The FTC's (un)Common Law Approach to Cybersecurity

Justin (Gus) Hurwitz

University of Nebraska College of Law

November 26, 2015

The Setting

- **The US has no general datasec law**
  - Rather, sector-by-sector
- **The FTC is working to fill that role**
  - What is the FTC?
    - "Unfair methods of competition [UMC]…, and unfair or deceptive acts or practices [UDAP]…, are hereby declared unlawful." 15 USC 45
  - Began raising concerns in 1990s
  - Congress didn't give FTC datasec power, so FTC proceeded using it's general UDAP authority

The FTC Approach

- **FTC can use adjudication or rules**
  - In the US, agencies can choose use either power
- **FTC has chosen to use adjudication**
  - There are good and bad reasons for this
  - Has brought 50+ deception, 50+ unfairness, cases
    - Almost all of these cases have settled
    - Points to these settlements as providing guidance re: good practices
  - Refers to this as its “common law” of data security

The FTC's "common law" is not

- **Common law is not just suing people!**
- **Settlements are not common law!**

- **Common law is a positive externality**
  - Results from parties bringing marginal cases to neutral decision maker, and
  - Neutral decision makers hearing many cases
  - Settlements indicate no case/controversey

Concerns with the FTC Approach

- **Does it make substantively good law?**
  - No! FTC guidance is not particularly good
  - No! FTC guidance does not broadly inform industry or change datasec norms
- **Is it legal?**
  - No! Does not provide parties with notice of what is or is not permitted conduct
- Recent cases: *Wyndham*, *LabMD*

Concerns with the FTC Approach

Judge William S. Duffey, Jr (D. Ga.), addressing FTC Counsel, *LabMD* MTD:

> No wonder you [FTC counsel] can't get this resolved …. **You have been completely unreasonable about this.** And even today you are not willing to accept any responsibility … . **I think that you will admit that there are no security standards from the FTC.** You kind of take them as they come and decide whether somebody's practices were or were not within what's permissible from your eyes.
>
> [H]ow does any company in the United States operate when [it] says, "well, tell me exactly what we are supposed to do," and you say, "well, all we can say is you are not supposed to do what you did." … **[Y]ou ought to give them some guidance as to what you do and do not expect, what is or is not required. You are a regulatory agency. I suspect you can do that.**

Concerns with the FTC Approach

Third Circuit Court of Appeals, *Wyndham* interlocutory appeal:

> We "agree with Wyndham that the **FTC's guidebook could not, on its own, provide 'ascertainable certainty' of** the FTC's interpretation of **what specific cybersecurity practices fail [Section 5].**"
>
> We "agree with Wyndham that the **[FTC's prior] consent orders**, which admit no liability and which focus on prospective requirements on the defendant, **were of little use to it in trying to understand the specific requirements imposed by [Section 5].**"
>
> We "recognize **it may be unfair to expect private parties** back in 2008 **to have examined FTC complaints or consent decrees**. Indeed, these may not be the kinds of legal documents they typically consulted."
>
> **"[The FTC has failed to explain how it had] informed the public that it needs to look at complaints and consent decrees for guidance."**

Concerns with the FTC Approach

Chief Admin Law Judge D. Michael Chappell, LabMD Initial Decision:

"If unfair conduct liability can be premised on 'unreasonable' data security alone, upon proof of a generalized, unspecified 'risk' of a future data breach, without regard to the probability of its occurrence, and without proof of actual or likely substantial consumer injury, then [the statutory standard provided in Section 5(n)] **would not provide the required constitutional notice of what is prohibited.**"

"**Fundamental fairness** dictates that proof of likely substantial consumer injury under Section 5(n) **requires proof of something more than an unspecified and hypothetical 'risk' of future harm**, as has been submitted in this case."

- Does it make substantively good law?
  - No! FTC guidance is not particularly good.
  - No! FTC guidance does not broadly inform industry or change datasec norms
- Is it legal?
  - No! Does not provide parties with notice of what is or is not permitted conduct
- Recent cases: *Wyndham*, *LabMD*

Alternatives

- **What's the goal?**
  - Data security is *hard*, landscape is changing
  - Most firms don't know, but want, to do it well
  - The problem is often that the software/ infrastructure isn't secure
  - No such thing as perfect security!
    - Good security involves: prevention, detection, mitigation, response
  - Goal is education/improvement, *not* punishment
    - Should be this way for foreseeable future

Alternatives

- **What's the goal?**
  - Data security is *hard*, landscape is changing
  - Most firms don't know, but want, to do it well
  - The problem is often that the software/ infrastructure isn't secure
  - No such thing as perfect security!
    - Good security involves: prevention, detection, mitigation, response
  - Goal is education/improvement, *not* punishment
    - Should be this way for foreseeable future

Alternatives

- **What to do?**
  - FTC: Focus on *developing norms* not *punishing firms*
  - FTC: Bring important cases in court
  - Courts: Reject FTC claims on due process grounds
  - Legislation: Provide for statutory damages
  - General: Improving security infrastructure
    - Hard to bring suits for defective software; broad immunity for intermediaries. These are bad security policy – shift burdens to less able/informed parties.

Alternatives

- What's the goal?
  - Data security is *hard*, landscape is changing
  - Most firms don't know, but want, to do it well
  - The problem is often that the software/ infrastructure isn't secure
  - No such thing as perfect security!
  - [illegible]
  - Goal is education/improvement, *not* punishment

Insurance!

- The best thing we can do to improve the state of firms' cyber/data security is to require, or create strong incentives to have, comprehensive cyber/ datasec insurance policies.
- Insurers have ability/data to develop best practices
- Insurers have ability/incentive to share best practices
- Insurers have ability/power to better infrastructure