Trends in Data Security and Privacy Civil Litigation

March 21, 2016

Martin Braun, Partner
Jonathan Cedarbaum, Partner
Mark Flanagan, Partner
Reed Freeman, Partner (*moderator*)
Alan Schoenfeld, Partner

WILMERHALE®

WILMER CUTLER PICKERING HALE AND DORR LLP®

Trends in Data Security and Privacy Civil Litigation

Overview of Data Breach/Cyberattack Class Actions

March 21, 2016

Jonathan Cedarbaum, Partner (Washington, DC)
Alan Schoenfeld, Partner (New York)

WILMERHALE

Attorney Advertising

WILMER CUTLER PICKERING HALE AND DORR LLP

Roadmap

- Overview
  - Data Breach/Cyberattack Cases
  - Types of Claims (Consumers, Employees, Shareholders)
- Claims & Defenses
  - Standing
  - Important Issues
  - Key Defenses
- Class Certification
  - Looking Back
  - Looking Forward

Overview: Data Breach/Cyberattack Cases

A familiar story:

On August 14, 2014, Defendants announced in press releases that from June 22, 2014 to July 17, 2014, hackers had gained unauthorized access to and installed malicious software on the portion of SuperValu's computer network that processes payment card transactions for Defendants' retail stores. The intrusion resulted in potential theft of information embedded in the magnetic strip of payment cards for sales transacted at 209 SuperValu stores and 836 AB Acquisition stores. The PII embedded in the magnetic strip included cardholder names, account numbers, expiration dates, and PINS. The press releases stated Defendants' offer of 12 months of complimentary consumer identity protection services to customers whose cards may have been affected by the data breach.

In re SuperValu, Inc., 2016 WL 81792, at *1 (D. Minn. Jan. 7, 2016).

Overview: Data Breach/Cyberattack Cases, con't.

Expect a data breach to result in civil litigation

- Home Depot was sued *before* it had even confirmed that it suffered a breach
- Target was sued in federal courts the *same* day it announced the breach
- Sony Pictures Entertainment was sued in *nine* class action cases, in federal and state court, within three months of disclosing its breach

Overview: Data Breach/Cyberattack Cases, con't.

Suits commonly brought by a breached company's consumers, shareholders and employees

- Depending upon the breach, other companies, such as counterparties and cobranding entities, may also bring suit
  - *See, e.g., First choice Federal Credit Union v. The Home Depot, Inc.*, No. 14-cv-2975 (N.D. Ga.) (putative class action brought by banks allegedly injured by Home Depot's breach by having to cancel or reissue access devices affected by the breach, or to close accounts, block transactions, etc.)

Overview: Data Breach/Cyberattack Cases, con't.

Litigation shaped by

- **Plaintiffs**
- **Types of PII affected**
  - Personal (SSN, birthdate, address, phone number)
  - Financial (debit/credit card, bank account credentials)
  - Health-Related/HIPAA (medical treatment history, insurance claims)

Overview: Data Breach/Cyberattack Cases, con't.

- **Nature of the breach**
  - Lost laptop or simple theft
  - PII specifically targeted/published online
  - Criminal cyberattack

- **Common types of claims:**
  - Defendant's data-security measures were inadequate (e.g., negligence, specialized state privacy statutes)
  - Defendant misrepresented data-security measures (e.g., UCL/fraud)
  - Defendant's disclosure/reaction too slow (e.g., data-breach notification statutes)

Overview: Types of Claims (Consumers)

Consumer class actions are most common, and they raise a host of common law, contract and statutory claims

Common Law Claims:

- **Negligence claims in this context typically allege a breach of the breached company's duties to:**
  - Exercise reasonable care in safeguarding and securing personal and financial information; and/or
  - Promptly and effectively notify consumers about unauthorized disclosure
- **Claims for breach of contract or of implied covenants typically involve the theory that a company breached either express or implied promises to consumers regarding adequacy of network security**

Overview: Types of Claims (Consumers) , con't.

State statutory claims

- **Violation of data protection and data-breach notification laws, which are sometimes general and sometimes specific to financial data.** *E.g.*, the Home Depot plaintiffs alleged claims under 38 state data-breach notification statutes
- **Violation of unfair competition laws, which typically prohibit unfair or deceptive acts and practices. The results vary from state to state:**
  - *In re TJX Cos. Retail Sec. Breach Litigation*, 564 F.3d 489, 496, 501-502 (1st Cir. 2009) (vacating dismissal of Massachusetts 93A claim where plaintiffs alleged "lack of security measures was 'unfair'")
  - *In re Heartland Payment Systems, Inc. Customer Data Security Breach Litigation*, 834 F. Supp. 2d 566, 602 (S.D. Tex. 2011) (complaint did not state claim for violation of California UCL where plaintiffs conclusorily alleged reliance)

Overview: Types of Claims (Consumers), con't.

Federal statutory claims

- **Violation of federal laws, either to support state-law claims or due to specific causes of action provided within the federal statute**
- ***E.g.*, Fair Credit Reporting Act (FCRA); Stored Communications Act (SCA); Gramm-Leach Bliley Act; Driver's Privacy Protection Act; Health Insurance Portability and Accountability Act (HIPAA)**
- Under FCRA, plaintiffs have alleged that a breached company failed to maintain reasonable procedures to "furnish" consumer reports, and so "consumer reports were released in violation of the statute's provisions." *Holmes v. Countrywide Fin. Corp.*, 2012 WL 2873892, at *15 (W.D. Ky. July 12, 2012)

Overview: Types of Claims (Consumers), con't.

Typical forms of relief sought in consumer class action cases

- Compensatory damages
- Statutory damages and penalties
- Punitive damages
- Injunctive and equitable relief
- Restitution
- Disgorgement
- Attorneys' fees and costs

Overview: Types of Claims (Consumers), con't.

Frequently asserted bases for damages

- Increased risk of future harm (*e.g.*, identity theft)
- Time and money spent on mitigation efforts
- Emotional injury/loss of privacy
- Loss of value of information
- Loss of benefit of the bargain

Overview: Types of Claims (Employees)

Claims brought in employee class actions can be similar

- **State Common Law Claims**
  - Negligence (failure to safeguard sensitive PII; delay in notification)
  - Bailment (failure to safeguard information in employer's possession)
  - Invasion of privacy
  - Breach of employment contract
- **State Statutory Claims**
  - Workers' compensation claims
  - State data claims (in *Sony, e.g.*, California Customer Records Act; California Confidentiality of Medical Information Act)
  - State UDAP claims

Overview: Types of Claims (Employees), con't.

- **Federal Statutory Claims**
  - Fair Credit Reporting Act
  - Fair and Accurate Credit Transactions Act

Overview: Types of Claims (Shareholders)

Common claims in shareholder derivative cases

- **Allegations Against Board Members and Executives**:
  - Failure to properly oversee the company;
  - Failure to prevent the data breach; and
  - Failure to announce the data breach quickly and effectively
- **Theory**: Plaintiffs allege that the individual defendants' failures have caused or will cause injury to the company
- **Common Claims**:
  - Breach of fiduciary duty
  - Waste of corporate assets
  - Gross mismanagement
  - Abuse of control

Overview: Types of Claims (Shareholders), con't.

Common relief sought in shareholder derivative cases

- Damages
- Improvements to corporate governance and internal procedures
- Restitution to the company of the defendants' compensation
- Attorneys' fees and costs

Claims & Defenses: Key Defenses

- Article III standing
- Failure to state a claim/defeating claims on the merits
- Failure to make a pre-suit demand (shareholders' cases)
- Class certification

Claims & Defenses: Article III Standing

The case or controversy requirement of the U.S. Constitution requires that a plaintiff show, as an "irreducible constitutional minimum of standing," that:

- it has suffered an "**injury in fact**" that is (a) **concrete and particularized** and (b) **actual or imminent**, not conjectural or hypothetical;
- the injury is **fairly traceable** to the challenged action of the defendant; and
- it is likely, that the injury will be **redressed by a favorable decision.**

Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 180-181 (2000); *see also Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-561 (1992)

Claims & Defenses: *Clapper*

***Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013)**:

- The U.S. Supreme Court "reiterated that threatened injury must be ***certainly impending*** to constitute injury in fact, and that allegations of ***possible* future injury are not sufficient**."
- The Court also held that a plaintiff cannot "manufacture standing merely by inflicting harm on [himself] based on [his] **fears of hypothetical harm that is not certainly impending**."

The Court's reasoning in *Clapper* seemingly applies directly to theories of harm commonly alleged in data breach cases:

- Increased risk of identity theft
- Costs involved in preventing future harm (*e.g.*, credit monitoring)

Claims & Defenses: Post-*Clapper*

Following *Clapper*, defendants in data-breach cases have often succeeded in dismissals based on lack of Article III standing:

- **Allegations in data breach cases may only assert hypothetical injuries** based on claim that personal or financial information was (or may have been) compromised in the breach. *See, e.g., Remijas v. Neiman Marcus Grp.*, LLC, 2014 WL 4627893, at *3 (N.D. Ill. 2014) (dismissing where "the overwhelming majority of the plaintiffs allege only that their data may have been stolen")

Claims & Defenses: Post-*Clapper,* con't.

- **Plaintiffs in data-breach cases often allege harm in the form of increased risk of identity theft in the future** based on the notion that cyber criminals wait to strike. *See, e.g., In re Science Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 2014 WL 1858458, at *8 (D.D.C. 2014) ("since *Clapper*," "courts have been even more emphatic in rejecting 'increased risk' as a theory of standing in data-breach cases. … After all, an increased risk or credible threat of impending harm is plainly different from certainly impending harm, and *certainly impending* harm is what the Constitution and *Clapper* require.")

Claims & Defenses: Post-*Clapper,* con't.

Since *Clapper*, a handful of data-breach cases have survived threshold standing challenges in the Seventh and Ninth Circuits:

- ***In re Adobe Systems, Inc. Privacy Litig.***, 2014 WL 4379916 (N.D. Cal. 2014) (finding that plaintiffs alleged concrete injury where hackers specifically targeted the PII after a weeks-long intrusion, used Adobe's own decryption keys, and posted some of the PII on the internet)
- ***In re Sony Gaming Networks & Customer Data Sec. Breach Litig. (Sony II)***, 996 F. Supp. 2d 942, 962 (S.D. Cal. Jan 21, 2014) ("Plaintiffs' allegations that their Personal Information was collected by Sony and then wrongfully disclosed as a result of the intrusion [is] sufficient to establish Article III standing at this stage in the proceedings.")

Claims & Defenses: Post-*Clapper*, con't.

- ***Corona v. Sony Pictures Entm't Inc.***, 2015 WL 3916744 (C.D. Cal. 2015) (alleged theft and publication of PII on online file-sharing websites is sufficient to confer Article III standing)

Claims & Defenses: Post-*Clapper*, con't.

The Seventh Circuit recently issued the first major post-*Clapper* standing decision by a court of appeals

- ***Remijas v. Neiman Marcus Group, LLC***, 794 F.3d 688 (7th Cir. 2015) (finding that like the circumstances in *In re Adobe*, the fact that hackers deliberately targeted Neiman Marcus's credit card information creates "an objectively reasonable likelihood that such an injury will occur")

Claims & Defenses: Post-*Clapper*, con't.

On February 14, 2016, Judge Koh once again found that plaintiffs showed standing to raise a claim under California's UCL in a major data breach involving the theft of nearly 80 million health records:

- ***In re Anthem, Inc. Data Breach Litig.***, No. 150MD002617-LHK (N.D. Cal. 2016) (finding that Anthem's failure to protect plaintiffs' health information deprived them of the "benefit of the bargain," amounting to economic injury sufficient for standing)
  - The court did not address whether "out of pocket costs" to prevent identity theft or "imminent risk of further costs" equate to economic injury to confer standing

Claims & Defenses: Key Defenses

Failure to state a claim

- **Given the widely varying results at the pleading stage, virtually every defendant in a data-breach case moves to dismiss. Plaintiffs are trying out untested theories (which some courts reject), and their allegations of injury are often speculative**.
- **Examples of dismissals based on failure to state a claim**
  - *In re Sony*, 996 F. Supp. 2d at 963 ("Plaintiffs' allegations of causation and harm are wholly conclusory[.]"); *id.* at 965 ("[E]ven though the Court finds Plaintiffs may have alleged a brief delay in the time period between the intrusion and when Sony notified consumers of the intrusion, the Court finds Plaintiffs have failed to allege that their injuries," *e.g.*, "credit monitoring services," "were proximately caused by Sony's alleged untimely delay.")

Claims & Defenses: Key Defenses, con't.

- *Holmes*, 2012 WL 2873892, at *5 ("Courts confirming their constitutional jurisdiction in risk-of-identity-theft cases have gone on to dismiss the action because the injury was not recompensable under state law.").

Claims & Defenses: Key Defenses, con't.

- **Square peg/round hole problem: Does the cause of action or the statute at issue cover the plaintiff, the alleged loss or the alleged misconduct?**
  - *Sony Pictures*, 2015 WL 3916744 (dismissing California *Customer* Records Act claim in employee class action).
  - Does the statute at issue cover, *e.g.*, diminution in value of PII?
- **Allegations of damages are often conclusory**, without any specificity as to what injury that plaintiffs in fact suffered as a result of the company's alleged misconduct.
  - *In re Sony*, 996 F. Supp. 2d at 964 ("Plaintiffs do not specifically allege what economic injury they allegedly suffered as a result of Sony's negligence, what property was allegedly damaged, or how the alleged property damage was proximately caused by Sony's breach.").

Claims & Defenses: Key Defenses, con't.

- **One common economic damage claim includes the cost to purchase credit monitoring services**.
  - *In re Sony*, 996 F. Supp. 2d at 965
  - *Holmes*, 2012 WL 2873892, at *6 ("Plaintiffs stake much of their response on the Holmes' payments for credit monitoring.")
  - Practice Pointer: In the wake of a breach, the company will need to make some quick decisions about remediation, which will likely shape the course of any follow-on litigation and the relief plaintiffs can seek

Claims & Defenses: Key Defenses, con't.

Failure to state a claim (shareholders)

- The allegations make conclusory claims that individual defendants failed to discharge required duties. But, as defendants have argued, it is impermissible to assume that individual defendants breached their duties simply because a data breach occurred on their watch, and conclusory allegations are insufficient to state viable claims.

- Relevant analysis here will likely turn on what individual defendants knew about any breach and when; whether and when they were warned about the risks of data breaches; why, when and how they decided to notify consumers

Claims & Defenses: Key Defenses, con't.

Failure to make a pre-suit demand (shareholders)

- Because any claims in the shareholder cases belong to the breached company, plaintiffs in any such cases will first need to plead that they made a demand for action upon the board, or that their failure to make a demand should be excused because it would have been futile.
- If Plaintiffs fail to do so, or if they make only generic conclusory allegations of futility, there is an argument that their cases should be dismissed for failure to make a pre-suit demand.
- *Palkon v. Holmes*, No. 2:14-CV-01234 SRC, 2014 WL 5341880, (D.N.J. Oct. 20, 2014).

Class Certification

Preliminary hurdles for class plaintiffs

Rule 23(a) – numerosity, commonality, typicality and adequacy of representation

- the class is so numerous that joinder of all members is impracticable;
- there are questions of law or fact common to the class;
- the claims or defenses of the representative parties are typical of the claims or defenses of the class; and
- the representative parties will fairly and adequately protect the interests of the class.

Class Certification, con’t.

Rule 23(b)(3) – predominance and superiority

- questions of law or fact common to class members predominate over any questions affecting only individual members, [and]
- a class action is superior to other available methods for fairly and efficiently adjudicating the controversy.

Class Certification – Looking Back

Defendants have generally been successful in arguing against certification because:

Typicality: No data-breach plaintiff is typical. What were their pre-breach data-protection measures? What did their pre-breach web footprint look like? How many other breaches were they involved in? What steps did they take in the wake of the breach to protect themselves? Did they take advantage of available remedies (provided by defendant in wake of breach, provided by banks, insurers, etc.)?

Class Certification – Looking Back, con't.

Actual reliance is required: A fraud or negligent misrepresentation claim, for example, "'cannot be certified when individual reliance will be an issue.'" *In re TJX Cos. Retail Sec. Breach Litig.*, 246 F.R.D. 389, 395 (D. Mass. 2007) (denying class certification)

No causation: "Given that there are a myriad of ways in which fraud losses can occur, as well as the fact that the plaintiffs themselves have admitted the difficulty of attributing any particular loss to the data breach," "evidence of general causation will not suffice to prove the element of causation with regard to fraud-related losses on a class-wide basis." *Id.* at 396-397

Class Certification – Looking Back, con't.

Individualized damages:

- "[L]ack of an expert opinion on [class plaintiffs'] ability to prove total damages to the jury is fatal." *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig*., 293 F.R.D. 21, 33 (D. Me. 2013)
- "[T]he fact that damages must be determined on a plaintiff-by-plaintiff basis further 'weighs against class status.'" *In re TJX*, 246 F.R.D. at 398

Class Certification – Looking Forward

More cases are nearing the class certification stage:

On September 15, 2015, a district court granted financial institutions' motion for class certification in a consolidated MDL *In re Target Corp. Customer Data Sec. Breach Litig.*, 309 F.R.D. 482 (D. Minn. 2015).

- Plaintiffs' theory of injury: injury in the form of replacing cards for customers, reimbursing fraud losses and taking other remedial steps in response to the Target data breach
- The court agreed: "[Reissuing cards] is not a 'future harm.' This is a cost borne at the time of the breach and as a result of the breach. … Plaintiffs have established for the purposes of the class-certification inquiry that they suffered injury proximately caused by the data breach."

Class Certification – Looking Forward, con't.

- No common damages defense: Losses stemming from reissuance and fraud must be made on a bank-by-bank, loss-by-loss basis, rendering damages too individual for classwide determination
- The court disagreed: "Although Plaintiffs' damages may ultimately require some individualized proof, at this stage Plaintiffs have established, through [their expert] report, that it is possible to prove classwide common injury and to reliably compute classwide damages resulting from reissuance costs and fraud losses."

The case is currently pending in the Eighth Circuit

Claims & Defenses: Practice Pointers

- **Post-Breach Response**: Assume you will be sued; what post-breach response best situates you to defend a class action by your customers or employees?
- **Data Security Audits**: Involve your lawyers
- **Coordination**: Like other data breach cases, if multiple suits are filed, whether in one court or in many jurisdictions, defendants will want to coordinate those lawsuits (*e.g.*, MDL proceedings) to minimize duplication and the risk of inconsistent judgments
  - *See, e.g., In re Target Corp. Customer Data Sec. Breach Litigation*, No. 14-md-02522 (D. Minn. May 7, 2014) (MDL involving "plaintiffs in … 81 Consumer Cases resid[ing] in more than two dozen states and … collectively assert[ing] well over 100 different causes of action")

Claims & Defenses: Practice Pointers, con't.

- Defendants will want to remove any cases that are filed in state court – assuming that they assert a federal cause of action, meet minimal diversity and jurisdictional threshold requirements of the Class Action Fairness Act (CAFA) or are otherwise removable – and consolidate them as well

Questions?

Jonathan Cedarbaum, Partner (Washington, DC)
jonathan.cedarbaum@wilmerhale.com
202.663.6315

Alan Schoenfeld, Partner (New York)
alan.schoenfeld@wilmerhale.com
212.937.7294

**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.*

Trends in Data Security and Privacy Civil Litigation

Trends in Privacy Class Actions: CFAA, ECPA/SCA, State-Law Claims

March 21, 2016

Mark Flanagan, Partner (Palo Alto)
Jonathan Cedarbaum, Partner (Washington DC)

WILMERHALE®

WILMER CUTLER PICKERING HALE AND DORR LLP ®

Road Map

- Some Key Issues
- Standing
  - *Spokeo*: Sufficiency of Statutory Violations?
  - Cognizable Injury
- Claims & Defenses
  - CFAA
  - Wiretap Act/ECPA/SCA
  - State law: common law and statutory, e.g., consumer protection
  - A New Frontier?: Biometrics
- 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, ECPA, SCA, 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
- Ninth Circuit held that standing existed by virtue of a violation of the plaintiff's statutory rights
- WilmerHale-authored amicus brief for eBay, Facebook, Google, LinkedIn, Twitter, Internet Association et al.
  - Technology companies particularly vulnerable to allegations of injury-in-law but not injury-in-fact (ECPA, TCPA, VPPA, etc.)
  - Actual injury requirement protects separation of powers by keeping law enforcement in hands of Executive Branch

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, I*nc., — F. Supp. 3d —-, 2015 WL 3538906, at *6 (D. Minn. June 4, 2015) (granting motion to dismiss);
  - *Austin-Spearman v. AARP and AARP Services, In*c., — 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 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 increasingly 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 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))
    - "readily 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 typically arise when companies "scan" emails or other 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
  - "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"
  - 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

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

- **Narrow 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 Wi-Fi 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 interpretation 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.): 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

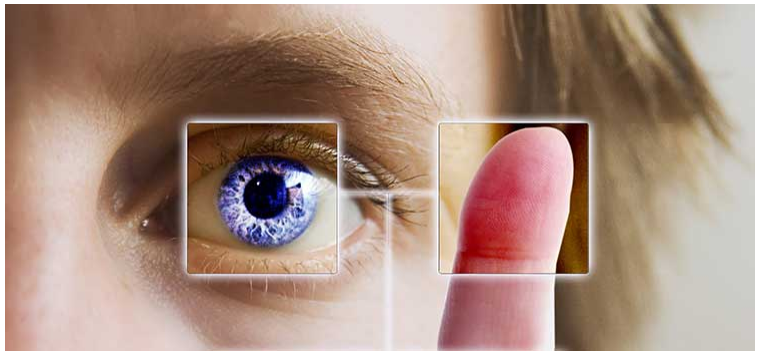
  - *Perkins v. LinkedIn Corp*., 53 F.Supp.3d 1190 (N.D. Cal. 2014): common-law right of publicity, Cal. Penal Code 502, UCL
  - Motion to dismiss granted in part and denied in part

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
  - Plaintiff not a Shutterfly user
  - District court denied motion to dismiss because plaintiff "has plausibly stated a claim for relief under the BIPA."
- BIPA class actions against Facebook and Google are ongoing



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 Cir. denied comScore's request for interlocutory appeal in July 2013
- comScore agreed to a $14 million settlement in May 2014

Questions?

Mark Flanagan, Partner (Palo Alto)
mark.flanagan@wilmerhale.com
650.858.6047

Jonathan Cedarbaum, Partner (Washington, DC)
jonathan.cedarbaum@wilmerhale.com
202.663.6315

**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.*

Trends in Data Security and Privacy Civil Litigation

Law and Litigation under the Telephone Consumer Protection Act (TCPA)

March 21, 2016

Alan Schoenfeld, Partner (New York)

WILMERHALE

Attorney Advertising

WILMER CUTLER PICKERING HALE AND DORR LLP ®

TCPA Statutory Takeaways

- Regulates telemarketing and the use of automated telephone dialing equipment for voice calls, faxes and text messages *See* 47 U.S.C. § 227
- Provides a private right of action and statutory damages for violations of the statute:
  - $500 per violation for negligent violations
  - $1,500 per violation for willful or knowing violations
- Damages are assessed on a per communication basis (maybe – we will return to this below). This has led to a proliferation of class action lawsuits and multi-million dollar settlements.

The Importance of Consent

- With few exceptions, "*prior express consent*" is required for non-telemarketing autodialed calls or calls made using an automated or prerecorded voice. See 47 U.S.C. § 227(b)(1)(A).
  - In some cases, consent may be inferred from the voluntary provision of a cell phone number
- For telemarketing messages, the FCC requires "*prior express written consent.*" See 2012 TCPA Order.
  - Bears the signature of the person to be called
  - Authorizes the delivery of autodialed telemarketing calls or text messages, or prerecorded telemarketing calls
  - Includes the phone number to which the individual authorizes such delivery
  - Discloses that the individual is not required to agree to such calls and/or messages as a condition of a purchase

FCC 2015 TCPA Declaratory Ruling & Order

- In July 2015, the FCC released an omnibus ruling responding to 21 petitions seeking clarification. *In re Rules and Regulations Implementing the Telephone Consumer Protection Act* of 1991, 30 FCC Rcd. 7961 (July 10, 2015).
- The Order focuses primarily on the following areas:
  - Definition of "automatic telephone dialing system" (ATDS)
  - Revocation of consent
  - Reassigned telephone numbers
  - Limited exceptions for certain "pro consumer" messages, *i.e.*, certain messages from financial institutions and healthcare providers
- Several Petitioners have challenged the Order on the ground that it is arbitrary and capricious, and otherwise contrary to law. The challenge is pending before the D.C. Circuit.

What Is An “ATDS” or “Autodialer”?

- The TCPA covers calls made using an automated telephone dialing system (ATDS), defined in the statute as “equipment which has the capacity—(A) to store or produce telephone numbers to be called, using a random or sequential number generator and (B) to dial such numbers.” 47 U.S.C. § 227(a)(1).
- The Order concludes that “the capacity of an autodialer is not limited to its current configuration but also includes its *potential functionalities*.” Order ¶ 16.
  - Covers equipment that lacks the present ability to dial randomly or sequentially, so long as the equipment could be modified or configured to have that ability
  - Some have contended that the FCC’s broad interpretation likely sweeps in most modern smartphones

Revoking Consent

- The Order concludes that the called party may revoke consent "at any time through *any reasonable means*," and that "[a] caller *may not limit* the manner in which revocation may occur." Order ¶ 47.
- The term "reasonable means" is left undefined by the FCC, but the Order makes clear that callers cannot place limits on the means of revocation.
  - Rejects idea that companies should be able to designate an exclusive or specific means of revoking consent
  - "Reasonable means" *may* include:(1) consumer-initiated calls, (2) requests made in response to a call/text, and (3) oral requests at an in-store bill payment location
  - Vagueness may present issues in training employees to recognize and record revocation of consent

Reassigned Telephone Numbers

- The Order concludes that "the consent … of the current subscriber (or non-subscriber customary user of the phone)" is what's relevant in determining "prior express consent," not that of the "intended recipient" of the call. Order ¶ 72.
- Creates liability for calls to reassigned wireless, but creates a one-call safe harbor:
  - No TCPA liability for first call to reassigned number
  - TCPA liability attaches to each call thereafter, even if the caller does not receive actual notice of the reassigned number
  - The ruling places the burden squarely on the caller to discover reassigned numbers and cease text messages
- The FCC has acknowledged that there is no comprehensive database or other guaranteed way for callers to identify reassigned mobile numbers, but companies should "institute new or better safeguards to avoid calling reassigned numbers"

Other Takeaways from the FCC Order

- **SMS Text Messages Are "Calls"** – Text messages are subject to the same consumer protections under the TCPA as voice calls
- **Internet-to-Phone Text Messages** – Considered the functional equivalent of SMS messages and require consent per the TCPA
  - Internet-to-phone text messages originate as e-mails and are sent to an e-mail address in the form of the recipient's wireless telephone number and the carrier's domain name
- **One-Time "Call-to-Action" Texts** – With some limitations, one-time messages sent in response to consumer texts requesting information do not violate the TCPA

TCPA Litigation Trends

- TCPA lawsuits are no longer limited to the world of debt collectors and telemarketers
- Lawsuits have been filed across many industries, including:
  - Social networking companies (Facebook, Twitter, GroupMe)
  - Sports franchises (Los Angeles Clippers, Buffalo Bills)
  - Pharmacies (CVS Pharmacy Inc., Rite Aid Corp.)
  - Travel and entertainment companies (Cirque du Soleil Co.)
  - Retailers (Best Buy Co., J.C. Penney Co.)
  - Online service providers (29 Prime Inc.)

TCPA Litigation Trends, con't.

- TCPA settlements have hit record highs
  - On the heels of multiple settlements in the $30-40 million range, in February 2015, a federal court in Chicago granted final approval of the largest TCPA class-action settlement to date, with Capital One and affiliates totaling approximately $75.5 million

TCPA Litigation: *Who Initiates the Call?*

- To be directly liable under the TCPA, the defendant must "initiate" or "make" the call(s) or text(s) in question
- Defendants have successfully argued that simply creating the platform by which others generate communications does not suffice. User involvement is key.
  - *McKenna v. WhisperText*, No. 5:14-cv-00424-PSG, 2015 WL 5264750 (N.D. Cal. Sept. 9, 2015) (text message inviting plaintiff to join platform did not violate TCPA because the platform could only send these texts at the affirmative direction of a user).
  - *Glauser v. GroupMe, Inc.*, No. 11-cv-2584 PJH, 2015 WL 475111 (N.D. Cal. Feb. 4, 2015) (application that allows users to create a "group" whose members would automatically receive pre-programmed welcome texts not an ATDS).

TCPA Litigation: *What Is An ATDS?*

- Courts have been split as to whether a device's "capacity" is limited to its present capabilities, or includes its potential functionalities
- The FCC has come down on the side of potential functionalities – but it is not clear how "attenuated" that potential may be
- Even following the July 2015 Order, at least one court has suggested that the theoretical ability to modify or adapt a device to autodial numbers does not bring the technology within the scope of the TCPA

TCPA Litigation: *What Is An ATDS?,*con't.

- *See Derby v. AOL, Inc.*, No. 5:15-cv-00452-RMW (N.D. Cal. Sept. 11, 2015) ("the [2015 Ruling] does not eliminate the requirement that an [ATDS] under the TCPA operate without human intervention")
- *But see Dominguez v. Yahoo, Inc.*, No. 14-1751, 2015 WL 6405811 (3d Cir. Oct. 23, 2015) (noting that per the July 2015 Order, "so long as the equipment is part of a 'system' that has the latent 'capacity' to place autodialed calls, the statutory definition is satisfied" and remanding for further factual development on that point)

TCPA Litigation: *Is There Consent?*

- Whether putative class members provided consent is individualized issue that has been found to preclude class certification
  - *See, e.g., Shamblin v. Obama for Am.*, No. 13-2428, 2015 U.S. Dist. LEXIS 54849 (M.D. Fla. Apr. 27, 2015) (issue of consent not susceptible to classwide proof)
- Whether consent was revoked likewise requires individualized inquiry that undermines commonality
  - *See, e.g., Gannon v. Network Telephone Services, Inc.*, et al., No. 13-56813, 2016 WL 145811 (9th Cir. Jan. 12, 2016)
  - Fact that consent can be revoked *by any* reasonable means per the July 2015 Order may yield even more individualized issues
  - Are the members of the class even ascertainable?

TCPA Litigation: *Open Issues*

- Vicarious liability
  - Courts are split on whether companies can be held vicariously liable for their agents' calls in violation of the TCPA
    - *Compare Thomas v. Taco Bell Corp.*, 582 F. App'x 678, 679-80 (9th Cir. 2014) (company not vicariously liable for text messages sent by third parties); *with Gomez v. Campbell-Ewald*, 768 F.3d 871 (9th Cir. 2014) (companies are not shielded from TCPA liability by using third-party marketing company)
  - Not addressed in July 2015 Order

TCPA Litigation: *Open Issues*

- Aggregate damages
  - TCPA does not address whether statutory damages should be assessed per communication or per violation
  - *See, e.g., Lary v. Trinity Physician Fin. & Ins. Servs.*, No. 14-11036, 2015 WL 1089326 (11th Cir. March 13, 2015) (fax violated two TCPA subsections; plaintiff could recover damages for both violations).

Questions?

Alan Schoenfeld, Partner (New York)
alan.schoenfeld@wilmerhale.com
212.937.7294

**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.*

Trends in Data Security and Privacy Civil Litigation

Litigation Under the Video Privacy Protection Act (VPPA)

March 21, 2016

Jonathan Cedarbaum, Partner (Washington, DC)

Attorney Advertising

WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP ®

Road Map

I. Overview and key issues
II. Who qualifies as a video tape service provider?
III. Who qualifies as a consumer?
IV. What exactly is personally identifiable information (PII)?
V. When is a disclosure of PII knowing?
VI. Some best practices

Background

- Enacted in 1988 “to preserve personal privacy with respect to the rental, purchase, or delivery of video tapes or similar audio visual materials” after a newspaper published then-Supreme Court nominee Robert Bork’s video rental history. Pub. L. No. 100-618, 102 Stat. 3195 (1988).

- Generally prohibits any “video tape service provider” from knowingly disclosing “personally identifiable information” about a “consumer” to third parties without the consumer’s consent. 18 U.S.C. § 2710(b).

- Allows for statutory damages of $2,500 per violation, punitive damages and attorneys’ fees. Id. § 2710(c).

Companies Face a Rapidly Changing Landscape

- Very few cases in the two decades following passage
- Beginning in 2011, plaintiffs advanced new theories seeking to broaden the scope of the VPPA to apply to online viewing platforms and delivery models that did not exist in 1988
- Law has evolved rapidly as federal courts across the country consider whether and how the VPPA applies to these complex new technologies
- Continued evolution of the VPPA could loom large in privacy law, as more companies offer streaming video content and enhanced user profile capabilities, and share information with third parties for analytics and advertising purposes

Key Issues in Recent VPPA Litigation

- Most class actions under the VPPA involve allegations that a streaming video provider disclosed class members' viewing histories to third parties without obtaining consent
- Recent litigation developments shed light on the many ways to defend against such allegations
  - Defendant may not be a "video tape service provider"
  - Plaintiffs may not be "consumers"
  - Defendant did not disclose "personally identifiable information"
  - If defendant did disclose PII, it was not a "knowing" disclosure

Who Qualifies As a Video Tape Service Provider?

- Defined as “any person, engaged in the business . . . of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials[.]” 18 U.S.C. § 2710(a)(4).

- In recent litigation, courts have held that providers of online streaming services are “video tape service providers”
  - Despite lack of physical video tapes, online streamed content held to fit within the ambit of “similar audio visual materials”

Who Qualifies As a Video Tape Service Provider?, con't.

- *In re Hulu Privacy Litig.*, No. 11-cv-3764, 2012 WL 3282960, at *5-*6 (N.D. Cal. Aug. 10, 2012) ("The court concludes that Congress used 'similar audio video materials' to ensure that VPAA's protections would retain their force even as technologies evolve.")
- *In re Nickelodeon Consumer Privacy Litig.*, MDL No. 2443, 2014 WL 3012873, at *9 n.9 (D.N.J. July 2, 2014) ("The Court notes that the only other court to address the issue of whether providers of streaming videos are VTSPs has found that they are, at least for pleading purposes. Viacom does not suggest a persuasive reason why the *Hulu* Court's conclusion was incorrect.")

Who Qualifies As a Consumer?

- Defined as a “renter, purchaser, or subscriber of goods or services from a video tape service provider.” 18 U.S.C. §2710(a)(1).

- Recent decisions have held that users who do not make some sort of commitment to a provider are not “subscribers” and therefore not “consumers”
  - *Ellis v. Cartoon Network, Inc.*, 803 F.3d 1251 (11th Cir. 2015) (holding that “downloading an app for free and using it to view content at no cost is not enough to make a user of the app a ‘subscriber’ under the VPPA”)

Who Qualifies As a Consumer?, cont.

- *Austin-Spearman v. AMC Network Entm't LLC*, 98 F. Supp. 3d 662, 668-71 (S.D.N.Y. 2015) ("casual consumption of web content, without any attempt to affiliate with or connect to the provider, exhibits none of the critical characteristics of subscription," and holding that a person who merely visits a provider's website and watches video clips is not a "subscriber")

- But users can make a sufficient commitment without paying for a service
  - *In re Hulu Privacy Litig.*, No. 11-cv-3764, 2012 WL 3282960, at *8 (N.D. Cal. Aug. 10, 2012) (holding that VPPA does not require a plaintiff to have paid for a company's services to be considered a "subscriber")

What Exactly is Personally Identifiable Information (PII)?

- Defined as information "which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710(a)(3).

- Courts are generally in agreement that anonymous, unique device IDs do *not* constitute PII—the information must itself identify an actual person
  - *Robinson v. Disney Online*, No. 14-cv-4146, 2015 WL 6161284, at *7 (S.D.N.Y. Oct. 20, 2015) (holding that an anonymized device serial number, without more, is not PII because such information does not "itself identify a particular person as viewed specific video materials")

What Exactly is Personally Identifiable Information (PII)?, con't.

- *Eichenberger v. ESPN, Inc.*, No. 14-cv-463, 2015 WL 7252985, at *5 (W.D. Wash. May 7, 2015) (PII is "information that identifies a specific individual and is not merely an anonymous identifier")

- However, one district court recently bucked the trend toward a narrower view of PII:

  - *Yershov v. Gannett Satellite Info. Network, Inc.*, 104 F. Supp. 3d 135 (D. Mass. 2015) (holding that a unique device ID, GPS location, and video viewing records, when transmitted together, constitute PII)

When Is a Disclosure of PII Knowing?

- Liability attaches under the VPPA only when a video tape service provider "knowingly discloses" PII to a third party without consent. 18 U.S.C. § 2710(b)(1).

- A recent decision in the *Hulu* litigation sets a high standard for plaintiffs to meet in proving a "knowing" disclosure
  - Hulu would disclose a user's identity (via cookies) and video selections to Facebook when the user's browser executed code to place Facebook's "like" button on Hulu's "watch" pages, whether or not the user "liked" the video.

When Is a Disclosure of PII Knowing?

- The district court explained that plaintiffs "must prove that the video-service provider actually knew that it was disclosing: 1) a user's identity; 2) the identity of the video material; and 3) the connection between the two – *i.e.*, that the given user had 'requested or obtained' the given video material." *In re Hulu Privacy Litig.*, 86 F. Supp. 3d 1090, 1097 (N.D. Cal. 2015).

- The court held that Hulu did not "knowingly" send identifiable information because there was no evidence that it was actually aware that Facebook might connect the separate data points. *Id.* at 1098.

Some Best Practices

- Companies that share user data with third parties should scrutinize the types of information that they are collecting and disclosing, and should ensure that appropriate controls are in place to guard against disclosing PII without consent.
- Companies should carefully evaluate the purposes for which information is being disclosed and whether disclosure may be considered part of the “ordinary course of business” such that potential liability under the VPPA can be avoided. 18 U.S.C. §2710(b)(2)(E).
- In instances where companies are sharing their users’ viewing histories, *e.g.*, through social media, they should review their policies and practices to ensure that they are seeking informed consent from consumers before disclosing. 18 U.S.C. §2710(b)(2)(B).

Video Privacy Protection Act, con't.

- Consent can be obtained electronically, but must be "distinct and separate" from other legal or financial terms
- Companies may obtain a durable consent for up to two years at a time

Looking Toward the Future

- Recent court decisions have generally favored companies that offer streaming video content online by showing appropriate restraint in applying the VPPA to new technologies
- But class action litigation is not likely to slow down anytime soon, especially given that there is no agency to prescribe industry-wide standards under the VPPA
  - Multiple class actions have been filed against a smart-TV manufacturer alleging that it violated the VPPA and other consumer protection laws by collecting and sharing viewing histories with third parties for analytics and advertising purposes
  - Rulings in cases currently on appeal could shift the landscape

Questions?

Jonathan Cedarbaum, Partner (Washington, DC)
jonathan.cedarbaum@wilmerhale.com
202.663.6315

**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.*

Trends in Data Security and Privacy Civil Litigation

European Data Security and Privacy Developments

March 21, 2016

Martin Braun, Partner (Frankfurt/Brussels)

WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP

Litigation in the European Union and the U.S. – Some Key Differences

- No discovery in continental Europe
- Class action litigation hardly exists
- No punitive damages
- Often faster, cheaper
- Different legal traditions in the different European countries
- Partial harmonization through European law
  - Data protection
  - Consumer protection
  - Libel/defamation
  - Conflicts of law, venue

A Series of Significant Cases before the European Court of Justice

- Privacy as a fundamental human right (*Digital Rights Ireland, Google Spain, Schrems*)
- IP address as personal data (*Breyer* - pending)
- Applicability of European data protection law, jurisdiction of data protection authorities (*Schrems, Weltimmo, Verein für Konsumenteninformation* - pending, *Wirtschaftsakademie Schleswig-Holstein* - pending)
- Liability of intermediaries (*McFadden* - pending)
- Effective enforcement of IP rights vs. privacy (*Coty Germany, Promusicae*)
- New cases regarding data retention (*pending*)

Civil and Consumer Protection Law-Driven Litigation Is Becoming More Relevant than Regulatory Litigation

- Litigation started by consumer protection organizations against unfair terms in privacy policies, unlawful data processing activities (Germany, France, Netherlands)
  - Privacy as a part of consumer protection?
  - Different legal regimes/traditions which extend far beyond the Data Protection Directive 95/46/EC)
- Cases regarding libel/defamation/personality rights
- Litigation against intermediaries (especially: right to be forgotten)

Civil and Consumer Protection Law-Driven Litigation Is Becoming More Relevant than Regulatory Litigation, con't.

- Effective remedies, damage claims for violations of privacy rights (UK: *Vidal Hall v Google*, Ireland*: CG v Facebook Ireland*)
- "Class Action" (Austria: *Schrems v Facebook*)
- So far: few cases regarding data transfers to the U.S. after *Schrems*
- Continuing strict views of the courts regarding unsolicited emails and messages
- Next big topic: cookies, tracking/profiling

IT Security, Data Breaches and Related Litigation

- Generally awareness of cyber-topics in Europe is increasing, but lagging the U.S. significantly
- Legal framework for (damage) claims is in place, but not used often (yet)
- Legal framework for claims against directors and officers following a breach is in place, but no significant known cases yet (waiting for the “Siemens” moment)

New Legislation

- Network and Information Security Directive of the European Union (“NIS Directive”), and
- EU Trade Secrets Directive of the European Union

Texts have been agreed in December 2015, will be published in the Official Journal in a few months

GDPR

- Text of new “General Data Protection Regulation” was agreed in December 2015, expected to be published this summer
- Full legal effect from 2018
- Applicable to all companies outside the EU that target the European markets and/or track individuals in Europe
- Individuals can sue any organization involved in the data processing (including processors) for full damages; follow-on litigation among involved entities

Additional

- Consumer protection organizations can start lawsuits in the event of non-compliant data processing
- Threat of massive fines by data protection organizations
- Harmonized breach notification obligations

Questions?

Martin Braun, Partner (Frankfurt and Brussels)
martin.braun@wilmerhale.com
+49 69 27 10 78 019

**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.*

Thank You

Martin Braun, Partner (Frankfurt and Brussels)
martin.braun@wilmerhale.com | +49 69 27 10 78 019

Jonathan Cedarbaum, Partner (Washington, DC)
jonathan.cedarbaum@wilmerhale.com | 202.663.6315

Mark Flanagan, Partner (Palo Alto)
mark.flanagan@wilmerhale.com | 650.858.6047

Reed Freeman, Partner (Washington, DC)
reed.freeman@wilmerhale.com | 202.663.6267

Alan Schoenfeld, Partner (New York)
alan.schoenfeld@wilmerhale.com | 212.937.7294