Cybersecurity, Privacy and Communications Webinar: Trends in Privacy Litigation

June 14, 2016

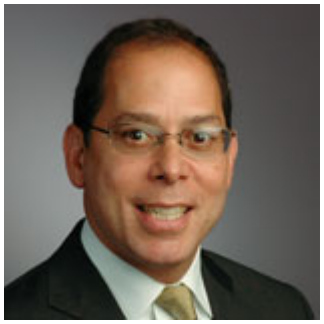
Jonathan G. Cedarbaum
Felicia Ellsworth
Mark Flanagan

WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP

Attorney Advertising

Speakers



Jonathan Cedarbaum
Partner

Felicia Ellsworth
Partner

Mark Flanagan
Partner

Webinar Guidelines

- Participants are in listen-only mode
- Submit questions via the Q&A box on the bottom right panel
- Questions will be answered as time permits
- Offering 1.0 CLE credit in California and New York*
- WebEx customer support: +1 888 447 1119, press 2

WilmerHale has been accredited by the New York State and California State Continuing Legal Education Boards as a provider of continuing legal education. This program is being planned with the intention to offer CLE credit in California and non-transitional credit in New York. This program, therefore, is not approved for New York newly admitted attorneys. Attendees of this program also may be able to claim England & Wales Unaccredited CPD for this program. WilmerHale is not an accredited provider of Virginia CLE, but we will apply for Virginia CLE credit if requested. The type and amount of credit awarded will be determined solely by the Virginia CLE Board. Attendees requesting CLE credit must attend the entire program.

Road Map

- Some Key Issues
- Standing
  - *Spokeo v. Robins*: Sufficiency of Statutory Violations?
  - Cognizable Injury
- Claims & Defenses
  - CFAA
  - Wiretap Act/ECPA/SCA
  - State law: common law and statutory, e.g., consumer protection
  - Biometrics: a new frontier?
- Class Certification

Some Key Issues

- Some Key Theories:
  - Unauthorized (i) collection, (ii) sharing, or (iii) use of personal information
  - Growing number of cases involving use of personal information for advertising/marketing
  - Employee monitoring, BYOD and social media raise new risks
  - Proliferating State privacy laws offer new avenues for plaintiffs to challenge data collection
- Battleground Issues:
  - Adequacy of plaintiffs' injury, both for standing and merits
  - Whether consumer consent sufficiently informed; opt-in versus opt-out
  - Scope of statutory causes of action, including Wiretap Act, SCA, CFAA, and State equivalents, as well as consumer protection statutes
  - Statutory claims particularly important for injury and liquidated damages provisions

Standing via Statute?: *Spokeo v. Robins*

- Question presented:
  - Whether Congress may confer Article III standing upon a plaintiff who suffers no concrete harm, by creating a private right of action for violation of a statute?
- Facts:
  - Robins sued Spokeo as a "consumer reporting agency" under the Fair Credit Reporting Act for statutory damages
  - Whether Robins adequately alleged any injury – *i.e.*, harm that is concrete and particularized – was disputed
- The Supreme Court held 6-2 that the Ninth Circuit failed to address the "concreteness" requirement
  - "[A] bare procedural violation, divorced from any concrete harm" is insufficient
  - But "concrete" harms need not always be "tangible" harms, and "the risk of real harm can[] satisfy the requirement of concreteness"

Standing, Injury, Damages: Other Theories

- Data collection class action plaintiffs struggle to show standing, but are persistent
- Examples of 2015 dismissals in cases alleging that companies allowed personally identifiable information about customer Internet browsing history to be collected and sent to the social media site Facebook:
  - *In re Hulu Privacy Litigation*, — F. Supp. 3d —-, No. 3:11-cv-03764 (N.D. Cal. Mar. 31, 2015) (granting summary judgment);
  - *Carlsen v. GameStop, Inc.*, — F. Supp. 3d —-, 2015 WL 3538906, at *6 (D. Minn. June 4, 2015) (granting motion to dismiss);
  - *Austin-Spearman v. AARP and AARP Services, Inc.*, — F. Supp. 3d —, 2015 WL 4555098 (D.D.C. July 28, 2015) (same).

Standing, Injury, Damages: Other Theories, con't.

- Breach of contract
  - *Svenson v. Google Inc.*, 2015 WL 1503429 (N.D. Cal. Apr. 1, 2015)
    - Alleged failure to honor privacy policies re: app purchasers' information
    - Allegedly damaged by not receiving the benefit of the bargain– i.e., contracted-for privacy protections
    - Similar, in some respects, to overpayment theory
- Diminution of value in personal information
  - *Svenson*: allegation of market for shared personal information sufficient to state claim for damages
    - [Note: *Svenson* also presents SCA issues, as to standing and statutory construction]
- Technological harm
  - *In re Google, Inc. Privacy Policy Litigation*, 2015 WL 4317479 (N.D. Cal. July 15, 2015)
    - Depletion of battery and bandwidth from transmission of personal information sufficient, but …
    - Amended complaint did not sufficiently allege it, case dismissed with prejudice

Computer Fraud & Abuse Act

- Began as a criminal statute designed principally to protect federal computers from hacking
- But includes a private right of action, and has been amended to cover virtually any computer connected to the Internet; as a result, it – and the growing number of State statutory analogues – are used in both privacy and data breach cases
- Relevant provisions:
  - "accesses a computer without authorization or exceeds authorized access" 18 U.S.C. § 1030(a)(2)
  - "accesses a protected computer without authorization, or exceeds authorized access" *Id*. § 1030(a)(4)
  - "'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter" *Id*. §1030(e)(6)

CFAA: “Exceeds Authorized Access”

In *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012), the en banc Ninth Circuit held that the CFAA’s prohibition on “exceed[ing] authorized access” is not intended to reach unauthorized use if access was authorized

- A former employee was charged after enlisting his former co-workers to download confidential company information in violation of a corporate computer-use policy
- Ninth Circuit majority, per Kozinski, C.J., held the government’s construction could expand the CFAA “far beyond computer hacking to criminalize any unauthorized use of information obtained from a computer”
- Concern that mere violation of consumer terms of use could be treated as a federal crime

CFAA: “Exceeds Authorized Access,” con’t.

Circuits are split:

- Second and Fourth Circuits have adopted the Ninth Circuit’s narrower view
- First, Fifth, Seventh and Eleventh Circuits have embraced the broader pro-government, pro-plaintiff interpretation
- “If this sharp division means anything, it is that the statute is readily susceptible to different interpretations” *United States v. Valle*, 807 F.3d 508, 524 (2d Cir. 2015)

CFAA Damage Requirement

Civil actions require “damage or loss” of at least $5,000 in value during any one-year period. 18 U.S.C. § 1030(g)

- Damage means “any impairment to the integrity or availability of data, a program, a system or information”

- Loss means “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system or information to its condition prior to the offense, and any revenue lost, cost incurred or other consequential damages incurred because of interruption of service”

CFAA Damage Requirement, con't.

- "Loss" added to the CFAA as part of USA PATRIOT Act, causing courts to frequently conflate or confuse how "damage" and "loss" apply to CFAA actions:
  - Some courts have required either damage or an "interruption in service" for a CFAA claim. *See TriTeq Lock & Sec. LLC v. Innovative Secured Sols.*, LLC, 2012 WL 394229 (N.D. Ill. Feb. 1, 2012) (because service not interrupted and no damage to systems, plaintiff failed to allege "loss")
  - Some courts have held that improper use by itself is not "damage." For example, disclosure or misappropriation of trade secrets does "not qualify as damage" under the CFAA. *Farmers Ins. Exch. v. Auto Club Grp.*, 823 F. Supp. 2d 847 (N.D. Ill. 2011)
  - Courts have also struggled with whether lost revenue due to unfair competition or lost business opportunities are "losses" under the CFAA. *Nexans Wires S.A. v. Sark-USA, Inc.*, 319 F. Supp. 2d 468 (S.D.N.Y. 2004)

Wiretap Act/Electronic Communications Privacy Act

Wiretap Act (18 U.S.C. § 2510 et seq.)

- Amended as part of the Electronic Communications Privacy Act of 1986, Wiretap Act prohibits intentional "intercept[ion]," disclosure or use of "wire, oral, or electronic communication," where interception is limited to "contents" of communication
  - Statutory exceptions include:
    - Consent (*Id.* § 2511(3)(b)(ii))
    - Ordinary course of business (*Id.* § 2510(5))
    - "[R]eadily accessible to the general public" (*Id.* § 2511(2)(g)(i))
- Remedies: the greater of either actual damages plus resulting profits or the greater of $100 per day of violation or $10,000
- Actions often arise when companies "scan" emails or content on social media for advertising, or when employers monitor employees (or former employees) on their personal devices or outside of work hours

Wiretap Act: “Contents” of a Communication

- “Contents includes any information concerning the substance, purport, or meaning of that communication” (18 U.S.C. § 2510(8))
- In *In re Zynga Privacy Litigation*, No. 11-18044 (9th Cir. 2014), plaintiffs alleged that Zynga’s and other companies’ sharing of “referrer header information” with advertisers violated Wiretap Act/ECPA
- Ninth Circuit affirmed dismissal
  - Referrer header info = Facebook ID and webpage address from which HTTP request sent does not constitute contents, even if former may include or easily lead to PII
  - “Under ECPA, the term ‘contents’ refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication”

Wiretap Act: Consent

Express and Implied Consent

- In *In re Google Inc. Gmail Litigation*, 13-MD-02430-LHK, 2013 WL 5423918 (N.D. Cal. Sept. 26, 2013): plaintiffs alleged scanning emails to create user profiles violated ECPA
  - Express consent not present: "[A] reasonable Gmail user who read the Privacy Policies would not have necessarily understood that her emails were being intercepted to create user profiles or to provide targeted advertisements"
  - Implied consent not present: "Google's theory of implied consent – that by merely sending emails to or receiving emails from a Gmail user, a non-Gmail user has consented to Google's interception of such emails for any purposes – would eviscerate the rule against interception"
- Establishing consent in most cases requires showing that the consenting party received actual notice of the monitoring and used the monitored system anyway

Wiretap Act: "In the Ordinary Course of Business"

While ECPA provides an exception for interceptions that occur "in the ordinary course of business" (18 U.S.C. §2510(5)(a)), there are different interpretations of this exception:

- **Narrower view**: exception applies "only where an electronic communication service provider's interception facilitates the transmission of the communication at issue or is incidental to the transmission of such communication" *In re Google Inc. Gmail Litigation,* 13-MD-02430-LHK (N.D. Cal. Sept. 26, 2013)

- **Broader view**: exception applies "where the provider is furthering its 'legitimate business purposes'—including advertising—and is not limited to only those acts that are technically necessary to processing email." *In re Google Inc. Privacy Policy Litigation*, No. 12-01382, 2013 WL 6248499 (N.D. Cal. Dec. 3, 2013)

Wiretap Act: “Readily Accessible to the General Public”

- ECPA also exempts interceptions of electronic and radio communications where these communications are “readily accessible to the general public. 18 U.S.C. § 2510(16)
- *Joffe v. Google*, 746 F3d 920 (9th Cir 2013), held unencrypted WiFi communications are not readily accessible:
  - WiFi transmissions not “readily accessible to the general public” more generally because they “are geographically limited and fail to travel far beyond the walls of the home or office where the access point is located”
  - “[I]ntercepting and decoding payload data communicated on a WiFi network requires sophisticated hardware and software”
  - “Radio communications” are predominantly auditory, excluding payload data transmitted over WiFi networks from exception for unencrypted radio communications

Stored Communications Act

Stored Communications Act (18 U.S.C. § 2701 et seq.)

- Prohibits:
  - Accessing without authorization a facility through which an electronic communication service is provided or intentionally exceeding an authorization to access such facility and obtaining, altering or preventing authorized access to a wire or electronic communication in electronic storage *Id.* § 2701(a)(2)
  - Providers of an electronic communication service to the public from knowingly divulging contents of communication while in electronic storage (*Id*. § 2702(a)(1))
  - Providers of remote computing services to the public from knowingly divulging contents of communication while in such a service (*Id*. § 2702(a)(2))
- Plaintiffs may recover a minimum of $1,000 per violation *Id.* § 2707

SCA: “Electronic Storage”

“Electronic storage” means:

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication (18 U.S.C. § 2510(17))

Courts have disagreed over meaning of “electronic storage”:

- *Theofel v. Farey-Jones*, 359 F.3d 1066, 1075-77 (9th Cir. 2004) (copies remaining on ISP server after emails received and opened are in “electronic storage”); *Fraser v. Nationwide Mutual Ins. Co*., 352 F.3d 107, 114-15 (3d Cir. 2004) (suggesting same in brief dictum); *Shefts v. Petrakis*, 2011 WL 5930469, at *6 (C.D. Ill. Nov. 29, 2011) (holding same);
- *Jennings v. Jennings,* 736 S.E.2d 242 (S. Car. 2012) (questioning *Theofel*); *United States v. Warshak*, 631 F.3d 266, 291-92 (6th Cir. 2010) (same); *United States v. Weaver*, 636 F. Supp.2d 769, 770-74 (C.D. Ill. 2009) (copies remaining on ISP server after emails received and opened are not in “electronic storage”); *In re DoubleClick, Inc. Privacy Litig*., 154 F. Supp.2d 497, 512 (S.D.N.Y. 2001) (only unopened emails can be in “electronic storage”).

Common State Law Claims

- Common-law claims
  - Breach of contract
  - Breach of the covenant of good faith and fair dealing
  - Fraud
  - Invasion of privacy

- Statutory claims
  - State CFAA (e.g., Cal. Penal Code § 502) or ECPA equivalents
  - UCL/consumer protection statutes
  - Specialized privacy statutes, e.g., medical or financial data

State Law Claims

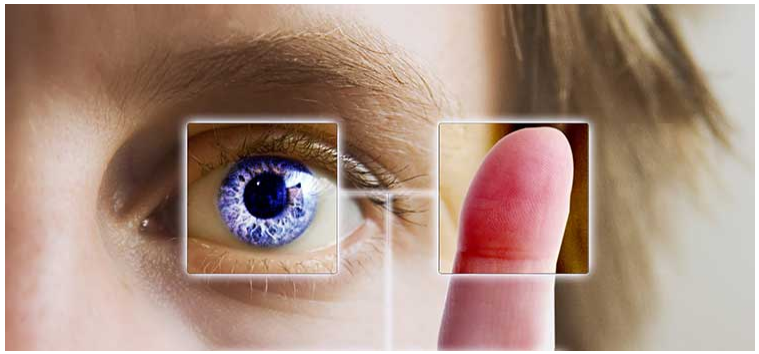
- Some recent examples of the kitchen sink approach
  - *In re Facebook Internet Tracking Litigation*, No. 5:12-2314 (N.D. Cal. 2015): actual fraud, constructive fraud, trespass to chattels, intrusion upon seclusion, invasion of privacy, Cal. Penal Code 502, breach of contract, breach of covenant of good faith and fair dealing, larceny
    - Motion to dismiss Second Amended Complaint pending
  - *Perkins v. LinkedIn Corp*., 53 F.Supp.3d 1190 (N.D. Cal. 2014): common-law right of publicity, Cal. Penal Code 502, UCL
    - Motion to dismiss granted in part and denied in part

A New Frontier? Biometrics

- IL Biometric Information Privacy Act (BIPA) restricts use of "biometric identifiers," defined as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry," and "biometric information", i.e., information based on biometric identifiers. 740 ILCS 14/10
- Companies handling biometric information must maintain a publicly available written policy governing retention and destruction.
- Companies must get informed written consent from consumers before obtaining or disclosing biometric information.
- High statutory damages (740 ILCS 14/20):
  - $1,000 per violation or actual damages for negligent actions
  - $5,000 per violation or actual damages for intentional or reckless violations

A New Frontier? Biometrics

- *Norberg v. Shutterfly, Inc.*, Case No. 15-cv-5351 (N.D. Ill. Dec. 29, 2015)
  - Alleges Shutterfly's facial recognition features violated BIPA by collecting, using facial geometry patterns without consent to identify individuals in photographs
  - District court denied motion to dismiss because plaintiff "has plausibly stated a claim for relief under the BIPA."
  - Case settled in April 2016 for an undisclosed sum
- Facebook's motion to dismiss a similar action was denied in May 2016.



Class Certification Challenges

Class certification has also proven challenging for plaintiffs

- Class certification denied in *In re Google Inc. Gmail Litigation*, 13-MD-02430-LHK, 2013 WL 5423918 (N.D. Cal. Sept. 26, 2013) because "individual issues regarding consent are likely to overwhelmingly predominate over common issues."
- Class certification granted in *In re Yahoo Mail Litig., 308 F.R.D. 577, 583 (N.D. Cal. 2015)*:
  - Class was narrower, comprised nonsubscribers who sent emails to Yahoo subscribers (and a California subset)
  - The class sought only injunctive relief rather than damages: commonality, not predominance, required
  - Typicality satisfied

Class Action Challenges

Harris v. comScore, Inc., 1:11-cv-05807, involves one of the largest privacy class actions ever certified:

- Plaintiffs alleged the placement of the OSSProxy program onto their computers violated CFAA, ECPA and the SCA
- District court found statutory damages alone sufficient to satisfy the commonality and predominance requirements (*Harris v. comScore, Inc.*, 292 F.R.D. 579 (N.D. Ill. 2013))
- Court found Supreme Court's "assumption" in *Comcast Corp. v. Behrend*, 133 S. Ct. 1426 (2013), that a class-wide damages calculation was required in antitrust cases, "even assuming it is applicable to privacy class actions in some way, is merely dicta and does not bind this court"
- Seventh Circuit denied comScore's request for interlocutory appeal in July 2013
- comScore agreed to a $14 million settlement in May 2014

Bringing Mass Actions to Avoid Class Action Certification Challenges

- Plaintiffs have alleged in *Corley et al v. Google Inc.*, 5:16-cv-00473 (Jan. 27, 2016 N.D. Cal), that Google's intercepting and scanning the content of their Google Apps for Education emails violates the Wiretap Act.
- Rather than attempting to bring a class action, however, plaintiffs are focusing on specifically on users who were told their emails would not be monitored.
- Original complaint had four named plaintiffs, but has since been amended to include over 700 named plaintiffs.

Questions?

Jonathan Cedarbaum, Partner

jonathan.cedarbaum@wilmerhale.com | +1 202 663 6315

Felicia Ellsworth, Partner

felicia.ellsworth@wilmerhale.com | +1 617 526 6687

Mark Flanagan, Partner

mark.flanagan@wilmerhale.com | +1 650 858 6047

**WilmerHale has been accredited by the New York State and California State Continuing Legal Education Boards as a provider of continuing legal education. This program is being planned with the intention to offer CLE credit in California and non-transitional credit in New York. This program, therefore, is not approved for New York newly admitted attorneys. Attendees of this program also may be able to claim England & Wales Unaccredited CPD for this program. WilmerHale is not an accredited provider of Virginia CLE, but we will apply for Virginia CLE credit if requested. The type and amount of credit awarded will be determined solely by the Virginia CLE Board. Attendees requesting CLE credit must attend the entire program.*