MULTIDISTRICT LITIGATION AGAINST FACEBOOK FOR PRIVACY VIOLATIONS AND EXPLOITATION OF USERS' PERSONAL DATA – FACEBOOK'S DEFENSES

BY LYDIA FERRARESE, ESQ., HERZFELD & RUBIN, P.C.

INTRODUCTION

- Cambridge Analytica's misuse of Facebook's Users' data has led to at least 18 lawsuits since the scandal
- Claims against Facebook include:
  - Privacy Violations (violations of Stored Communication Act - 18 USC 2701, Video Privacy Protection Act – 18 USC 2710, Deceit by concealment or omission- Cal. Civ. Code 1709-1710)
  - Breach of User Agreement
  - Negligence and gross negligence
  - Consumer Fraud
  - Unfair Competition
- Facebook's Main Defense: Lack of Standing

ARTICLE III STANDING

- **Standing**: the legal right to initiate a lawsuit
- **Requirements**[1]:
  - (1) Injury in Fact
  - (2) Causal relationship between the injury and the challenged conduct
  - (3)A likelihood that the injury will be redressed by a favorable decision
- Data privacy case law focuses on point 1 – whether there was an injury in fact

[1] *Lujan v. Defenders of Wildlife*, 112 S. Ct. 2130 (1992)

PLAINTIFFS' ALLEGED INJURIES AND FACEBOOK'S STANDING DEFENSE

Plaintiffs' Allegations

- Substantial threat of identity theft or fraud
- Cognizable injury to privacy interests
- Injury to their property interest

Facebook's Response

- **No substantial threat of identity theft**– data collected by Cambridge Analytical was limited to name, gender, birth date, and photographs posted and tagged in.
- **Fear of hypothetical future harm does not confer standing**
- **No injury to property interest** – fact that FB gained from activity but Plaintiffs did not does not mean there was an injury
- **Ad Targeting** – using limited information provided by Plaintiffs cannot constitute privacy injury.[1]

[1] *See Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016)(Plaintiff must allege facts showing a specific, personal harm with close relationship to harm alleged in lawsuit)

STANDING IN DATA PRIVACY CASES – PRECEDENT

- *Krottner v. Starbucks Corp.*, (9th Cir. 2010)
  - Employees sued Starbucks after a laptop containing their unencrypted personal data (names, addresses, SSNs) was stolen
  - **Held**: Plaintiffs were divided into two classes: those alleging that they had suffered financial loss from the breach had standing as there was a credible threat of real and immediate harm stemming from theft of a laptop containing unencrypted personal data
- *In re Zappos, Inc.*, (9th Cir. 2018)
  - Hackers gained access to names, account numbers, passwords, addresses, and credit card info of 24 million Zappos users.
  - Users filed suit alleging Zappos did not adequately protect data.
  - **Held**: Following *Krottner*, Court held that exposure of names, account numbers, email addresses, billing and shipping addresses, telephone numbers and credit and debit card gave "hackers the means to commit fraud or identity theft."

STANDING IN DATA PRIVACY CASES – PRECEDENT, CONT.

- *Reilly v. Ceridian Corp.* (3rd Cir. 2011)
  - Hackers obtained names, birth dates, bank account information and SSNs of employees of Ceridian's (payroll processing company) client.
  - Plaintiffs alleged: (1) an increased risk of identity theft, (2) incurred costs to monitor credit activity, (3) emotional distress
  - **Held**: hypothetical future injury and money/ time spent monitoring financial information does **not** establish standing. Allegations rely on speculation that:
    - (1) hacker read, copied, and understood information; (2) hacker intends to commit future criminal acts by misusing information; and (3) hacker is able to use such information to detriment of plaintiffs via unauthorized transactions. Money/time spent to monitor financial information does not establish standing.

STANDING IN DATA PRIVACY CASES – PRECEDENT, CONT.

- *Attias v. CareFirst, Inc.* (D.C. Cir. 2019)
  - CareFirst and its subsidiaries are health insurance companies. Hackers obtained names, birth dates, SSNs, and credit card info of customers who subsequently brought a class action suit
  - District Court dismissed for lack of standing, Appeals Court overturned and remanded back to District Court
  - **Held**: Dismissed for failure to state a claim upon which relief could be granted
    - Speculative harm, or threat of future harm not yet realized, is not sufficient to create cause of action
    - Mitigation costs (e.g. credit monitoring) do not constitute actual damages; Benefit of the bargain theory rejected.
    - No duty to reasonably safeguard data separate from any contractual duties:
      - Duty to refrain from causing others harm does not translate to affirmative duty to act
      - Breach was not foreseeable (Plaintiffs did not properly allege this point)
      - Nature of the parties' relationship

STANDING IN DATA PRIVACY CASES – PRECEDENT, CONT.

- *Remijas v. Neiman Marcus Group, LLC* (7th Cir. 2015)
  - Hackers attacked Neiman Marcus and accessed credit card information of over 300,000 customers, some of whom found fraudulent charges on their cards
  - **Held**:
    - Court reasoned Plaintiffs showed risk of harm because "why else would hackers break into a store's database?"
    - **No standing** based on "loss of private information" theory because (1) no property right exists in one's private information, and (2) this would give individuals standing even if they couldn't show a substantial risk of further use of their information
  - NM settled suit for $1.5M in January 2019

FACEBOOK'S OTHER DEFENSES

- Aside from standing, Facebook asserted several other defenses:
  - (1) **Consent** – FB users consented to the terms of use of the website when creating an account. The Data Use Policy informed users that information shared with friends could be disclosed to apps
  - (2) **Exculpatory Clause** – FB's terms and conditions contains language stating that it is not responsible for the actions of third parties
  - (3) **VPPA and Stored Communications Act are Inapplicable** - FB argued that laws, particularly the SCA, do not apply, since the information collected is public
  - (4) **Failure to Identify what Sensitive/ Protected Information was Disseminated-**
  - (5) **No Right of Publicity** – FB relies on case law stating that collection of demographic information has never been deemed a violation of right to publicity. There are no allegations that anyone "merchandised" likeness
  - (6) **Fraudulent Omissions**- No duty to disclose such details (FB disclosed that third party agreement may control)
  - (7) **California Unfair Competition Law-** FB claims that "unfair" conduct under UCL must show the conduct "threatens an incipient violation of an antitrust law, or violates the policy or spirit of one of those laws."
  - (8) **Unjust enrichment**- Not applicable because these is an agreement
  - (9) **Negligence**- Plaintiffs admit the absence of a special relationship between Plaintiffs and FB
  - (10) **Breach of contract-** FB argues that the Data Use Policy clearly discloses that people could share information with third parties

DATA PRIVACY LEGAL DEVELOPMENTS IN THE UNITED STATES

- **California Consumer Privacy Act of 2018 (CCPA)**
  - Applies to businesses that meet any <u>one</u> of the following:
    - Annual gross revenues in excess of $25,000,000
    - Handles data of more than 50,000 people or devices
    - Has 50% or more of its revenue coming from the sale of personal information
  - Gives consumers the right to:
    - Receive notice of what personal information (PI) is being collected and for what purpose
    - Know whether their PI is sold or disclosed, and if so, the categories of third parties to whom it is disclosed
    - Decline sale of PI
    - Access to PI that is collected

THANK YOU