Litigation Trends in Cybersecurity and Privacy

Jeffrey L. Poston
Clifford J. Zatz
February 24, 2015

The webinar will begin shortly. Please stand by. The slides will be sent to you after the event.
Jeff is co-chair of the firm’s Privacy and Cybersecurity Group and a member of the Litigation Group. He is a trial attorney by trade focused on counseling and defending clients in complex data protection matters involving class actions and regulatory enforcement actions.

He has represented clients in a variety of industries in matters involving privacy and protection of personal information. This includes defending and counseling clients in class actions asserting violation of the Telephone Consumer Protection Act (“TCPA”).

Jeff has represented healthcare companies involved in some of the largest alleged data breach cases brought under the federal Hi-Tech Act and various state privacy, data security and unfair competition laws. Jeff has negotiated favorable settlements of these claims with state regulators and attorneys general. Recently, he was part of a litigation team that obtained a dismissal of nine consolidated class actions in the Eastern District of California, alleging that a national healthcare company violated the California Medical Information Act ("CMIA") by disclosing the data of over one million members.

Jeff also counsels clients on front-end compliance issues involving the continuance of state and federal privacy laws, including HIPAA, and the TCPA.
Cliff Zatz, Partner – Washington, DC

Cliff is a trial lawyer and chairs the firm's Product Liability & Torts Group. Cliff has litigated product liability, toxic tort, environmental, wrongful death, defamation, breach of contract, intellectual property, and other cases.

For almost thirty years, Cliff has defended personal injury and property damage cases involving consumer, occupational, and environmental exposure to chemicals and other products. He has represented clients in individual, class action, and community-wide exposure cases. He has tried cases arising out of environmental exposure to trichloroethylene, vinyl chloride, PCBs, and dioxins; formaldehyde in home insulation; and occupational exposure to benzene and isocyanates.

Cliff has advised and represented companies on product liability issues involving automotive products, alcoholic beverages, cellular telephones, sunscreen, and food products. He has defended patent cases involving digital cellular telephone technology, contact lens solution, and the design patent on the "scrunchie" fabric-covered ponytail holder.

Cliff has also litigated OSHA, worker's compensation, and labor and employment discrimination cases before trial and appellate courts, arbitrators, and administrative agencies.
Litigation Hot Areas

1. Continuing PII Class Actions

2. Internet of Things Class Actions

3. Plaintiffs’ Bar Special: TCPA Class Actions
Loss/Theft of Data

- State Regulators
- Law Enforcement - Police - FBI
- Incident Response Plan
- SEC Disclosures
- Business Reputation
- Vendor Involvement/Indemnity
- Internal Investigation/Forensics
- Insurance Coverage
- Individual Notifications
- Class Actions
- Federal Regulators - FTC - OCR
- State AG Notification/Enforcement
- Class Actions
What Do You Do If You Are Breached/Hacked?
If You Don’t Know Now, You’ve Lost
Be Prepared with a Living, Breathing Incident Response Plan

Incident Response Plan

• GC’s Office
• Privacy Office
• IT
• Outside Counsel
• Forensics Firm
• Media Relations
• Dry Runs/Table Top Exercises
• Training/Policies to Ensure Incident Reported Up the Chain
• Risk Assessments
• Vendor Oversight
Weak Link = Vendors

• Vendors are the source of 42%\(^1\) of security breaches
• Vendors can help or hurt your privacy/cyber compliance
• Choose savvy vendors with established policies and procedures around privacy/cyber
• Vet your vendors in advance (especially those handling sensitive or personal information)
  – Questionnaires
  – Audits
  – Certification to standards
  – Evaluation of policies and procedures
  – Notice around non-compliance

\(^1\) Source: Ponemon Institute: U.S. Cost of a Data Breach Study 2013
Vendor Issues When Litigation Hits

• Joint Defense Agreement
• Who is notifying members?
• Liability for Vendor Conduct
• Need to think ahead to class litigation
• Need to understand scope of indemnity
  – Timing of claim
  – Tolling agreement
• If ultimate position is common - *e.g.*, class suffered no injury, then need united front in public while deferring any fight with vendor
Recent High-Profile Incidents

Target (Disclosed on 12/19/13)
  – MDL with over 100 named plaintiffs
  – Suits by banks
  – Congressional hearings

Sony (Disclosed on 11/24/14)
  – 7 class actions/pending
  – Congressional hearings

Anthem (Disclosed on 1/29/15)
  – 17 class actions already filed
  – State AGs investigation
Litigation Theories

• Negligence (failure to adequately protect PI)
• Unfair business practices
• Federal statutes
  – FCRA
  – Wiretap Act
  – Stored Communications Act
• State statutes
  – CMIA
• Unjust enrichment
• Notification delay
• Breach of privacy rights
Threshold Defense: Article III Standing

**Injury in fact:**

An invasion of a legally protected interest which is:

a) Concrete and particularized; and

b) Actual or imminent, not conjectural or hypothetical
Standing is Key

PRE-CLAPPER:

  - 11th Circuit reverses the District Court which had dismissed the case for failure to state a cognizable injury
  - Stolen laptops were unencrypted
  - Plaintiffs alleged identity theft occurred 10-14 months after the theft
  - Plaintiffs had taken precautions to protect the information
  - The 11th Circuit held that the plaintiffs alleged injury in fact sufficient to meet the *Twombly / Iqbal* standards

- **Krottner v. Starbucks, 628 F.3d 1139 (9th Cir. 2010)**
  - Stolen laptop with 97,000 SSNs
  - Court ruled that “increased risk of harm” conferred standing

• FISA allows surveillance of non-U.S. individuals.
• Plaintiffs (U.S. citizens, some of whom were attorneys) argued that they would inevitably be wiretapped in violation of the Constitution
• 2nd Circuit ruled that plaintiffs had standing as there was an “objectively reasonable” likelihood that the government would intercept their communications
• The Supreme Court reverses:
  – The injury must be sufficiently concrete and imminent
  – Threatened injury must be “certainly impending”
  – Can’t rely on a speculative chain of possibilities, and cannot manufacture standing by inflicting harm on themselves
Post-Clapper

*In re Barnes & Noble Pin Pad Litigation*, 1:12-cv-08617 (N.D. Ill. 2013)

- Hackers steal credit card information
- Plaintiffs alleged inadequate protection of the PII, and increased risk of identity theft as well as emotional distress
- Court dismisses the case relying on *Clapper*
  - No actual injury
  - No “certainly impending” injury
  - No allegation of actual theft

*See also Linkedin User Privacy Litigation* (N.D. Cal 3/6/13)
Post-Clapper


- 2011 breach of 3 public networks, compromising unencrypted names, birth dates and passwords for 100 million users
- Putative class alleges 51 claims; the Court dismisses 43, but rejects the *Clapper* standing arguments
- The Court relied on *Krottner*, holding that the PII was wrongfully disseminated thereby increasing the risk of future harms
- The Court concluded that *Clapper* did not “tighten” the standing framework, but rather reaffirmed it
- Legal obligation to provide “reasonable network security” to protect users' personal data
- Court dismissed the negligence claims for failure to satisfy causation and cognizable injury requirements
- The Court allowed the unfair competition claims to proceed
Post-Clapper

Remijas v. Neiman Marcus Grp., LLC
(N.D. Ill. 9/16/14)

• Plaintiffs claimed increased risk of future harm

• Court granted Motion to Dismiss based on failure to allege that “the risk of identity theft is sufficiently imminent to confer standing”
Post-Clapper

*In re Target Corp. Customer Data Sec. Breach Litig.* MDL 14-2522 (D. Minn. 12/18/14)

- Plaintiffs sufficiently pled standing
- Alleged unlawful charges, blocked access to bank accounts, late payments
Here Come The Regulators

• Be proactive with regulators
• Establish relationship/bring them in the loop
• You don’t want them to find out about this second hand
• Make sure they know the situation is fluid and you will update them
Notification Issues

• State Breach Notification Laws
  – States plus D.C., Puerto Rico, and Virgin Islands
  – 47 different standards, some involving “risk of harm”
  – AGs have enforcement authority
  – Timing: “in the most expedient time possible,” “without unreasonable delay”
  – If required to notify in some states, notify in all states

• Who notifies – you or your vendor?

• Don’t sugarcoat notification letter

• What do you do if you cannot determine extent of incident?
  – Notify everyone?
  – Notify no one?
Anthem Incident

• Did everything right
  – Quick detection
  – Got out in front of it and disclosed to public

• No good deed goes unpunished
  – 10 AGs initially laud response
  – One week later publicly criticize for lack of individual notification
  – Complete disconnect
Internet of Things Litigation

- Next frontier in litigation and regulatory enforcement
- Technology getting ahead of regulation
- FTC and State AG focus
Internet of Things Issues

- Ubiquitous collection of data
- Difficult to anonymize data
- Unbeknownst to consumers
- Notice and consent are difficult
- No real consumer choice/ability to opt out
- Almost anything is hackable and there may be limited ability to disclose improper use of data
Cyber Security Meets Product Liability

Cyber Security Meets Product Liability

- Hacker announces “stupidly simple” way to access site code and memory of hotel key card systems

- Widely publicized in *Forbes* and other news media

- Four million affected locks in hotels around the world

- Five nationwide class actions filed by hotel owners and operators alleged:
  - Negligence
  - Breach of express warranty
  - Breach of implied warranty
  - Magnuson-Moss Warranty Act
  - Unjust enrichment
Cyber Security Meets Product Liability

• Does hackability = liability?

  – Is vulnerability to hacking a “defect”?

  – Is it an “inherent” defect? A “manifest” defect?

  – Is such a defect alone an “injury”?

  – Is a warranty against hackability implied?
Cyber Security Meets Product Liability

• Motion to dismiss granted

• No Article III standing
  – No “certainly impending” injury under Clapper
  – “Defect” alone ≠ actual, present injury
  – Access would require criminal act by third party
  – Fear of injury does not create standing
Cyber Security Meets Product Liability

• The “Lost Data” Analogy

  – Data breach cases: no injury absent actual identity theft or abuse of personal data

  – Costs incurred in response to risk of hotel room breach are not “injury”

  – Hotel locks are not “doomed to fail”

  – No unauthorized entry into any plaintiff’s property unless and until third party “succeeds in exploiting the defect”
What’s different about this kind of suit?

- It’s about product integrity, not privacy
- Hacker isn’t seeking personal information
- Hacker’s goal is to take control of or compromise the product
- Defendant is a manufacturer, not a data collector
- All sellers in the chain may be strictly liable
- Regulatory compliance or industry standard isn’t necessarily a defense. Must think outside the regulatory box
Cyber Security Meets Product Liability

• Implications: What if hackability *does* equal liability?

• “All your devices can be hacked.”
  [http://www.ted.com/talks/avi_rubin_all_your_devices_can_be_hacked?language=en](http://www.ted.com/talks/avi_rubin_all_your_devices_can_be_hacked?language=en)

  • Medical devices (FDA guidelines)
  • Cars (Markey report)
  • Home security systems, baby monitors
  • Smart phones, smart TVs
  • Internet of Things (FTC staff report)
Cyber Security Meets Product Liability

“\textit{In their initial tests with a laptop...[researchers] were able to cause cars to suddenly accelerate, turn, kill the brakes, activate the horn, control the headlights, and modify the speedometer and gas gauge readings.}”
Cyber Security Meets Product Liability

- TRENDnet
  - FTC’s first Internet of Things enforcement action
  - Hacker accessed and posted links to “secure” live camera feeds
  - Publicly displayed “babies asleep in their cribs, young children playing, and adults going about their daily lives”
  - Failure to adequately secure cameras as deceptive and unfair trade practice
  - TRENDnet as both product manufacturer and collector of sensitive data
A Few Thoughts About the Sony Hack

• It’s about your own security and privacy, too.
  – Private information of more than 15,000 current or former employees allegedly stolen
  – Embarrassing internal communications made public

• Reminder: Hackers can have a variety of motives.
  – Competitive advantage
  – Damage to reputation
  – Revenge
  – Embezzlement
  – Theft of trade secrets and IP
  – Theft of marketing plans, customer lists, pricing information
  – Suspension/debarment
  – Case in point: KGL v. Doe defamation suit
A Few Thoughts About the Sony Hack (cont’d)

• When your e-mails and documents are stolen:
  – No privilege claims
  – No relevance or burden objections
  – No protective order
  – No protection from document retention policy
  – No limit to further dissemination

• When they’re gone, they’re gone

• More than ever, be careful what you create
TCPA Overview

• Prohibits calls to numbers on “Do Not Call” list. 47 U.S.C. §227(c)

• Restrictions automated marketing calls, texts, and faxes. (“Robo Calls”) 47 U.S.C. §227(b)

• Must have prior express consent to contact consumers using automated systems, artificial callers and prerecorded messages.
  – There is no “established business relationship” exception anymore.
  – Manually dialed calls with no pre-recorded message are permissible.

• Telemarketers using automated devices to self-identify and reveal contact information in the message.
  – New rules require automated opt-out mechanism.

• Vicarious liability “On Behalf Of”

• HUGE RISKS: penalties are $500 to $1500 per violation, very active class action bar.
TCPA Settlements: Last 6 Months

- Comenity Bank, S.D. Cal.: $8.5m
- AT&T Mobility, D.Mont.: $45m
- Bank of America, C.D.Cal: $32m
- Capital One, N.D.Ill.: $75.5m
- TruGreen, N.D.Ill.: $4.5m
- LA Clippers, C.D.Cal.: $5m
- Best Buy, W.D.Wash.: $4.5m
“On Behalf Of” Liability

• Conduct and liability of telemarketers imputed to “Seller”

• *United States of America v. Dish Network* (C.D. Ill. 12/11/14)
  – Dish Network liable for 57 million illegal calls
  – Court found “agency” based on support to telemarketers and knowledge of unlawful activities
  – US Gov: Theoretically $725 billion in statutory damages

• Motion for Reconsideration partially granted as agency between Dish and retailers disputed