=%22WOW%22&hl=en&as_sdt=4,332 (last visited Oct. 18, 2013).

⁶ 18 U.S.C. § 1030, et seq.

⁷ See Memorandum Opinion and Order, *Valentine v. WideOpen West Finance LLC*, No. 09 C 7653 (N.D. Ill. Mar. 26, 2012) [Doc. No. 123].

⁸ See Second Amended Complaint.

The Court's Findings

Enacted in 1986 to amend the federal wiretap laws, the ECPA protects wire, oral, and electronic communications while in transit, as well as communications held in electronic storage. The statutes create penalties for any person who intentionally (1) "intercepts," "uses," or "discloses" any wire or oral communication by using any electronic, mechanical, or other device, or (2) without authority accesses a wire or electronic communication while in storage. The law specifically defines "intercept" as the "aural or other acquisition of the contents of any . . . electronic . . . communication through the use of any electronic, mechanical, or other device."⁹ The ECPA enumerates a handful of specific exceptions to these prohibitions, among them, when interception by an "electronic, mechanical or other device" is carried out "by a provider of wire or electronic communication service *in the ordinary course of its business*"¹⁰ (emphasis added).

The plaintiffs alleged that by intentionally diverting customers' Internet activity to NebuAd for analysis, WOW violated the "interception," "disclosure," and "use" prongs of the law. In December 2012, Judge Chang dismissed the plaintiffs' "interception" claim, determining that WOW merely acted as a conduit for NebuAd in the ordinary course of its business, and did not itself "acquire" user information within the meaning of the ECPA, making it immune from liability.¹¹ Although the ECPA itself does not define "acquisition," Judge Chang applied the word's common meaning—"to come into possession, control, or power of disposal."¹² He explained that because the plaintiffs alleged that "WOW merely facilitated NebuAd's acquisition of Plaintiffs'

information," without ever itself coming into "possession or control" of that information, it was NebuAd that "actually acquired the communications in the sense of the statute."¹³ Judge Chang also found that WOW could not be held secondarily liable for aiding and abetting NebuAd because the ECPA does not allow for such claims.¹⁴

Judge Chang's earlier order left the plaintiffs' "disclosure" and "use" allegations under 18 U.S.C. §§ 2511(1)(c) and (1)(d) unresolved, and he asked the parties for additional briefing on both issues. However, his recent ruling affirmatively closes the door on WOW's liability, explaining that without allegations of an "acquisition," all *three* claims fail.¹⁵ The judge reasoned that a person cannot violate the "disclosure or use" subparagraphs of the statute unless that person first "know[s] or ha[s] reason to know that the information was obtained through the interception of a[n] . . . electronic communication in violation of this subsection."¹⁶ Thus, because the plaintiffs failed to allege that WOW had intercepted information to disclose or use, they had no viable claim under any portion of the ECPA.¹⁷

Judge Chang relied heavily on the Tenth Circuit's recent opinion and order granting summary judgment to ISP Embarq Management Company (Embarq) in a parallel suit arising from Embarq's previous partnership with NebuAd.¹⁸ In *Kirch v. Embarq Management Company*, the Tenth Circuit emphasized that Embarq was not liable because the record showed that NebuAd's device had not allowed it to gather any more information than what it already had accessed in the "ordinary course of business." The opinion is one of very few federal appeals court decisions construing the ECPA's application to online behavioral

advertising, and it suggests that by explicitly authorizing "interceptions" that occur in the "ordinary-course-of-business acquisitions of electronic communications," Congress immunized ISPs' participation in such activities from the ECPA.

Notably, the plaintiffs also had sought to keep their suit alive by moving to amend their complaint a third time to add claims that WOW intentionally procured NebuAd to intercept their communications, and that WOW had violated Section 2511(3)(a) by "divulging" the contents of the plaintiffs' communications to NebuAd. The court's recent order denied the plaintiffs' request, finding that they had failed to offer a sufficient explanation for failing to include these claims in their prior complaints. Moreover, the court explained that because the plaintiffs had not sufficiently alleged an "acquisition," it was futile to include a new "divulgence" claim without pleading additional facts.¹⁹

Implications

Under Judge Chang's recent ruling, carriers, advertisers, and website publishers cannot incur civil ECPA liability simply by participating in online advertising programs carried out by third parties. The decision also provides some clarity about the types of interceptions of electronic communications the ECPA authorizes under the "ordinary course of business" exception.

Nevertheless, it is important to stress that robust disclosure practices that secure user consent remain the best defense against privacy litigation. Accordingly, companies should regularly review their privacy policies to ensure that all users are adequately apprised of their practices and procedures.

⁹ 18 U.S.C. § 2510(4).

¹⁰ *Id.* at § 2510(5)(a)(1) ("ordinary course of business" exception).

¹¹ See December 20, 2012 Order at 7-8.

¹² *Id.* at 7.

¹³ *Id.* at 7-8.

¹⁴ *Id.* at 9.

¹⁵ September 2013 Dismissal Order at 6.

¹⁶ *Id.* at 13.

¹⁷ *Id.* at 14.

¹⁸ *Id.* at 10 [citing Memorandum Opinion and Order, *Kirch v. Embarq Mgmt. Co.*, No. 11-3275 (10th Cir. Dec. 28, 2012), available at http://scholar.google.com/scholar_case?case=1666725371651300106&q=%22Kirch+v.+Embarq%22&hl=en&as_sdt=4,106,120 (last visited Oct. 18, 2013)].

¹⁹ *Id.* at 17-18.

W&S Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

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

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

This communication is provided for your information only and is not intended to constitute professional advice as to any particular situation.
© 2013 Wilson Sonsini Goodrich & Rosati, Professional Corporation. All rights reserved.

