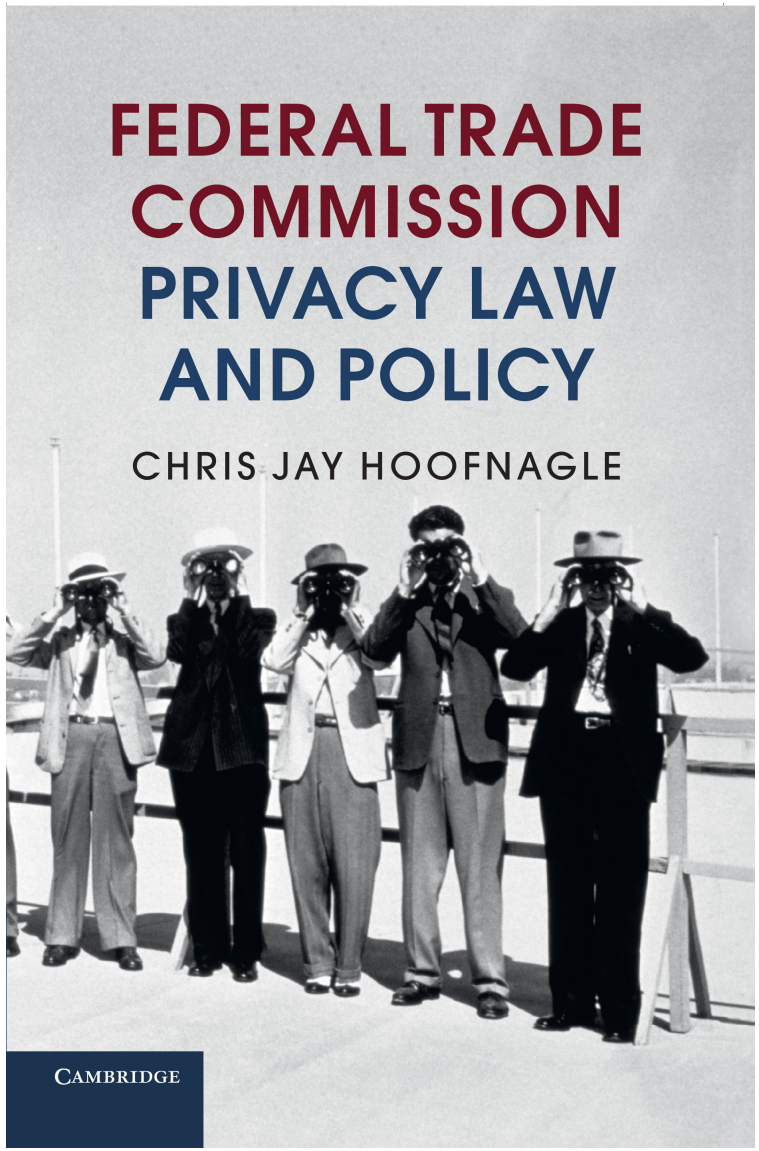
Consumer Protection as Cybersecurity Law

Chris Hoofnagle, Adjunct Professor,
UC Berkeley School of Information & School of Law

Harvard Kennedy School Cybersecurity Project
Speaker's Series
March 25, 2019



Current research agenda

- Law and policy implications of the second quantum revolution
  - Quantum metrology & sensing
  - Communications
  - Computing
- Starting a cybersecurity book project with a goal of connecting the different disciplinary threads and assumptions of the field.
  - Where are they congruent, incongruent?
  - Is there a way to create useful, cross-disciplinary discussion to erode cyber's fundamental challenges

Roadmap for today: Consumer Protection as Cybersecurity Law

1. The FTC's history shapes its ability to police consumer protection
2. How the FTC regulates surveillance, cyber
3. The President Trump FTC & looking ahead

n.b. much of my talk today is based on ***The Role of the Federal Trade Commission in Regulating Surveillance***, in THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW (David Gray and Stephen Henderson, eds)(Cambridge University Press 2018)

FTC: historical highlights

- The FTC is a century-old organization
- It was created to regulate monopoly & trust—not for consumer protection
- A compromise between warring factions caused it to have spectacular investigative and adjudicatory powers
  - The FTC's power to investigate is inquisitorial
  - The modern FTC can demand that entire industries provide information about their activities ***under oath***
  - The FTC can sue almost any kind of entity

FTC's early challenges

- The FTC was given a broad, vague mandate—to prevent unfair competition
- "…could there be a more impious attack on the triune separation of powers?"
  - Justice Learned Hand writing in the New Republic, Jan. 9, 1915
- Courts, flummoxed with this delegation, cabined the FTC's power to the common law
  - Common law consumer protection simply wasn't up to the task of addressing modern consumer problems
  - This is a recurring theme!

FTC & second wave consumerism

- Product labeling, Printers' Ink statute, common-law consumer protection approaches fail
- A reawakening of consumer concern about products and marketing in the 1930s led Congress to give the FTC its modern statutory power
- The Commission is hereby empowered and directed to ***prevent*** [entities] from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.
  - 15 USC 45(a)(2)(1938 amendments)
  - What is unfair/deceptive? Largely left to the Commission to decide

Fast forwarding a bit

- Important to distinguish between the FTC's unfairness and deception powers
- Deception is not politically controversial. The FTC has broad powers, untethered from common-law elements, to police it. Any misrepresentation that causes consumer "detriment" suffices. There is no cost-benefit-analysis requirement (CBA)
- Unfairness is controversial because it in effect prohibits a business practice. Amendments to the FTCA require "substantial injury," that the injury be unavoidable, and that the injury outweigh the benefit to consumers. Inherently this requires CBA.

SMOKING *and* HEALTH

REPORT OF THE ADVISORY COMMITTEE
TO THE SURGEON GENERAL
OF THE PUBLIC HEALTH SERVICE

U.S. DEPARTMENT OF HEALTH, EDUCATION, AND WELFARE
Public Health Service

The FTC's cigarette warning label & genesis of "unfairness"

- "CAUTION: cigarette smoking is dangerous to your health and may cause death from cancer and other diseases"
  - Drafted by Richard Posner! And Philip Elman
- But Congress intervened!
  - "Cigarette smoking may be hazardous to your health."
  - The blowback included a bar on the FTC from specifying stronger warnings on packs or advertising
  - Preempted the states from similar measures.
- The point of this diversion
  - If the FTC gets too aggressive, Congress clips its wings
  - The FTC is beginning to fledge again after being clipped by Kidvid

2. FTC and Cyber: Paul Rosenzweig

- "…the FTC now owns cybersecurity in the private sector." (2015)
- "The FTC's efforts are currently the only effective aspect of a Federal program to compel the business community to adopt more stringent cybersecurity measures" (2014)

How does the FTC regulate cyber?

1. The FTC interprets its unfairness authority to require "reasonable" security
2. The FTC bolsters "consent" requirements in surveillance matters
3. The FTC erodes intermediary, software immunity

Meta effects:

- More security in consumer devices promotes some kinds of cybersecurity
- An increase in "reasonable expectation of privacy" that we have in society › › knock on effects w/r/t privacy ***as citizen***

1. Reasonable security - substance

- FTC expects companies to have reasonable security & an info sec plan
- Special controls required for CC#s, sensitive data
- Vetting of vendors
- FTC will bring a case against if:
  - Breach resulting from OWASP top 10
  - The matter will result in some new, interesting expansion of FTC doctrine
  - The respondent doesn't try to make consumers whole
  - Consumer records show complaints, vulns exposed by researchers

Reasonable security - political debate

- All systems are insecure, and all companies have breaches
- When companies have breaches, they are investigated by the FTC and state AGs
  - They thus feel that the victim has been blamed!
  - They claim there is no harm
  - They claim that there are no generally-agreed-upon security norms
    - Thus reliance on OWASP…
- Anger about security cases has led to heated rhetoric and blowback for the FTC including due process challenges to the FTC's organic authority
  - Wyndham (3rd Cir.): supported FTC's security enforcement
  - LabMD (11th Cir.) held that orders were not enforceable – what is "reasonable" security?
  - D-Link (N.D. Cal.) currently set for trial, but appears to be in settlement negotiation

So we're in the weird place. The business community says it hates rulemaking, and lobbies against it, yet in litigation, businesses say enforcement violates due process …without the rules they oppose

Regulatory void = state actors move ahead

- NY DFS cyber guidelines now in effect (23 NYCRR 500)
  - Require firms to have bespoke policies (14 topics)
  - Annual pen testing, bi-annual vulns assessment
  - Encryption at rest, ceiling on data retention
  - 72 hour notification of "cybersecurity event"
    - Reasonable likelihood of material harm
  - Executives must certify
  - Scope: non-public info
  - Goal: safety & soundness, protect customers
- CCPA, CA SB 327 (IoT security)

Great student project: GLBA security rule

- Much more prescriptive! Thanks LabMD!
- Publicly-available on March 5th, comments due 60 days after publication in Federal Register
- Still hasn't appeared in the FR, so there's time!
- Safeguards Rule, 16 CFR Part 314, Project No. P145407

[Billing Code: 6750-01S]

FEDERAL TRADE COMMISSION

16 CFR Part 314

RIN 3084-AB35

Standards for Safeguarding Customer Information

AGENCY: Federal Trade Commission.

ACTION: Notice of proposed rulemaking; request for public comment.

SUMMARY: The Federal Trade Commission ("FTC" or "Commission") requests public comment on its proposal to amend the Standards for Safeguarding Customer Information ("Safeguards Rule" or "Rule"). The proposal contains five main modifications to the existing Rule. First, it adds provisions designed to provide covered financial institutions with more guidance on how to develop and implement specific aspects of an overall information security program, such as access controls, authentication, and encryption. Second, it adds provisions designed to improve the accountability of financial institutions' information security programs, such as by requiring periodic reports to boards of directors or governing bodies. Third, it exempts small businesses from certain requirements. Fourth, it expands the definition of "financial institution" to include entities engaged in activities that the Federal Reserve Board determines to be incidental to financial activities. Such a change would add "finders"–companies that bring together buyers and sellers of a product or service–within the scope of the Rule. Finally, the Commission proposes to include the definition of "financial institution" and related examples in the Rule itself rather than incorporate them

2. Consent and surveillance

- Wiretapping laws require ***actual*** or ***implied*** (not constructive) consent
- FTC has brought cases against spyware companies for how they have marketed monitoring software (Cyberspy)
  - Required system tray notification (if not administrator)
- FTC has enforced actual consent requirements for intrusive marketing practices
  - Flash cookies, consent workarounds, history sniffing (ScanScout, Google)
  - Web monitoring software (In re Sears, Rent to Own cases)
- Really what's happening here is that the FTC is filling the void for wiretap act/CFAA violations that fail because of standing, etc.

Surveillance & encryption policy

- Former FTC Commissioner Terrell McSweeny had been a strong opponent of backdoors
  - Politico Morning Cybersecurity, Jan. 7, 2016

McSWEENY COMES OUT SWINGING ON ENCRYPTION — From our friends at Morning Tech: FTC Commissioner Terrell McSweeny may not dabble day-to-day in national security issues, but she stressed at the CES conference in Las Vegas that governments "have to resist the notion that backdoors" are the right tool for the job on encryption. Noting that "in this environment we're connecting more and more of our daily lives to more and more of our things," the Democratic commissioner warned against creating "vulnerabilities in our systems," which she said would "undermine" privacy.

3. Eroding intermediary, software immunity

- FTC shut down one of the last bulletproof hosts in US (3FN, 2009)
- Reducing user security/just plain poor security can be unfair
  - Manufacturer-bundled phone software reduced security of Android (HTC)
  - Rootkit to enforce DRM (Sony's XCP)
  - Browser toolbar that sent traffic over http (Upromise)
  - IoT webcams w/ public feeds (TRENDnet)
- Companies that facilitate spying (e.g. by storing surveilled data or by helping others effectuate illegal surveillance) can be unfair
- Companies reselling pilfered personal information (Accusearch)—FTC beat a CDA 230 defense

3. The FTC in the President Trump Era

War on the administrative state

- "Article I is the Congress, Article II is the President. Article III are the courts. And then there's this administrative state, combining all three," McGahn told TIME in an exclusive interview. "They make the law, they enforce the law, and then they decide who violates the law, destroying the constitutional separation of powers that was designed to protect individual liberty."
  - Zeke J Miller, President Trump's Lawyers Plan a White House Legal Attack on Federal Agency Power, Time, Marc 13, 2017

Yet the FTC is doing ok

- 5-0 cases, collegiality is sound, appointees are qualified, reasonable people

Joseph J. Simons
Chairman

Sworn in: May 1, 2018

Biography | Speeches, Articles, & Testimony | Twitter

Noah Joshua Phillips
Commissioner

Sworn in: May 2, 2018

Biography | Speeches, Articles, & Testimony | Twitter

Rohit Chopra
Commissioner

Sworn in: May 2, 2018

Biography | Speeches, Articles, & Testimony | Twitter

Rebecca Kelly Slaughter
Commissioner

Sworn in: May 2, 2018

Biography | Speeches, Articles, & Testimony | Twitter

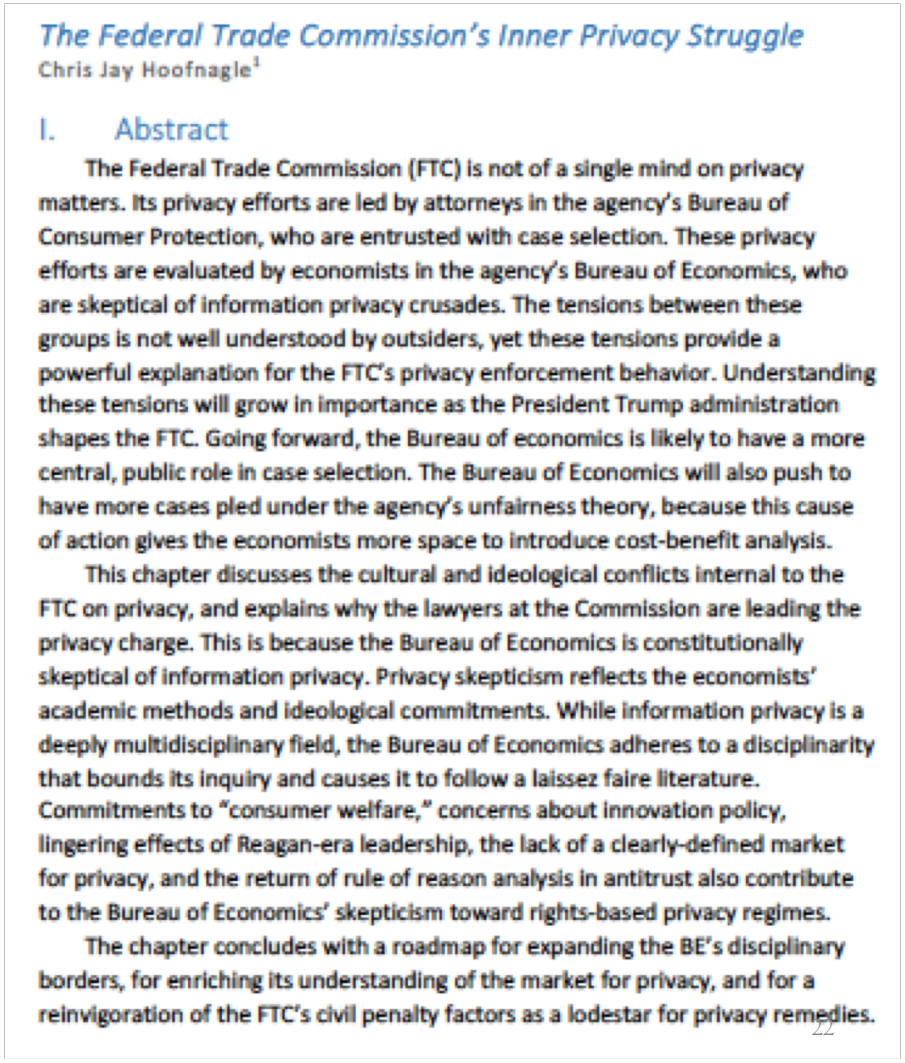
Christine S. Wilson
Commissioner

Sworn in: September 26, 2018

Biography | Speeches, Articles, & Testimony

Role of economists

- Attorneys set enforcement agenda
- Economists evaluate cases
  - Economists are skeptical of privacy
  - Evaluations are not public
- Attorneys short circuit that evaluation by pleading cases as deception rather than unfairness
- Economists want more cases plead as unfairness, and a more public role in evaluation



The Federal Trade Commission's Inner Privacy Struggle

Chris Jay Hoofnagle[1]

I. Abstract

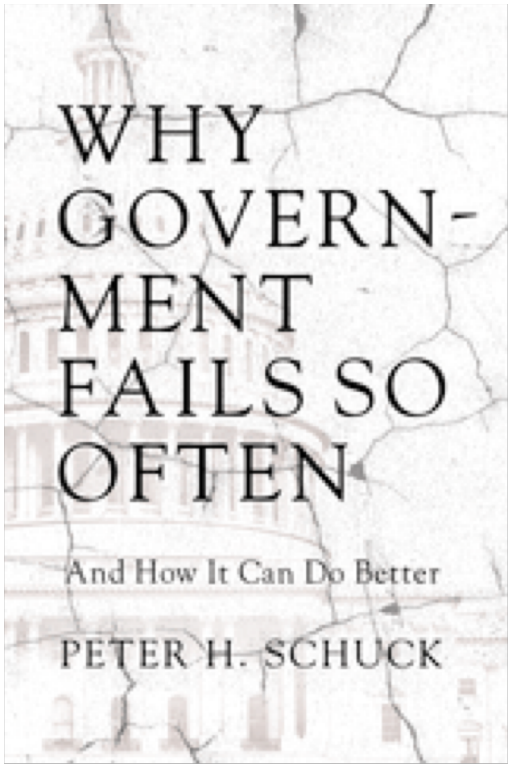
The Federal Trade Commission (FTC) is not of a single mind on privacy matters. Its privacy efforts are led by attorneys in the agency's Bureau of Consumer Protection, who are entrusted with case selection. These privacy efforts are evaluated by economists in the agency's Bureau of Economics, who are skeptical of information privacy crusades. The tensions between these groups is not well understood by outsiders, yet these tensions provide a powerful explanation for the FTC's privacy enforcement behavior. Understanding these tensions will grow in importance as the President Trump administration shapes the FTC. Going forward, the Bureau of economics is likely to have a more central, public role in case selection. The Bureau of Economics will also push to have more cases pled under the agency's unfairness theory, because this cause of action gives the economists more space to introduce cost-benefit analysis.

This chapter discusses the cultural and ideological conflicts internal to the FTC on privacy, and explains why the lawyers at the Commission are leading the privacy charge. This is because the Bureau of Economics is constitutionally skeptical of information privacy. Privacy skepticism reflects the economists' academic methods and ideological commitments. While information privacy is a deeply multidisciplinary field, the Bureau of Economics adheres to a disciplinarity that bounds its inquiry and causes it to follow a laissez faire literature. Commitments to "consumer welfare," concerns about innovation policy, lingering effects of Reagan-era leadership, the lack of a clearly-defined market for privacy, and the return of rule of reason analysis in antitrust also contribute to the Bureau of Economics' skepticism toward rights-based privacy regimes.

The chapter concludes with a roadmap for expanding the BE's disciplinary borders, for enriching its understanding of the market for privacy, and for a reinvigoration of the FTC's civil penalty factors as a lodestar for privacy remedies.

Increased role of cost-benefit-analysis

- CBA is a good thing (read Schuck!), but…
- Calls for "rigorous" and "sound" economic analysis are code for "find any rationale for the proposition that FTC action is perverse"
- CBA advocates almost always assume that consumers time and transaction costs are = $0
- CBA advocates almost always neglect other costs or other savings, often ignoring the very point of the protection
- CAN-SPAM rulemaking & my font size comments



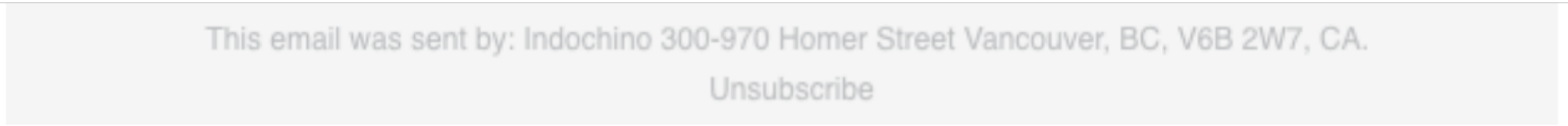


Figure 2: This email has a background color (#f5f5f5) and text color (#c0c2c4) that results in a 1.6 contrast ratio, failing all standards for adequate readability. For reference, white text on a white background would have a contrast ratio of 1.

A regulatory regime for the 21st Century?

- Businesses don't want rules, they want performance standards
- But performance standards require expertise, flexibility (think VW!)
  - Problem of deep capture
- Business community is lobbying, litigating for return of 19th century common law approaches—
  - Focus on "harm"
    - i.e., whatever I decide is "harmful" is what the FTC is going to police
    - Problem of cultural cognition
  - Reading "materiality" requirement into deception
  - Reading reliance into deception, limiting harm to relied-upon representations
    - §5 lacks a materiality requirement, ***unlike*** the FTC's false ads statute

Research questions you could consider

- How can this small agency that only brings about 20 cases a year possibly promote security in a meaningful way?
- What "cybersecurity" is promoted by a consumer-protection-oriented agency?
- Should "reasonable security" be the FTC's lodestar, or has security become as important as product safety, thus requiring a higher standard, such as strict liability?
- How can the FTC signal its expectations to businesses and afford them due process without developing formal rules, which can be sclerotic?

Thank you. ☺