

Data Breaches, Big Data, and FTC Oversight

Pierre Grosdidier

May 4, 2018

haynesboone

© 2015 Haynes and Boone, LLP

The FTC and data security

- Main federal agency re. data security
- Authority in FTC Act
 - 15 U.S.C. 45 (“Section 5”)
- 60+ FTC settlements since 2002
- Key case
 - *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015)
 - Three breaches in 2008–10
 - 600,000 credit card; \$10.6m in fraud
 - Holding: Section 5 authorizes FTC to regulate cybersecurity

haynesboone

© 2015 Haynes and Boone, LLP

FTC v. Wyndham Worldwide Corp.

- It is inequitable to:
 - promise security to attract customers;
 - fail to deliver with poor security;
 - “expose unsuspecting customers” to harm;
 - and keep the profits.

haynesboone

© 2015 Haynes and Boone, LLP

3

FTC Act Sections 5(a), (n)

- “[U]nfair or deceptive acts or practices in or affecting commerce, are . . . unlawful.”
- Unlawful as unfair if “the act or practice
 - causes or is likely to cause substantial injury to consumers
 - which is not reasonably avoidable by consumers themselves and
 - not outweighed by countervailing benefits to consumers or to competition.”

haynesboone

© 2015 Haynes and Boone, LLP

4

In re LabMD, Inc., FTC No. 9357

•



hc

TIVERSA, INC.: WHITE KNIGHT OR HI-TECH PROTECTION RACKET?

© 201

5

In re LabMD, Inc. Complaint

- Complicated procedural history
- Initial Decision: ALJ dismissed the FTC complaint (Nov. 13, 2015)
- Full Commission reverses (July 29, 2016)
- Appeal to 11th Circuit Court
 - June 21, 2017 oral argument
 - “A tree fell and nobody heard it.”
 - “The aroma . . . is that [Tiversa] was shaking down private industry with the help of the FTC.”
 - Still waiting for a decision . . .

haynesboone

© 2015 Haynes and Boone, LLP

6

LabMD: the FTC's arguments

- A company's lax computer security measures create a significant risk of concrete harm and are likely to cause substantial consumer injury.
- *Proof of actual identity theft is not required.*
- Under this argument, Section 5 liability can be imposed merely based on the risk that inadequate security measures will cause a data breach that will cause future harm.

haynesboone

© 2015 Haynes and Boone, LLP

7

LabMD: The ALJ's arguments

- FTC had “proven the ‘possibility’ of harm, but not any ‘probability’ or likelihood of harm.”
- Finding that consumers likely to suffer future harm “would require speculation upon speculation.”
- FTC should concern itself with “substantial” injuries, and not “trivial or merely speculative harm.”

haynesboone

© 2015 Haynes and Boone, LLP

8

LabMD: Commission's arguments

- Release of 1718 File breached Section 5
- 11-month 1718 File exposure is a breach
 - Created “significant risk” of substantial consumer injury
- Commission punts on whether inadequate security alone constitutes a breach
 - “[W]e need not address Complaint Counsel’s broader argument.”

haynesboone

© 2015 Haynes and Boone, LLP

9

LabMD ten years after the breach

- 1718 File exposed for one year
- Only copied by Tiversa
- Not one complaint ever filed
- No evidence of harm
- LabMD is out of business
- LabMD principals filed *Bivens* action
- FBI raided Tiversa’s offices in 03/16

haynesboone

© 2015 Haynes and Boone, LLP

10

LabMD ten years after the breach



© 2015 Haynes and Boone, LLP

11

What's one to do?

- Commission Statement of Jan. 31, 2014
- FTC “does not require perfect security”
- Requires “reasonable and appropriate security” through “***a continuous process***”
- “[N]o one-size-fits-all data security program”
- “[M]ere fact that a breach occurred does not mean” a violation of the law
- FTC-published guidelines

haynesboone

© 2015 Haynes and Boone, LLP

12

FTC publications re. data security

- Protecting Personal Information, 2011
- Start with Security; lessons learned from FTC cases, 2015
- Stick with Security FTC blog
- Cases that did not follow the guidelines:
 - *In re LabMD, Inc.*, FTC No. 9357
 - *In re Adobe Systems Inc. Privacy Litigation*, No. 13-cv-05226-LHK, 2014 WL 4379916 (N.D. Cal. Sept. 4, 2014)
 - *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015)

haynesboone

© 2015 Haynes and Boone, LLP

13

Things LabMD did wrong

- No data purge (100,000 unneeded records)
- No access segregation
- No password policies (“labmd”)
- No unauthorized access detection
- No effective antivirus and firewalls
- No risk assessments
- No security training
- No security program
- Haphazard, reactive, ineffective inspections

haynesboone

© 2015 Haynes and Boone, LLP

14

Things Adobe did wrong

- Hackers stole and decrypted credit card nos.; code
- Quotes from the opinion:
 - “Adobe’s security practices were deeply flawed”
 - “did not conform to industry standards”
 - “encryption scheme was poorly implemented”
 - “Adobe . . . failed to
 - employ intrusion detection systems,
 - properly segment its network, or
 - implement user or network level system controls.”

haynesboone

© 2015 Haynes and Boone, LLP

15



Things Wyndham did wrong

- Three attacks in three years
- Default user ID and password (“micros”)
 - Micros Systems, Inc.
- No firewalls
- Out-of-date operating system
 - No security update in over three years
- No third-party access restrictions
- No unauthorized access detection
- No security investigations

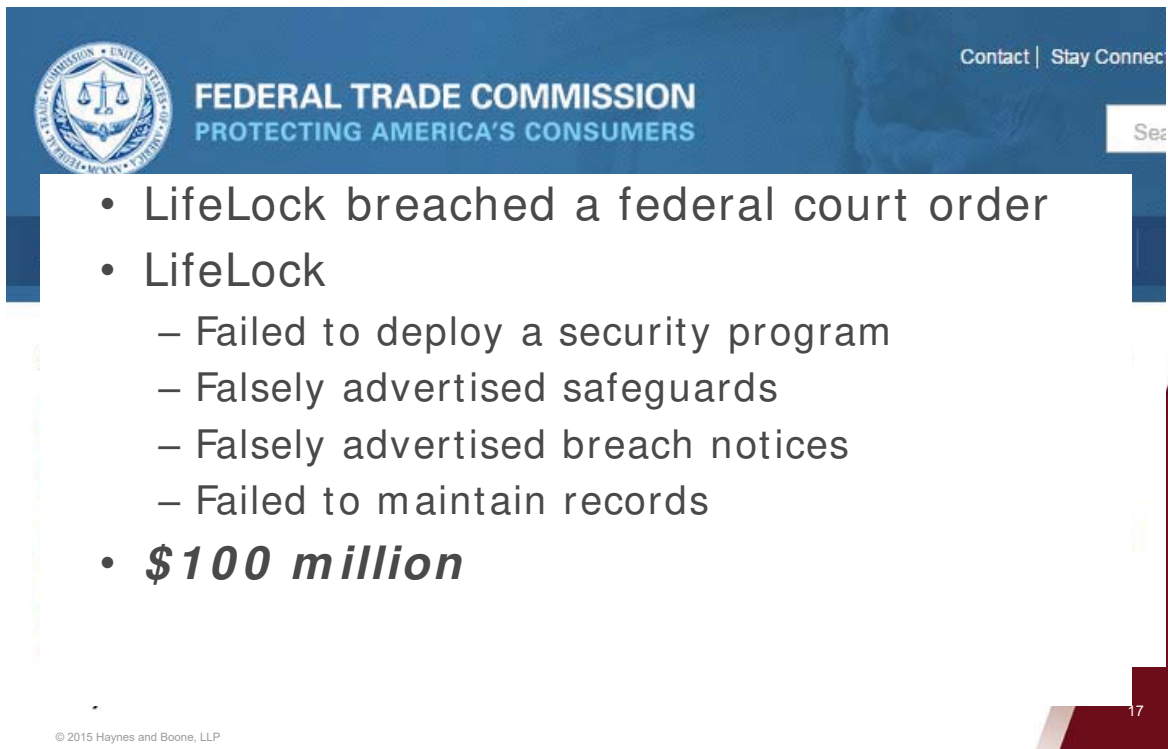
haynesboone

© 2015 Haynes and Boone, LLP

16



LifeLock FTC Penalty



The screenshot shows the Federal Trade Commission (FTC) website. At the top left is the FTC seal. To its right, the text reads "FEDERAL TRADE COMMISSION" and "PROTECTING AMERICA'S CONSUMERS". In the top right corner, there are links for "Contact" and "Stay Connected". Below this, a white box contains a bulleted list of LifeLock's violations and the penalty amount. The background of the website is blue with a faint image of a person's face.

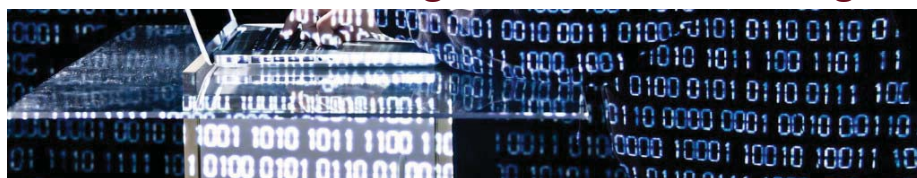
- LifeLock breached a federal court order
- LifeLock
 - Failed to deploy a security program
 - Falsely advertised safeguards
 - Falsely advertised breach notices
 - Failed to maintain records
- **\$100 million**

© 2015 Haynes and Boone, LLP

Do not rest on your laurels



FTC Statement: “security is a continuous process of assessing and addressing risk.”



haynesboone

© 2015 Haynes and Boone, LLP

**Audit your system security
Get second opinion**

Have a data breach plan

- Security is now a Legal-IT joint effort



Data breach consequences & issues

- Huge, costly distraction
 - Forensic and legal investigations
 - Crisis management
- Class actions
 - Consumers
 - Target breach: 10¢ per consumer
 - Vendors
 - Shareholders
 - Banks
 - \$8 per card replacement cost
- Data breach insurance policy terms?

haynesboone

© 2015 Haynes and Boone, LLP

Big Data

- Data stores
 - Internet footprints
 - Transaction history
 - Social media
- Information
 - Conclusions
 - Predictions
 - Decisions

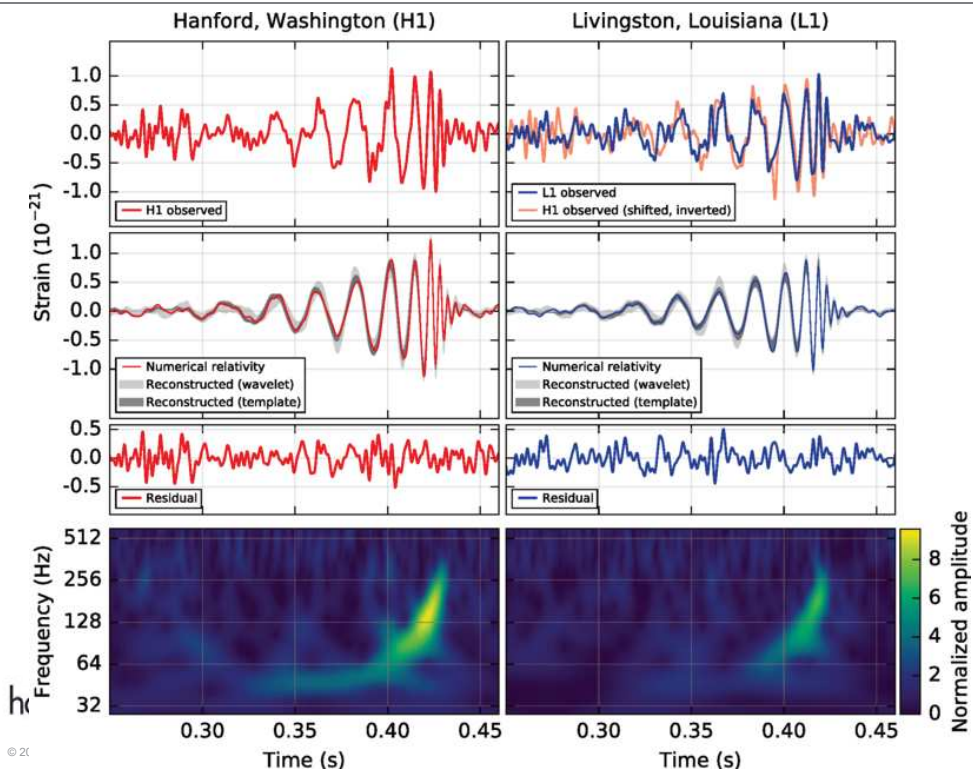


haynesboone

© 2015 Haynes and Boone, LLP

21

Data to information ex. (LIGO)

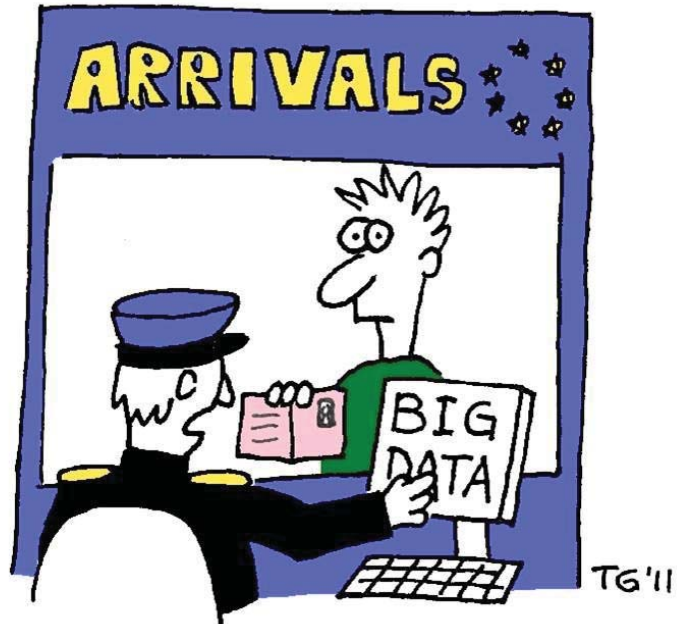


© 2015

22

Big Data

- Applications
 - Targeted advertising
 - Customer selection



“Your recent Amazon purchases, Tweet score, Internet browsing history, and Facebook ‘Likes’ make you 17.3% desirable in this country. Your return flight home is at Gate E23. TY & GB.”

© 2015 Haynes and Doune, LLC

23

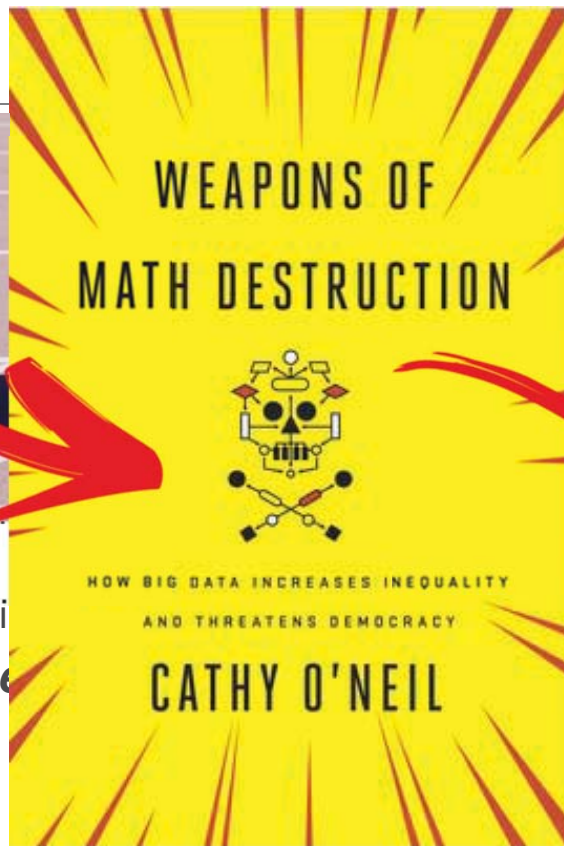
The FTC



- Misuse protection
- **Fact-spe**

haynesboone

© 2015 Haynes and Boone, LLP



g data

Exclusion?

re, and



Four BD issues to keep in mind

- Data set representativeness
 - Bias toward Internet users
- Model bias
 - Model incorporates embedded biases
- Model errors
 - Google Flu Trends did not work
 - Correlation does not mean causation
- “Ethical or fairness concerns”
- *Reminder: concern is the exclusion of “low-income and underserved populations”*

haynesboone

© 2015 Haynes and Boone, LLP

25

Potentially applicable statutes

- Fair Credit Reporting Act
- Equal Credit Opportunity Act
- Title VII of the Civil Rights Act of 1964
- Americans with Disabilities Act
- Age Discrimination in Employment Act
- Fair Housing Act
- Genetic Information Nondiscrimination Act.
- Federal Trade Commission Act

haynesboone

© 2015 Haynes and Boone, LLP

26

Fair Credit Reporting Act

- Big data use to prepare and sell reports that are used to make consumer-related eligibility decisions might be considered credit reporting agencies subject to the FCRA
 - employment, credit, housing
- Even companies that merely purchase and use this information might have their own FCRA obligations that are intended to protect consumers

haynesboone

© 2015 Haynes and Boone, LLP

27

FCRA Safe harbor

- FCRA does not apply to companies when they use data derived from their own relationship with their customers for purposes of making decisions about them
- *Other federal statutes might apply*

haynesboone

© 2015 Haynes and Boone, LLP

28

FTC Act

- Risks of
 - Misrepresenting big data use
 - “Big data” data breach
 - Selling data to fraudsters or identity thieves

Takeaways

- Data security
 - Take data security seriously
 - Joint effort between Legal and IT
 - Have a data breach plan
- Big data
 - Think through the use of big data
 - Understand the analytics
 - Protect the data

haynesboone

© 2015 Haynes and Boone, LLP

Find the full text of this and thousands of other resources from leading experts in dozens of legal practice areas in the [UT Law CLE eLibrary \(utcle.org/elibrary\)](https://utcle.org/elibrary)

Title search: Data Breaches, Big Data, and FTC Oversight

Also available as part of the eCourse

[Answer Bar: Global Data Security Considerations for the Corporate Client](#)

First appeared as part of the conference materials for the
2018 STUDIO WEBCAST: Data Breaches, Big Data, and FTC Oversight session
"Data Breaches, Big Data, and FTC Oversight"