Data Breach Litigation: 
Empirical analysis and 
Current trends

Tonia Klausner, Wilson Sonsini Goodrich & Rosati, PC

Sasha Romanosky, RAND

11/6/2013
How is US policy addressing harms caused by data breaches?

• “Should a baseline data privacy legislation include a private right of action?” (Commerce 2010)

• Individuals use any means available to sue firms for alleged harms caused by data loss.

• However, very little is known about these suits.

• How to balance the firm’s right to collect and innovate using PII with an individual’s right to privacy?
Examples of data breaches

- Thief steals personal information (SSN, etc), and files a fraudulent tax refund.

- Pharmacy tosses medical files and employment applications in the trash (In re Rite Aid Corp., FTC File No. 072-3121).

- Social Security Administration discloses HIV results of a pilot to the FAA (Cooper v. FAA, 596 F. 3d 538).

- Financial payment processor is hacked, compromising 130 million credit card numbers (In re Heartland Payment Systems).
Research questions

Q1: When are firms more likely to be sued (in federal court)?
• Helps firms identify what they can do to avoid litigation.

Q2: Which data breach lawsuits settle?
• Helps understand how the legal system is addressing privacy harms.

Definitions
• Data breach: unauthorized disclosure of personal information
• Disclosure: loss/theft hardware, cyberhack, or improper disposal
• Personal information: SSN, credit card, medical, financial, etc.
Data collection

• Obtained list of all reported data breaches (datalossdb.org)

• Used Westlaw to determine which breaches were federally litigated.

• Purchased docket filings from PACER; manually coded dozens of variables involving the breach and case characteristics.

• 1,772 data breaches (2005-2010), 230 federal lawsuits
What do these suits typically look like?

- Usually private class actions (some FTC, SEC).
- Defendants are typically large firms (e.g. banks, retailers).
- Complaints allege both common law (tort, contract) and statutory causes of action (VPPA, DPPA). Almost 90 unique causes of action for virtually the same event!
- Plaintiffs seek relief for actual loss, preventive costs, potential future loss, emotional distress.
- Disposition: only 2 cases have reached trial, all others are either dismissed or settled.
Litigation rate is ‘typical’ at 3-4%

Breach and lawsuit trends

Litigation rate
Results Q1: Which breaches are being litigated?

- Breaches are more likely to be litigated if they:
  - *show evidence of actual harm (financial loss):* 3.5 times
  - *involving loss of financial information:* 6 times
  - *caused by improper disclosure of information:* 3 times

- Breaches are less likely to be litigated with offers of free credit monitoring: 6.5 times
Q2: Which data breach lawsuits settle?

Count of dismissed and settled lawsuits

Settlement rate
Results Q2: Which cases are settling?

- Firms are 30% more likely to settle when:
  - plaintiffs allege actual (financial) harm, and
  - class is certified (increase from 47% to 60%)

- Surprisingly, statutory damages were not found to drive settlement

- But, are defendants settling too often?:

<table>
<thead>
<tr>
<th></th>
<th>No harm (n=135)</th>
<th>Actual Harm (n=28)</th>
</tr>
</thead>
<tbody>
<tr>
<td>% of lawsuits</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dismissed</td>
<td>51%</td>
<td>29%</td>
</tr>
<tr>
<td>Settled</td>
<td>49%</td>
<td>71%</td>
</tr>
</tbody>
</table>
What does this suggest about effectiveness of current legal system?
What do we know about settlement awards?

- Additional awards include redress for idtheft losses and expenses, cy pres awards to research, non-profits, charities.

- E.g. $50k, $2.8m, $5m, $6m, $8m, $9.5m.

<table>
<thead>
<tr>
<th></th>
<th>Mean</th>
<th>Min</th>
<th>Max</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attorneys get</td>
<td>$1.2m</td>
<td>$8k</td>
<td>$6.5m</td>
<td>15</td>
</tr>
<tr>
<td>Named Plaintiffs get</td>
<td>$2.5k</td>
<td>$500</td>
<td>$15k</td>
<td>19</td>
</tr>
</tbody>
</table>
Standing

Historically Best First Line of Defense


“First, a plaintiff must demonstrate that she has suffered an injury in fact which is actual, concrete, and particularized. Second, the plaintiff must show a causal connection between the conduct complained of and the injury. Third, the plaintiff must establish that the injury will be redressed by a favorable decision. The plaintiff has the burden of establishing each of these three requirements.”

“More than three years after the theft, Plaintiff has not alleged that she has suffered anything greater than an increased risk of identity theft. Because Plaintiff has not alleged that she has suffered any concrete damages, she does not have standing under the case-or-controversy requirement.”
Standing

More recent split of authority
1st & 3rd Cir. vs. 9th & 7th Cir.

“We conclude that Appellants' allegations of hypothetical, future injury are insufficient to establish standing. Appellants' contentions rely on speculation that the hacker: (1) read, copied, and understood their personal information; (2) intends to commit future criminal acts by misusing the information; and (3) is able to use such information to the detriment of Appellants by making unauthorized transactions in Appellants' names. Unless and until these conjectures come true, Appellants have not suffered any injury; there has been no misuse of the information, and thus, no harm.”

“If a plaintiff faces ‘a credible threat of harm’ and that harm is ‘both real and immediate, not conjectural or hypothetical,’ the plaintiff has met the injury-in-fact requirement for standing under Article III. Here, Plaintiffs-Appellants have alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data.”
Strength added to standing argument by U.S. Supreme Court?


- """"[W]e have repeatedly reiterated that ‘threatened injury must be *certainly impending* to constitute injury in fact,’ and that ‘[a]llegations of *possible* future injury’ are not sufficient.”

- Rejects "objectively reasonable likelihood" standard as inconsistent with requirement that threatened injury must be certainly impending

- "[R]espondents' theory of standing, which relies on a highly attenuated chain of possibilities, does not satisfy the requirement that threatened injury must be certainly impending.”

- "Respondents' contention that they have standing because they incurred certain costs as a reasonable reaction to a risk of harm is unavailing--because the harm respondents seek to avoid is not certainly impending. In other words, respondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.”
Second Line of Defense: No Damages/Failure to State a Claim

- **Krottner v. Starbucks Corp., 406 Fed. Appx. 129 (9th Cir. 2010):**
  
  "Plaintiffs-Appellants have not established a cognizable injury for purposes of their negligence claim. Under Washington law, ‘[a]ctual loss or damage is an essential element in the formulation of the traditional elements necessary for a cause of action in negligence . . . . The mere danger of future harm, unaccompanied by present damage, will not support a negligence action.’"

- **Pisciotta v. Old National Bancorp, 499 F.3d 629 (7th Cir. 2007):**
  
  Both negligence and breach of implied contract claims require “a compensable injury”
  
  No Indiana case on point to looked to state data breach statute: “The narrowness of the defined duties imposed, combined with state-enforced penalties as the exclusive remedy, strongly suggest that Indiana law would not recognize the costs of credit monitoring that the plaintiffs seek to recover in this case as compensable damages.”

- Standing found because some plaintiffs information had actually been used
- First Cir. found cognizable injury to support negligence and implied contract claims based on foreseeable mitigation expenditures
- Four named plaintiffs moved for certification of a class of customers who incurred out-of-pocket costs in mitigation efforts that they undertook in response to learning of the data intrusion
- Plaintiffs offered no class-wide proof on total damages, leaving court with prospect of a trial involving individual issues for each class member as to what happened to his/her data and account, what he/she did about it, and why – therefore individual issues predominated over common questions
Trends in Litigation

Cases brought:

• New theories of standing

• Away from negligence/breach of contract and towards unfair and deceptive business practices claims

• From data breach to data collection and use
FTC Investigations/Actions

• The FTC views privacy and data security enforcement as a critical component of its consumer protection function.

• Authority: Section 5 of the FTC Act, 15 U.S.C. S 45, prohibits unfair or deceptive acts or practices in or affecting commerce.

• FTC enforcement actions have focused on:
  – Failures to keep promises to maintain security of personal information
  – Failures to adequately safeguard the privacy of consumer information
Has the FTC gone too far?


- FTC alleged that Wyndham data security practices that resulted in data breaches were unfair and deceptive in violation of the FTC Act
- Wyndham’s motion to dismiss (dkt no. 91 filed 4/26/13) challenges FTC’s authority over data security practices as unfair
  - “[T]he FTC argues that the general language of Section 5 gives it the broad authority to set data-security standards for *any* American business operating in *any* industry. No court has ever held that Section 5 gives the FTC such unbounded authority.”
  - Relies on *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120 (2000): “‘[W]here the scope of [an] earlier statute is broad but . . . Subsequent statutes more specifically address the topic at hand,’ the ‘later federal statute[s] should control [a court’s] construction of the [earlier] statute.’”

**In re LabMd Inc., Docket No. 9357 (FTC)**

- FTC alleged that LabMD's failure to employ "reasonable and appropriate measures" to prevent unauthorized access to lab patients' personal information constituted an unfair act or practice
- LabMD’s answer challenges the FTC’s authority over data security practices
Two Pre-Breach Defenses

1. Insurance
   - You will have a breach
   - It will be expensive even if ultimately no liability attaches
   - There is specific cyber insurance out there to cover the costs of responding to a breach

   - **Stolt-Nielsen SA v. Animal Feeds International Corp., 130 S. Ct. 1758 (2010):** “[A] party may not be compelled under the FAA to submit to class arbitration unless there is a contractual basis for concluding that the party agreed to do so.”
   - **AT&T Mobility LLC v. Concepcion, 131 S. Ct. 1740 (2011):** Federal Arbitration Act preempts state laws that render arbitration agreements unenforceable; “Requiring the availability of classwide arbitration interferes with fundamental attributes of arbitration and thus creates a scheme inconsistent with the FAA.”
   - **But see In re: American Express Merchants’ Litigation, No. 06-1871-cv (2d Cir. Feb. 1, 2012):** finding class action waiver in arbitration provision unenforceable.
QUESTIONS

Tonia Klausner
Wilson Sonsini Goodrich & Rosati PC
tklausner@wsgr.com

Sasha Romanosky, RAND
sromanos@andrew.cmu.edu

11/6/2013