FTC PROCESS AND THE MISGUIDED NOTION OF AN FTC "COMMON LAW" OF DATA SECURITY

Geoffrey A. Manne & Ben Sperry

Commissioner Brill[1] and a few academics[2] have described the FTC's data security settlements as developing a "common law" of data security. It is not readily apparent, however, that the over 50 independent complaints and settlement agreements between the FTC and particular companies amounts to what is traditionally understood as the common law. Moreover, because the FTC's enforcement and adjudication process differs so substantially from traditional civil adjudication, even if the FTC's data security settlements have certain common law characteristics, it is likely that the *content* of the FTC's data security law differs substantially from what would emerge from – and what would be desirable in – in a traditional common law process.

As it happens, however, we do have an *actual* common law of data security — that is, data security cases adjudicated in civil courts — with which to compare the FTC's process and settlements.

Those who defend the notion of an FTC data security common law identify the shortcomings of common law in civil courts—alleging, in essence, a sort of "market failure"—and they suggest that the FTC's common law approach can and should correct this market failure, in part because the FTC does have a common law process. These claims are often largely descriptive, but, as suggested, there must be a normative preference inherent in the "common law" conclusion – or else, who cares?

In fact, advocates of calling FTC data security complaints and consent decrees "common law" generally point to versions of purposeful evolution and predictability as the desirable hallmarks of common law. And as to the latter of these, we actually think they are right in important ways, unlike some other critics of the common law claim. But because of systemic process problems and dynamics these scholars miss, FTC data security enforcement actions actually demonstrate few if any of the true hallmarks of the common law, including something like evolution toward efficiency. On balance, in fact, expanded FTC interventions in data security cases would likely harm, not help.

The contrary conclusion is mostly a version of the Nirvana fallacy – the assumption that because there is an alleged "market failure" (courts under-enforcing data security rules), and be-

---

[1] Commissioner Julie Brill, *Privacy, Consumer Protection, and Competition*, speech given at 12th Annual Loyola Antitrust Colloquium (Apr. 27, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/privacy-consumer-protection-and-competition/120427loyolasymposium.pdf ("Yet our privacy cases are also more generally informative about data collection and use practices that are acceptable, and those that cross the line, under Section 5 of the Federal Trade Commission Act creating what some have referred to as a common law of privacy in this country.").

[2] *See, e.g.*, Daniel Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

cause the FTC has the *power* to overcome this claimed failure (broad discretion to enforce more), it should do so. Missing from this analysis is an actual analytical defense of the "should" statement, which, instead, is simply inferred from the premises. In this paper we undertake that analysis and demonstrate that the conclusion is unwarranted.

The primary problem is that defenders of the FTC common law argument look only at the FTC's outputs (its data security consent decrees)[3] and neglect to ask or assess whether process problems render those outputs defective in systematic ways.

Ironically, our analysis doesn't turn on the conclusion some have offered that the problem with the FTC as gap-filler/market-failure corrective is that it systematically engages in *over*-enforcement. To the contrary, we think the history of the FTC's data security enforcement shows a remarkable *lack* of vision. In particular, it has done remarkably little to push the boundaries of what optimal data security law requires in changing circumstances.

So when Hartzog & Solove, for example, say "We contend that the FTC currently serves as an essential lynchpin in the U.S. data protection regulatory regime. Curtailing the FTC's powers would severely upend the entire U.S. privacy regulatory regime," We think they are wildly overstating the importance of the FTC.

But that said, it is possible for the FTC's enforcement actions to be simultaneously both under and over-inclusive, and while the agency has broken no new ground in how the law applies and what remedies it suggests, it *has* applied the law in novel circumstances and it has occasionally broken new doctrinal ground.

Far from being a feature, as Hartzog & Solove describe the FTC's unfettered discretion, we see it as a bug. Perhaps the FTC has colored inside the lines in many respects thus far, but there is nothing stopping it from straying – and sharply and radically so – at any moment.

It is also notable that the FTC doesn't even deal in any consistent or thorough way with the boundary issues it *does* confront, where it might have actual added value. In other words, the FTC doesn't bother to justify its expansions of the exercise of its authority when it undertakes them. Nor is it systematic in its application of the same old law to new situations, other than that it systematically does so without any explanation of why it's appropriate to reach the same result over and over again in the face of considerably different facts.

In short, our assessment is this: So far the FTC has been largely useless in evolving the law of data security, but the real problem lies in what happens when it decides to try to be useful. An even worse state of affairs than the status quo (a relatively useless FTC in data security) would be a muscular FTC with no judicial check on its authority.

This paper attempts to analyze this alleged administrative "common law" with reference to the actual common law baseline of data security developing in federal courtrooms. We consider the

[3] In fact, defenders of the approach also look at other outputs like policy statements and reports. We confine our analysis here to enforcement actions. Thus, it is conceivable that there are common law attributes in these other outputs, not subject to the problems we identify here, that on net render the FTC's larger body of work actually common-law-like. We seriously doubt it, but we don't conclude one way or the other here.

dynamics in both processes, and assess to what extent they comport with the attributes of common law, and whether they likely further the desirable aspects of a common law process.

Finding decidedly different outcomes in FTC vs. civil court actions, we offer the theory that these different outcomes are the predictable consequence of different processes in each venue, and that these different processes strongly suggest that, while civil court outcomes follow the general pattern of common law evolution (with caveats), the FTC's outcomes simply do not.

Background: The FTC's Data Security Universe

The FTC uses its Section 5 authority over unfair and deceptive practices to police business conduct that allegedly provides inadequate protection for customer data in companies' possession. Until the recent *FTC v. LabMD* and *FTC v. Wyndham* cases, the FTC had an unbroken streak of over 40 data security complaints ending in consent decrees without any administrative or judicial trial. Following the initiation of the cases against Wyndham and LabMD, which are both still pending, the streak has resumed with another 10 or so cases ending in consents without trial.

In *FTC v. Wyndham*, the District Court of New Jersey rejected Wyndham's motion to dismiss. Judge Salas' opinion argued that the FTC's interpretations of the FTC Act "while not controlling upon the courts by reason of their authority, do constitute a **body of experience and informed judgment to which courts and litigants may properly resort for guidance**." (emphasis added).

This is not the first time the FTC's complaints and consent decrees have been compared to something like the common law. FTC Commissioner Julie Brill, academics like Solove and Hartzog, and even the Commission itself in its rejection of LabMD's motion to dismiss have identified these unadjudicated assertions as a developing common law of data security.

Interestingly, in quoting *General Electric Co. v. Gilbert* in her *Wyndham* opinion, Judge Salas omitted the very next sentence which states: "The weight of such a judgment in a particular case will depend upon the thoroughness evident in its consideration, the validity of its reasoning, its consistency with earlier and later pronouncements, and all those factors which give it power to persuade, if lacking power to control." The court seemed to suggest that the complaints and consent decrees described above possess those qualities. But, as we will discuss in more detail below, that's a difficult conclusion to sustain.

In fact, our empirical analysis finds, among other things, that:

(1) Defendants fare systematically worse (in terms of decisions against them, not necessarily the size of damages, which we don't evaluate) at the FTC than in civil courts;

(2) FTC complaints lack the factual allegations that are present in civil court complaints;

(3) The FTC consistently (if implicitly) finds that the same defects in data protection practices lead to alleged injuries, regardless of the underlying characteristics of the defendant and the circumstances at issue;

(4) The FTC's complaints fail to explain causation between conduct and alleged injuries compared to civil court complaints, and they fail to explain causation between remedies and both conduct and alleged injuries;

(5) The practices that constitute "reasonable" data security at the FTC and thus would prevent liability are remarkably consistent, whereas the range of both acceptable and unacceptable practices identified by civil courts is much more variable;

(6) At the same time, the FTC rarely identifies with specificity what practices it deems *unacceptable*, whereas civil courts regularly constrain their discretion by identifying specific practices that can lead to liability.

We also make further findings comparing specific outcomes (i.e., frequency of settlement; rate of successful motions to dismiss, etc.) between the two venues. But this comparison of outcomes is less straightforward than it seems.

It is tempting to compare, say, the rate of settlements at the FTC with the rate of settlements between litigants in civil court. But given FTC process and the relevance of case selection dynamics (described below), it is probably more apt to analogize FTC staff to civil court plaintiffs and the Commission to trial judges – and thus, to compare the Commission's decision to bring the staff's proposed complaint to a trial court's rejection of a motion to dismiss, and to compare the Commission's settlements to a civil court judgment in favor of the plaintiff.

It's not clear what the analogue to civil court settlements would be at the FTC. Given the interactions between defendants and staff at the investigation stage, arguably some or all of the FTC's closed investigations are akin to trial court settlements, but they are at least as likely to be comparable to trial court decisions in favor of defendants. A closer, systematic look at the FTC's complaints might suggest that some of these should be counted as "settlements before trial" rather than as plaintiff victories, but we have looked pretty closely at the complaints and, particularly in the absence of much useful discussion in the few closing letters we have, it's impossible to definitively support such an analogy. Similarly, some remedies imposed in Commission consent decrees might more accurately be counted as "settlements of litigated cases."

In order to get a better handle on the universe of cases at the FTC that didn't result in settlements, we filed a FOIA request with the agency. It showed only seven closing letters and three emails closing investigations without bringing a case.

As a preliminary matter, we consider what this might mean:

1. One possibility is that the FTC is incredibly good at picking cases and has legitimately found only 15% to be wanting once investigation has begun. Unlikely.

2. Second is that there is no "truth-based" sorting mechanism at play from which to infer any kind of evolving process. Rather, the reason for such a high success rate is that the only cases that make it to even *investigation* (let alone Commission action, although these are almost the same, as it happens) are ones for which ultimate approval by the Commission and settlement were foregone conclusions.

3. But it is also possible that the use of "quick look" – cursory investigation without opening official investigation – means sorting happens *before* investigations are opened, and the "real" number of closed cases is potentially wildly larger. Unfortunately, either we weren't given or the FTC didn't

have responsive docs to our FOIA request that would give us the number of "quick look" cases to evaluate this empirically. But there is reason to be dubious.

It also happens that 100% of cases recommended by the staff to the Commission result in complaints.

What are the likely implications?

1. Not only is there no judicial review, there is effectively no Commission review of the cases. Yes, the Commission votes on the cases that are brought, but the Commission systematically sees only the cases the staff knows it can convince a majority of Commissioners to bring – which over time becomes a self-reinforcing rule, not an evolving common law.
    a. Caveat – unless the make-up of the Commission changes over time in an evolutionary fashion. This is possible, given that the commissioners are generally chosen from among the cognoscenti, but it is also somewhat unlikely given that historically most of these have been *antitrust* cognoscenti, and that, regardless, political and other variables likely dramatically erode any explanatory power the "insider" variable might have.
2. This only highlights even more strongly that the standard of review for these cases is very low under Section 5(b), "reason to believe," and the selection of cases doesn't have much explanatory power for future potential defendants. If staff brings cases on the basis of expected Commission vote, it, too, must be assessing on the basis of "reason to believe." And, what's worse, by not even letting the *Commissioners* see the universe of rejected cases, "reason to believe" becomes a self-fulfilling prophecy.
3. Related, it also strongly supports the point that data security cases are little more than per se liability based on the fact of a breach, rather than any connection between conduct and breach. It is plausible, if not likely, that the fact of a breach would provide "reason to believe." But given evidence that suggests at least 85% of cases are taken to the Commission on the basis of staff's belief that Commission will find "reason to believe," and thus are brought based on possibly nothing more than the fact of breach; and given that over 96% of these are settled (and 100% until last 2 years); there is no reason to *expect* the content of the Commission's data security settlements to be anything more than consistent recitations of a particular set of criteria (the Safeguards Rule). In other words, when the only tool you have is a hammer, everything looks like a nail.
4. Of course, this also undermines the likely accuracy of quick-look as a sorting mechanism, because the ultimate analysis described above will ultimately filter down to that level. Which gets us back to where we started – there is no systematic sorting going on, and no good reason at first cut to believe common law evolution occurs in the FTC's data security cases.

> 5. This also means not just that there is no common law as a descriptive matter, but that we should be suspicious that the benefits of common law process are being realized at the FTC . . .

Seen in this light a few possible conclusions emerge:

1. The closest the FTC *ever* comes to deciding in favor of defendants is in the 10 out of 65 investigations (15%) closed by the staff without a complaint. More likely these compare better to pre-trial settlements given the expense of complying with the FTC's compulsory process. Thus, at most 15% of FTC investigations result in anything that could be called a victory for defendants, and probably some or all of these are better counted as settlements so the actual number is lower. By contrast, in civil adjudication, more than 60% of cases result in a victory (dismissal) for defendants.
2. At the FTC, plaintiffs win a "motion to dismiss" 100% of the time; in civil court they *lose* about 60% of motions to dismiss.
3. While the FTC – the plaintiff – has won 96% of cases while rarely pleading injury with any substantiality (with the other 4 percent not decided yet) civil court plaintiffs win a much lower percentage of lawsuits, achieving a settlement in 71% of cases where actual injury was plead and 49% of cases where actual injury was not plead.
4. Counting "favorable" remedies (using consent decree length as a simplified proxy) as settlements of litigated cases rather than plaintiff victories would mean about 47% of litigated cases settle at the FTC and 53% result in plaintiff victories. This compares to __% of litigated cases settling in civil court and none or almost none resulting in plaintiff victories.

The general result is, of course, wholly predictable given the FTC's fundamental position as both prosecutor and judge: No matter how you slice it, plaintiffs do far, far better at the FTC than in trial court, and defendants do measurably worse at the FTC.

It is this dynamic in large part that leads to the simplistic conclusion that the FTC can act as a gap filler – picking up where the courts have abdicated their responsibility to police data security practices.

But apart from assuming without proving that the rate of plaintiff victories in civil courts is too low, this also assumes that the FTC is doing more than just providing justice to the specific parties not being compensated by the courts; there is no sense in which the FTC could be said to be doing the latter given the relatively tiny number of cases it brings.

But the FTC *could* be optimizing the system in at least two ways: Because of its almost limitless scope and its ability to impose potentially costly 20 year consent orders, it may be offering more—and possibly more-optimal—deterrence. And/or, because it has essentially unfettered discretion, it may be offering more optimal law—pushing legal boundaries that broaden the scope and improve the quality of the law of data security.

We certainly agree that the FTC might be providing additional deterrence. But no one has established in any way that, if it is doing so, this results in more *optimal* deterrence.

And in some ways it may be expanding the scope of the factual situations to which liability attaches. But, again, there is absolutely no evidence one way or the other to suggest this would be a net improvement.

More important, there is reason to think that it might *not* be. Because the FTC operates essentially without judicial constraints, and because (for the same reason) there is no feedback mechanism in terms of the further application of precedent at the FTC, it is reasonable to assume that the Commission's structure allows a wide range of idiosyncratic preferences among the staff, Commission and Presidents who appoint Commissioners, for that matter, to dominate efficient or otherwise objectively preferable decision-making. This is extremely unlikely to systematically result in "better" law.

But also problematic for the claim that the FTC should operate to "correct" sub-optimal adjudication in the courts is the fact that, as reflected in some of the numbers discussed and as described above, the process by which cases are selected and adjudicated at the FTC demonstrates a serious, systematic deviation from the likely optimal process that might be obtained through an *actual* common law approach. The FTC is dominated by a systematic lack of information at the Commission level, a self-fulfilling prophecy problem, and, as just noted, the absence of external review or feedback. Courts, too, are plagued by public choice problems that suggest they may not tend as rapidly or consistently toward efficiency as some defenders of the common law have suggested. But the ways in which courts deviate from an optimal common law process are magnified at the FTC.

Why Are We Discussing the Common Law, and Does the FTC Have One, Anyway?

It is worth asking why this debate over the common law attributes of the FTC matters. For the debate to be about anything other than mere descriptive accuracy, it must be the case that defenders of the "FTC's settlements as common law" argument think this is a worthwhile thing to defend.

Hartzog and Solove, e.g. don't spend much time on the defense of the common law, but rest largely on the claim that the FTC's approach, like the common law, provides fair notice and guidance for market actors, just like a common law would:

> The FTC has not been arbitrary and unpredictable in its enforcement. FTC enforcement has certainly changed over the course of the past fifteen years, but the trajectory of development has followed a predictable set of patterns. These patterns are those of common law development. Indeed, we argue that the body of FTC settlements is the functional equivalent of privacy common law. Understood as such, there is nothing unusual about how the doctrines emerging from the FTC settlements have evolved.[4]

To us, the absence of arbitrariness and unpredictability are well and good, but insufficient to establish that a system is a common law system.

[4] Solove & Hartzog, *supra* note **Error! Bookmark not defined.**, at 608.

Rather, the common law's emergent, evolutionary order offers the prospect of efficiency, some say—an evolution that permits legal rules and their application to shift with changing circumstances and to emerge efficient.

There are critics of this view, even within the law and economics field, but the efficiency arguments (and their critics) serve to offer up a set of characteristics that might plausibly be considered benefits of the common law. More important, they offer a set of characteristics that might help to identify when a system is common-law-like, and when it is not.

To begin with, and as noted, the common law is not static, and as society and technology change over time, the common law evolves with it:

> It must be remembered that the common law is the result of growth, and that its development has been determined by the social needs of the community which it governs. It is the resultant of conflicting social forces, and those forces which are for the time dominant leave their impress upon the law. It is of judicial origin, and seeks to establish doctrines and rules for the determination, protection, and enforcement of legal rights. Manifestly it must change as society changes and new rights are recognized. To be an efficient instrument, and not a mere abstraction, it must gradually adapt itself to changed conditions.[5]

In Lord Mansfield's characterization, "the common law 'does not consist of particular cases, but of general principles, which are illustrated and explained by those cases.'"[6] Further, the common law is evolutionary in nature, with the outcome of each particular case depending substantially on the precedent laid down in previous cases. The common law thus emerges through the accretion of marginal glosses on general rules, dictated by new circumstances.

The common law arguably leads to legal rules with at least two substantial benefits—efficiency and predictability or certainty. The repeated adjudication of inefficient or otherwise suboptimal rules results in a system that generally offers marginal improvements to the law. The incentives of parties brining cases generally means "hard cases," and thus judicial decisions that have to define both what facts and circumstances violate the law *and* what facts and circumstances don't. Thus, a benefit of a "real" common law evolution is that it produces a body of law and analysis that actors can use to determine what conduct they can undertake without risk of liability *and* what they cannot.

In the abstract, of course, the FTC's data security process is neither evolutionary in nature nor does it produce such well-defined rules. Rather, it is a succession of wholly independent cases, without any precedent, narrow in scope, and binding only on the parties to each particular case. Moreover it is generally devoid of analysis of the causal link between conduct and liability and entirely devoid of analysis of which facts do not lead to liability. Like all regulation it tends to be static; the FTC is, after all, an *enforcement* agency, charged with enforcing the strictures of specific and little-changing pieces of legislation and regulation. For better or worse, much of the FTC's data security adjudication adheres unerringly to the terms of the regulations it enforces

---

[5] *Id.* at 234.

[6] F.A. HAYEK, LAW, I LEGISLATION & LIBERTY: RULES & ORDER 86 (1973) (citing W.S. HOLDSWORTH, SOME LESSONS FROM LEGAL HISTORY 18 (1928) (*quoting* Lord Mansfield)).

with vanishingly little in the way of gloss or evolution. As such (and, we believe, for worse), the FTC's process in data security cases tends to reject the ever-evolving "local knowledge" of individual actors and substitutes instead the inherently limited legislative and regulatory pronouncements of the past.

By contrast, real common law, as a result of its case-by-case, bottom-up process, adapts to changing attributes of society over time, largely absent the knowledge and rent-seeking problems of legislatures or administrative agencies.[7] The mechanism of constant litigation of inefficient rules allows the common law to retain a generally efficient character unmatched by legislation, regulation, or even administrative enforcement.[8]

Because the common law process depends on the issues selected for litigation and the effects of the decisions resulting from that litigation, both the process by which disputes come to the decision-makers' attention, as well as (to a lesser extent, because errors will be corrected over time) the incentives and ability of the decision-maker to render welfare-enhancing decisions, determine the value of the common law process. These are decidedly problematic at the FTC.

In what follows, we discuss in more detail some of the most significant characteristics of a common law system likely to lead, all else equal, to better legal outcomes, and discuss whether and to what extent they arise at the FTC. The conclusion is overwhelmingly against the FTC as a source of what scholars typically mean by "common law."

Decision-maker preference for efficient rules. (Posner)

To a significant extent Posner's theory has been challenged by more nuanced analyses that recognize public choice problems as ameliorating Posner's basic analysis. But to the extent that it remains accurate, even if on the margin, there is little reason to believe that FTC Commissioners have much systematic preference for efficient consumer protection rules. This is true not only because ex post casual empiricism suggests it, but also because few Commissioners are appointed because of a preference for efficiency, there is a very attenuated "culture" of efficiency in the FTC's consumer protection practice, and bureaucratic and political dynamics frequently will require deviation from any efficiency preferences.

It must also often be the case that, especially in the most important (i.e., novel) cases, even an efficiency-preferring Commissioner will err, and there is no judicial review and only attenuated, other external feedback to correct such mistakes.

Interest of the parties in establishing precedent. (Rubin & Priest)

> *When both parties to litigation are interested in precedent, efficient outcomes are more likely to evolve over time.*

Because of the small number of cases and the use of 20-year decrees that make precedent nearly irrelevant to potential future cases for any particular litigant, defendants at the FTC have little interest in precedent. More important, because the FTC itself is not bound by precedent, neither the FTC *nor* defendants have much interest in precedent; it is largely irrelevant to their

[7] *See, e.g.*, John Hasnas, *The Depoliticization of Law*, 9 THEORETICAL INQUIRIES IN LAW 529 (2008).

[8] *See, e.g.*, RICHARD POSNER, ECONOMIC ANALYSIS OF LAW, 8th ed. (2011).

calculus. Thus, the mechanism in common law by which inefficient legal rules are litigated toward efficiency (and efficient legal rules are left to stand) doesn't operate at the FTC.

> *When one party is interested in precedent, outcomes will favor that party, regardless of efficiency.*

While the FTC isn't interested in precedent per se, it *does* have a strong interest in litigating and winning. Winning for the FTC (staff) is a foregone conclusion (ultimately 96% of recommended cases thus far (and potentially 100%) have been FTC victories), so it has a pure interest in litigating regardless of the efficiency of the rule – the internal dynamics ensure this.

Even a preference for efficient rules (assuming, against all likelihood, that individual staffers or the staff as a whole can determine efficient rules—a determination not necessary to reach efficiency in the civil common law's evolutionary process), this will often be dominated by the preference for litigation.

The Commission, as well, has an interest in litigating and winning (again, winning is a foregone conclusion), but also again, an (unavoidably unreliable) preference for efficiency may be dominated by the preference for litigation *and* by the dynamics of majority voting.

Defendants meanwhile have no interest in litigating – nor do they have much ability to bring about settlements at the investigation stage.

Collectively this means litigation incentives are enormously stronger for the FTC, and there is no inherent preference for efficient outcomes – nor any evolutionary feedback process to impose efficiency externally.

> *Both parties uninterested in precedent; status quo persists, whether efficient or not.*

Seemingly the only thing the FTC has going for it is that its decisions have no precedential effect, its preferences favor litigation over boundary-pushing (on some dimensions), and it can adjudicate very few cases. This means that in the majority of possible fact patterns that could possibly lead to liability, the FTC won't act at all, and neither, of course, will potential defendants attempt to force litigation (except against competitors, of course, another dynamic counseling against the notion of "common law" – or in any way optimizing – adjudication by the FTC).

However, the threat of action, and the seeming randomness (from the point of view of potentially affected companies) of its selection of cases means it does cast a big shadow and does deter a lot more conduct than it directly adjudicates. It is an empirical question whether this deterrent effect has a net negative effect on efficiency given the general lack of precedent and small case load. There is good reason to assume it does.

> **Given some ignorance of the parties, the market will evolve more efficient solutions over time, even if these appear inefficient. (Alchian)**

As Manne & Zywicki have explained in a previous paper, firms develop internal mechanisms that may appear inefficient but actually solve a behavioral anomaly, resulting in net (ex post) rational behavior. But regulators will systematically target these seemingly inefficient behaviors, missing the underlying problem they may be solving, while firms themselves as well as ju-

dicial decision-makers may not be aware of why such structures are efficient. This means that, while potential defendants may wrongly avoid or seek litigation because of a mistaken assessment of some complained of behavior, and courts may systematically err in adjudicating them, the FTC has a systematic bias to challenge relatively efficient conduct. This is mitigated to some extent but its overall small caseload (which implicitly lets stand the status quo in the majority of cases), but, again, its deterrent effect mitigates this mitigation.

Interestingly, where firms evolve structures to deal with their internal irrationalities, the FTC decidedly does not. Rather, the FTC has a structure that actually exacerbates them – rewarding staff decisions to investigate and recommend complaints on the basis of their expectations about the Commission's likely vote with no significant external feedback mechanism to impede such behavior.

In turn, this means that the Commission's own decision-making is systematically impaired, because Commissioners are exposed to a biased sample of cases, believing over time (because it has always been true), that when staff recommends a data security case, it should support the recommendation—which further impairs the Commission's ability to overcome that bias by systematically keeping from the Commission knowledge of the universe of cases *not* investigated by the staff and giving it a false sense of the universe of cases at issue/affected by its decision and any particular case's problems relative to that context.

To be sure, this effect is mitigated by informal communications within the agency (and the absence of constraints on external sources of information). But the improbable case selection and win rates suggest this may have limited effect.

Arguably this dynamic helps to explain the recent *Apple* decision, in which a majority of the commission essentially treated Apple just like the claimed analogous "bad actor" uninformed consent cases involving unauthorized billers and crammers – somehow missing that Apple was importantly different than they.

Variation combined with a selection process leading to efficiency. (Alchian)

There are two elements to an evolutionary model—variation and selection. Alchian argues that even if variation is entirely random, if the selection process is sharp enough then it will seem that the variation itself was purposeful (i.e., intended to produce the result it seems to solve). Of course, if the variation itself is also intentional, then it might converge to the efficient process more rapidly.

But the FTC's cases are anything but varied, nor is the selection process meaningful. Because the staff selects cases to recommend, and thus selects cases to investigate, based on the expected likelihood of a majority vote in favor by the Commission, in the most important respect (outcome) and many other still important respects (amenability to the Safeguards Rule, e.g.), there is little or no variation in the options being selected.

Relatedly, because the Commission seems, when all the idiosyncrasies are averaged out, to select cases to which its Safeguards Rule definition of reasonableness will apply, and because it reinforces the lack of variation in selection by bringing all proposed data security complaints, there is no poignancy in its selection process. In other words, to a rough approximation, all staff has to do is offer a case, and it will be predictably approved. This is not a mechanism likely to

lead to any particular or discernible evolutionary vector, and even less likely to systematically lead to the evolution of efficient outcomes.

As noted below, the cases do contain variety in underlying facts, but this variety is steadfastly ignored (seemingly) by the Commission, and in nearly every case, regardless of facts, the same outcome is reached: liability (via settlement) for failure to adhere to the prescribed practices of the Safeguards Rule, and the imposition of those practices as a remedy.

Thus there is both homogeneity in the options being offered, as well as a "foolish consistency" in the process of selection. Such a state of affairs is simply self-reinforcing, and, unlike the immensely more varied cases that come before common law courts and the much sharper and less "game-able" judicial selection process, unlikely to lead to systematically better outcomes.

It is worth reiterating that the homogeneity that this bureaucratic dynamic impels isn't actually so homogenous in some ways. Because there is, in fact, no common-law-like precedent that binds the Commission, the sorts of cases for which it is likely to muster three votes shifts over time. But it does so without any consistent or discernible direction, without any identifiable "evolution"; rather, it is a function of idiosyncratic preferences and political currents. This means that there will be variation in types of cases, fact patterns, and even (possibly boundary-pushing) doctrinal interpretation.

This reality, however, lends support to the conclusion that the sorting mechanism followed by the decision-makers at each stage of the process is not about "truth" or the effort to optimize results, but rather about "getting to yes." If it weren't, it seems extremely unlikely that we'd see an 85% success rate at the initial investigation stage, a 100% success rate at the Commission review stage, and a 96% success rate at the enforcement stage. It's hard enough for the staff to be so accurate when trying to match a "quick look" at a case with an expected three-vote majority; it would be nearly impossible to be so accurate drawing a three-vote majority in favor of cases chosen on the basis of the staff's assessment that a case was "objectively good" given the relative longevity of staff and the ever-changing make up, and idiosyncrasies and political agendas, of the Commission.

One might object that the incentives of common law plaintiffs are equally mismatched with the incentives of common law judges and defendants – except in data security cases in civil court the success rate reflects this.

Promotion of predictability and certainty (rule of law) (Various).

Contra some critics of the FTC settlements as common law claim, we believe the FTC's data security cases have, as a historical matter, offered a considerable degree of certainty in certain respects. Most importantly, the remarkable consistency of remedies – essentially, the prescribed process from which the FTC is likely to infer reasonableness of data security practices – means every actor is on fair notice and well-informed about what the FTC expects. It is extremely difficult to maintain that parties don't know what is expected of them, even absent analytically useful statements by the agency.

What is clear is that, almost without regard to any underlying characteristics, size of injury, number of injured parties, etc., an almost identical set of practices is prescribed by the agency to remedy alleged unreasonableness in data security, meaning, no matter what industry, size,

or extent of possible harm, every business regulated by the FTC should know what is expected of it. The FTC has been remarkably consistent in this.

Now, we believe this is actually a *bad* thing. The absence of any apparent connection between different circumstances and different remedies – or, put differently, the absence of any explanation why very different circumstances are properly addressed by the very same data security processes – is never much explained and hasn't evolved in over a decade. The likelihood that this consistency reflects the optimal outcome is extremely low.

In this sense the FTC's data security settlements aren't an evolving common law – they are a static statement of "reasonable" practices, repeated about 55 times over the years and applied to a wide enough array of circumstances that it is reasonable to assume that they apply to *all* circumstances. This is consistency. But it isn't the common law. The common law requires consistency of application – a consistent theory of liability, which, given different circumstances, means *inconsistent* results. Instead, here we have consistent results which, given inconsistent facts, means a sort of *in*consistency of application.

This is a missed opportunity for the FTC. There are no doubt new technologies, new situations, changing norms, etc., that the FTC could provide guidance on – for which the FTC might offer its expert opinion and help guide industry practices (not least through its assessment of industry self-regulation). But instead, the FTC is, in its data security enforcement, largely useless. Or, at least, it has been since it promulgated the Safeguards Rule from which its "reasonable" practices are derived. The government could have freed up scads of resources not only at the agency but among all of us here occupied with analyzing the FTC, if it had simply enshrined the Safeguards Rule into law and been done with it.

On second thought, keeping the FTC occupied with a complex apparatus that on net does little more than simply restate the same rule over and over is probably better for society than whatever alternative the government would have put those resources to.

A slightly more charitable interpretation is that, so far, the Safeguards Rule really is simply a statement of best practices that applies to everyone. And the FTC's repeated, but not excessive enforcement of it is a low-cost way of getting efficient practices in the market.

While this may not cut *against* the FTC, it also doesn't support the contention that the FTC is filling gaps and helping expand common law litigation to cover new, welfare-enhancing ground. Instead, it suggest that the FTC is engaged in little "boundary pushing" and adding very little (other than national scope) to what courts are doing.

One piece of evidence to support this claim is the treatment of mitigation expenses as damages in the FTC's *Wyndham* complaint. At first glance, this seems like an "evolutionary" move – it is a break with past practice, expanding the scope of cognizable damages, and it might reflect a better understanding of the optimal treatment of mitigation expenses, or changing conditions.

But the common law is likely, for reasons discussed, institutionally capable of fixing itself better than the FTC is. And supporting evidence is found in *Anderson v. Hannaford Bros.* (1st Cir 2011) and *Curry v. AvMed* (11th Cir. 2014), both of which use broader definitions of injury than the common law or FTC previously allowed in data breach cases to include mitigation damages. At best the FTC is keeping pace with the courts, but *Hannaford Bros.* actually got there several years earlier.

Moreover, *AvMed*, for example, contains a detailed discussion of causation – something no FTC complaint or settlement has adequately done and most eschew entirely – and interprets a claim of "losses" to mean only "unreimbursed losses," whereas the *Wyndham* complaint arguably goes well beyond the legitimate pushing of boundaries by specifically claiming reimbursed damages as cognizable. What's more, it claims damages suffered by credit card companies – decidedly not "consumers" – as cognizable.

Finally, to the extent the *Wyndham* complaint contains more details and better developed legal claims than any other FTC action, it is notable that it is the only data security case the FTC has brought in a civil trial court, indicating that it is the common law court, and not the FTC, that is responsible for the more useful pleadings.

Other dynamics

Higher value rules lead to more litigation to get "better" rules

Zywicki argues that where the higher the expected value of a legal rule or the expected durability of the rule, the more parties will be willing to invest litigation. This can lead (via Rubin's analysis) to the production of more legal rules and eventually more efficiency. Such dynamics are claimed to be characteristics of the common law.

At the FTC neither holds. While defendants have incentives to minimize the effect of the FTC's rules on them, once a settlement is reached, the party has no interest in what the FTC puts into its complaint or analysis; in part *because* of the longevity of consent orders, as well as the unlikelihood of subsequent adjudication, there is no incentive to litigate in order to get a "better" statement of the rule, and no incentive, even if settling, to influence its content. Only the remedy matters.

But this means not even parties to FTC actions have influence over rules, and even this (small) feedback mechanism is absent. Coupled with the absence (because of these incentives to settle rather than litigate) of judicial review, there is nothing other than the fanciful idea that a succession of political appointees engaged in majority voting, along with the staffers trying to influence them, independently and intentionally creates an evolving body of law with its case selection and settlements. The fact that no discernible evolutionary path is evident is testament to the absurdity of this claim.

Lawyers as repeat players

Bailey & Rubin point out that even though injured *individuals* are not repeat players (with an interest in precedent a la Rubin), the lawyers who represent them often are, and they have an interest in expanding the reach and content of laws. Thus adjudication in civil courts may demonstrate the symmetrical interests in precedent likely to lead to efficient outcomes.

Of course, a dedicated cadre of lawyers revolves around the FTC. But arguably, they have the opposite effect. Their incentive is to maintain a certain level of legal scope, to be sure, but even more, their interest is in facilitating relationships with FTC Commissioners and staff. This translates into a disincentive to rock the boat or challenge Commission outcomes directly, rather than a heightened interest in litigation.

Evidence of this comes from LabMD's CEO, who writes that his repeated, initial efforts to find a consumer protection lawyer to bring his (first-ever) legal challenge to an FTC data security complaint were met with statements of support for the strength of his case and the soundness of his arguments, but a succession of steadfast refusals to take his case, precisely because it would amount to challenging the agency and would imperil the lawyers' standing with its personnel.

The Process of FTC Adjudication Versus Private Civil Actions

In a private data security action, including claims by state regulators, the plaintiff must bring a lawsuit in a court of law. This is important for several reasons. First, this means that the plaintiff must be able to allege sufficient facts in the complaint to survive a motion to dismiss.[9] While the standard under FRCP 8(a) is relatively liberal, it still requires the plaintiff to plead enough facts to make the claim plausible on its face. As stated by the Supreme Court in *Iqbal*: there must be more than "threadbare recitals of the elements of a cause of action, supported by mere conclusory statements."[10] The plaintiff must also be able to allege a cognizable harm in order to survive a motion to dismiss on standing grounds. These rulings help businesses know what they can be held liable for, even if suits end in settlements or dismissals before reaching the merits.

Further, courts have the ability to weed out cases which cannot meet the standard of plausibility or legal possibility before plaintiffs can get to discovery. Discovery costs are often one of the largest expenditures defendants face.[11] Many defendants will settle to avoid them, even if they do not believe the underlying claim has merit.[12] These features of private suits limit the ability of plaintiffs to use the legal system to remedy alleged data security harms—but they also provide important procedural protections to defendants the reduce pressure to settle unnecessarily.

When the FTC brings a Section 5 suit, however, they do not need to bring the suit in a court of law. The FTC can instead begin an investigation into possible data security problems by coming directly to a business and asking for their cooperation in a non-public inquiry. Of course, private litigants could do this, too, but defendants are less likely to cooperate in private cases. This is because the FTC has the ability to use civil investigative demands (CIDs), which are like a sub-

---

[9] *Iqbal*, 556 U.S. at 678; *Twombly*, 550 U.S. at 570.

[10] *Iqbal*, 556 U.S. at 678.

[11] LAWYERS FOR CIVIL JUSTICE, ET. AL, LITIGATION COST SURVEY OF MAJOR COMPANIES (2010), *available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Duke%20Materials/Library/Litigation%20Cost%20Survey%20of%20Major%20Companies.pdf.

[12] Pamela A. MacLean, *Cost of Discovery a Driving Force in Settling Cases, Study Shows*, THE NATIONAL LAW JOURNAL (Sept. 10, 2008), http://www.alm.law.com/jsp/article.jsp?id=1202424413938&slreturn=20140412095737 (a "joint survey, released… by the American College of Trial Lawyers and the Institute for the Advancement of the American Legal System, found that 83 percent of the nearly 1,500 lawyers responding found costs, not the merits of a case, the deciding factor in settling").

poena and have very little judicial review attached to them.[13] In a direct reversal of the procedure in private suits, the FTC gets to do discovery before showing an independent reviewer that it has sufficient facts to plead a plausible harm or show that the harms alleged are legally cognizable.

Even after investigating a company, entirely at the company's expense, the FTC need not bring a complaint in a court of law. The FTC has the ability to bring complaints in Part 3 adjudications,[14] as it has in *FTC v. LabMD*. Even if a defendant can win in front of the Administrative Law Judge, the FTC can then appeal to the FTC Commissioners who brought the original suit itself before the lawsuit reaches judicial review. As FTC Commissioner Wright notes:

> [T]he key to understanding the threat of Section 5 is the interaction between its lack of boundaries and the FTC's administrative process advantages.... Consider the following empirical observation that demonstrates at the very least that the institutional framework that has evolved around the application of Section 5 cases in administrative adjudication is quite different than that faced by Article III judges in federal court in the United States. The FTC has voted out a number of complaints in administrative adjudication that have been tried by administrative law judges ("ALJs") in the past nearly twenty years. In each of those cases, after the administrative decision was appealed to the Commission, the Commission ruled in favor of FTC staff. In other words, in 100 percent of cases where the ALJ ruled in favor of the FTC, the Commission affirmed; and in 100 percent of the cases in which the ALJ ruled against the FTC, the Commission reversed. By way of contrast, when the antitrust decisions of federal district court judges are appealed to the federal courts of appeal, plaintiffs do not come anywhere close to a 100 percent success rate. Indeed, the win rate is much closer to 50 percent.[15]

All the while, companies face all the costs of responding to the FTC's requests for information.[16] Of course, the FTC may bring suit in a court of law, like it did in *FTC v. Wyndham*. But *Wyndham* is the first data security case litigated by the FTC in a court of law in the entirety of its 11 years

---

[13] In fact, the FTC Commissioners in charge of issuing the CID hear the motion to quash before it can be appealed to a court of law. *See, e.g.*, FTC v. LabMD, Inc., No. 1:12-cv-3005-WSD, at 11-12 (N.D. Ga. Nov. 26, 2012); In the Matter of LabMD, Inc., No. 102-3099 at 9 (Apr. 20, 2012).

[14] 16 C.F.R. § 3.1 *et seq.* (2003).

[15] Joshua Wright, *Recalibrating Section 5: A Response to the CPI Symposium* at 4, CPI ANTITRUST CHRONICLE (November 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/recalibrating-section-5-response-cpi-symposium/1311section5.pdf.

[16] This cost is not negligible in data security cases. Mike Daugherty, CEO of LabMD, estimated in 2012 that his business had spent over $500,000 fighting the FTC investigation to that point. Amy Wenk, *Atlanta Medical Lab Facing Off Against FTC*, ATLANTA BUSINESS CHRONICLE (September 5, 2012), http://www.bizjournals.com/atlanta/print-edition/2012/09/07/atlanta-medical-lab-facing-off-against.html. LabMD provided thousands of pages of documents and met face-to-face with FTC officials 7 times before a complaint was even issued. *See* Verified Complaint of LabMD v. FTC in United States District Court for the District of Columbia ¶¶ 54-78, *available at* http://causeofaction.org/assets/uploads/2013/11/LabMD-Inc.-v.-FTC-et-al.Complaint.11.14.2013.pdf.

brining such cases. All of the others, aside from the two mentioned, have ended in consent decrees, *with no judicial review*. These consent decrees are offered the same day as the complaint is made public.

The use of consent decrees in these cases carries with it some important effects. First, it prevents outsiders (including other businesses subject the FTC's regulatory oversight) from assessing the circumstances of the case and its settlement and the respondents' decisions to accept the consent order, leaving them without significant guidance as to the viability of their own conduct.

> There is, in other words, no candid discussion of the facts or policy arguments that weighed against a decision to intervene, or presentation of objective information that would allow an external observer to construct the relevant arguments.[17]

Moreover, consent orders offer very little information to assist third parties in discerning and evaluating the FTC's strategy and tactics, and very little information useful to their decisions whether to challenge any private litigation in court or accept settlements there (see below on the litigate/settle decision).

In part for these reasons, respondents in FTC actions have little incentive to challenge the FTC even in its own administrative court (hence the near-perfect record of consent decrees). As Commissioner Wright further notes (discussing Section 5's Unfair Methods of Competition provision, but in language equally applicable to UDAP):

> The combination of institutional and procedural advantages with the vague nature of the Commission's Section 5 authority gives the agency the ability, in some cases, to elicit a settlement even though the conduct in question very likely may not be anticompetitive. This is because firms typically prefer to settle a Section 5 claim rather than going through lengthy and costly administrative litigation in which they are both shooting at a moving target and have the chips stacked against them. Significantly, such settlements also perpetuate the uncertainty that exists as a result of the ambiguity associated with the Commission's UMC authority by encouraging a process by which the contours of Section 5 are drawn without any meaningful adversarial proceeding or substantive analysis of the Commission's authority.[18]

FTC Consent decrees usually require companies to do a number of things in order to correct the alleged data security violations, along with reporting requirements and FTC oversight for 20 years.[19] The FTC does not require businesses to admit guilt in consent decrees, but the relatively long length of the decrees gives the FTC considerable power over their business practices.

---

[17] Gellhorn & Kovacic, Analytical Approaches and Institutional Processes for Implementing Competition Policy Reforms by the Federal Trade Commission, [FTC Hearings] (1995).

[18] Wright, *Recalibrating*, *supra* note 15, at 5.

[19]

The FTC may penalize even the slightest violation of a consent decree, even if the violation was not willful or resulting in any damages.[20]

It is noteworthy, however, that the FTC has no ability to levy penalties on defendants directly. While consent decrees can impose relatively costly reporting requirements on businesses, fines of up $10,000 can be levied by the FTC only if consent decrees – not Section 5 itself – are violated.[21] In private actions, on the other hand, litigants seek monetary judgments, and these could amount to significant sums.

It is also worth noting that even in cases alleging a claim based on deception, the FTC generally requires improved security practices in its consent orders, not merely disclosure. As we discuss in the next section, this imposes a far more costly remedy on respondents than would a mere disclosure requirement (or injunction against misrepresentation).

Defendants Generally Settle in Private Actions if Actual Harm is Plead

Another paper that looked at private data security actions made several findings that support the proposition that there is a surprisingly-well functioning common law marketplace for data security remedies. The work of Romanosky, Hoffman, and Acquisti found that the

> overall settlement rate in our dataset (86/164 = **52%**) is much higher than legal privacy scholarship would suggest… The top two pair-wise comparisons illustrate a similar result: the majority of cases that allege actual harm or achieved class certification, settled. That is, **of the cases that alleged actual harm (n=28), 71% of them settled,** whereas only 49% of them without actual harm (n=135) settled. Similarly, o**f the cases that achieved class certification, 85% settled**, whereas when the class was not certified, only 48% settled.[22]

Even "data breach lawsuits lacking actual harm or class certification are almost as equally likely to reach settlement as dismissal. That is, in cases without these characteristics, the plaintiff faces approximately a 50/50 chance of obtaining a settlement."[23] In other words, actual harms are already consistently remedied without FTC intervention through Section 5.

Other findings corroborate our own, as well as contribute additional details to the description of private data security actions:

- odds of a firm being sued are 3.5 times greater when individuals suffered financial harm, but over 6 times lower when the firm provides free credit monitoring to those affected by the breach. Moreover, the odds of a firm being sued as a result of improperly disposing data are 3 times greater relative to breaches caused by lost/stolen data, and 6

[20] In the privacy realm, for instance, the FTC fined Google $22.5 million for promising on a help page that it would not collect information that was true at the time but later was inaccurate due to changes made by Apple in its Safari browser. *See* Berin and Geoff's stuff on that.

[21] 15 U.S.C. § 45(l) (2012).

[22] Sasha Romanosky, David Hoffman, & Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation* 19, 20 (Temple University Legal Studies Research Paper No. 2012-30, Apr. 6, 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1986461.

[23] *Id.* at 20.

times greater when the data breach involved the loss of financial information. Our analysis suggests that defendants settle 30% more often when plaintiffs allege financial loss from a data breach, or when faced with a certified class action suit. The odds of a settlement are found to be 10 times greater when the breach is caused by a cyber-attack, relative to lost or stolen hardware, and the compromise of medical data increases the probability of settlement by 31%.[24]

- 78% of federally-litigated breaches did not result in financial loss, while 22% did result in financial loss. However, breaches appear less likely to be litigated in federal court absent financial harm… breaches resulting from the unauthorized disclosure (or disposal) of personal information and computer hack (cyberattack) are more likely to be litigated in federal court, while breaches due to lost/stolen hardware are less likely to be litigated in federal court.[25]
- Breaches involving financial data and credit card numbers are more likely to be litigated in federal court, which provides some support for H1c. Social security numbers (SSN), on the other hand, comprised about 78% of non-litigated breaches, though only 58% of litigated breaches. Medical data appear to be equally represented in federally-litigated and non-federally-litigated breaches.[26]

Analysis of FTC Complaints and Consent Decrees

The basic attributes of these complaints and settlements/judgments in the administrative and civil court cases permit some tentative conclusions regarding the validity of the FTC's "common law" claim. As we discuss above, the nature of the FTC's process suggests that several of the expected attributes of common law adjudication will be absent from its cases, and the data suggest that they are.

First, there is no reference or citation to precedent in the FTC administrative cases. While this isn't surprising for administrative adjudications consisting of only complaints and consent orders, the absence of analysis and reference to precedent do challenge the characterization of the FTC's data security actions as "common law." It is true that some of the accompanying Analyses to Aid Public Comment include reference to prior cases and some further analysis.[27] But these references and analyses aren't particularly helpful to the argument.

In several cases there *is* a blanket reference to prior cases with similar orders. In the Analysis to Aid Public Comment in *Nationwide*, for example, the Commission notes that "[t]his provision is substantially similar to comparable provisions obtained in prior Commission orders under Section 5 of the FTC Act," followed by citations to four cases: *Petco*, *Tower Records*, *Guess?* and *Microsoft*. But as none of these cases was brought under GLB, nor any of the respondents a financial institution – among many other differences – far from demonstrating adherence to prece-

[24] *Id.* at 3.

[25] *Id.* at 12.

[26] *Id.* at 13.

[27] We haven't completed our review of the ancillary documents, but suggest some preliminary observations here.

dent, the reference actually suggests the opposite: that the FTC decides cases *without* regard to the relevant facts of its prior cases.

In fact, in keeping with the administrative enforcement model, the majority of the FTC's cases, regardless of cause of action or facts, impose the same remedy: the set of security standards laid out in the FTC's Safeguards Rule. Most notably, this is true regardless of whether the respondents were financial institutions (to which the Safeguards Rule directly applies) or not (to which the Rule has no direct application), and regardless of whether the claim is generally one of deception or unfairness.

This latter point underscores the reality that, in practice, the FTC generally enforces a "reasonableness" standard in all data security cases, requiring security practices to be "reasonable," but leaving the exact definition of "reasonableness" in any given context undefined. The lack of differentiation in analysis and between remedies applied to respondents with different characteristics, engaged in different conduct, and challenged under different legal standards is damning to the FTC-consent-decrees-as-common-law theory.

Also worth noting is that while at the FTC all actions but one were decided in the FTC's favor with a settlement, nearly all of the actions in civil court were decided in the defendant's favor by motion to dismiss. There may be any number of explanations for the discrepancy, of course, but the stark difference in outcomes between the actual common law and the FTC's process suggests that the two are not operating in the same fashion.

Meanwhile, the discrepancy in outcomes in the cases in which both the FTC and a private plaintiff brought cases against the same actor for the same conduct (discussed below) bolsters this conclusion. At minimum, the willingness of respondents/defendants to settle with the FTC – in some cases even *after* winning a motion to dismiss in civil court – stands in stark contrast to the parties' willingness to fight – and win – in civil court.

While much of this can surely be explained by the availability of a motion to dismiss before discovery in civil court, it is precisely that difference in process that further condemns the common law argument.

As Gellhorn and Kovacic note (writing about antitrust cases, but with equal applicability here):

> [B]ecause the information that formally accompanies the release of consent agreements is so austere and incomplete, the emphasis on consent agreements as policy instruments magnifies the role of enforcement agency discretion and correspondingly increases the importance of Washington insiders as means for identifying and articulating the basis for the exercise of such discretion.[28]

Our analysis of the cases bolsters the claim that little in the way of guidance is offered by the cases, and even less in the way of information relating to the FTC's overall aims in its data security "jurisprudence." To the extent that a common law process is evolutionary and accretive, the FTC's process is decidedly not.

Moreover, compared to civil court adjudication, we expect the FTC's complaints to lack specificity. This is largely borne out in the cases we analyzed.

---

[28] Gellhorn & Kovacic, supra note. ____.

Franklin's Budget Car Sales, Inc. is representative. The FTC's complaint alleges that respondent violated the Safeguards Rule (enforced via the FTC Act) by:

- Failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information;
- Failing to design and implement information safeguards to control the risks to customer information and failing to regularly test and monitor them;
- Failing to investigate, evaluate, and adjust the information security program in light of known or identified risks;
- Failing to develop, implement, and maintain a comprehensive written information security program; and
- Failing to designate an employee to coordinate the company's information security program.[29]

The Consent Order addresses these issues by

- Prohibiting misrepresentation of respondent's security practices;
- Prohibiting the "violat[ion of] any provision of the . . . Safeguards Rule . . . or the . . . Privacy Rule."
- Requiring the establishment and implementation of "a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers."

Implementation of the security program must include:

- The designation of an employee or employees to coordinate and be accountable for the information security program;
- The identification of material internal and external security risks;
- The design and implementation of reasonable safeguards to control the risks identified through risk assessment;
- The development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information;
- The evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring; and
- The implementation of biennial assessments from an objective third party.[30]

While some of the language in the Order is fairly specific, none of it is tied in any meaningful way to specific factual allegations of defective security practices. Instead, the Complaint alleges generally unreasonable practices and the Order requires the implementation of generally reasonable practices. Where more specific problems are identified (e.g., failure to implement

29

30

"safeguards," failure to develop a "comprehensive written information security program," failure to "designate an employee to coordinate a security program"), there is considerable vagueness even in this relative specificity: Nowhere does the agency specify *how* to implement its directives — what type of employee will be sufficient, what "reasonable safeguards" entail, etc.

The language here is drawn from the FTC's standards for the Safeguards Rule. According to the FTC, these standards are, by design, "flexible, and contain few, if any, specific requirements."[31] As it happens, nearly all of the FTC's consent orders contain essentially the precise language of the standards. In other words, the FTC's cases offer no additional evaluation or information to respondents — or anyone else regulated by the FTC — beyond that contained in the FTC's "flexible" Standard (implemented in 2002). One would be hard-pressed to identify any evolving standards in the FTC's Orders over the decade in which the cases arise, and there is no discernible nexus between the specific facts of any case and the corresponding remedy.

Thus, in the case of *Franklin's Budget Car Sales*, although the PII was accessed through a P2P network, the Complaint and Order are nearly identical to other cases in which no P2P network was involved. In *Tower Records*, for example, the problem was "broken account and session management." Nevertheless, the remedies in both cases are nearly identical, as are the claims.

While misrepresentation (deception) is obviously not dependent on the specific defect leading to the release of PII in contravention of a respondent's privacy claims, the absence of any information sufficient to evaluate the "reasonableness" of security practices, the materiality of the misrepresentation and the extent of harm render the FTC's actions little more than simple, unembellished restatements of the general principles incorporated in the statutory language.

Tower Records' breach lasted for 8 days and affected 5,225 consumers; Franklin's Budget Car Sales' affected 95,000 consumers. Moreover, Tower Records was a sizeable national retailer, while Franklin's was a local car dealership in Statesboro, Georgia. We don't yet have precise data on the sizes of the two (privately-held) companies, but it is hard to imagine that Tower putting at risk the PII of 5,000 of its enormous number of customers is in any way comparable to Franklin's putting at risk the PII of 95,000 consumers. Can general statements that private data will be protected in both of these lead to material misrepresentation, particularly given that the FTC's complaints allege only that such statements "were disseminated or caused to be disseminated"?

For each of these companies the essential claim was of "unreasonable" security practices, and the remedies essentially identical.

Qualitative Analysis: Overlap Cases

There are seven cases that are overlapping between the FTC and Federal District Court.[32] Only one is a Federal District Court case that has a party which overlaps with a case brought by the United States under the authorization of the FTC at the Federal District Court; the remaining six overlap with the FTC administrative cases.

---

[31] FTC, Standards for Safeguarding Consumer Information, 16 CFR Part 314 (2002), http://www.ftc.gov/os/2002/05/67fr36585.pdf.

[32] There are two cases in the Federal District court with DSW, Inc. as a party to the case that make of 2 of the 6 cases.

These cases are particularly useful for analyzing the different processes followed by the FTC and private litigants. Comparing the complaints, opinions, and settlements will also be useful for evaluating some of the theories proposed above. Below, we will use our available data to present case studies on the overlapping cases and offer some preliminary observations.

In Re TJX[33]

TJX Companies, Inc., a corporation with many subsidiaries, which includes large retail stores such as TJ Maxx, Marshalls, and Homegoods,[34] had sensitive consumer data breached by hackers over a fourteen-month period from July 2005 to mid-January 2007. According to the Wall Street Journal,

> The biggest known theft of credit-card numbers in history began... outside a Marshalls discount clothing store near St. Paul, Minn. There, investigators now believe, hackers pointed a telescope-shaped antenna toward the store and used a laptop computer to decode data streaming through the air between hand-held price-checking devices, cash registers and the store's computers. That helped them hack into the central database of Marshalls' parent, TJX Cos. in Framingham, Mass., to repeatedly purloin information about customers... The $17.4-billion retailer's wireless network had less security than many people have on their home networks, and for 18 months the company -- which also owns T.J. Maxx, Home Goods and A.J. Wright -- had no idea what was going on. The hackers, who have not been found, downloaded at least 45.7 million credit- and debit-card numbers from about a year's worth of records, the company says. A person familiar with the firm's internal investigation says they may have grabbed as many as 200 million card numbers all told from four years' records.[35]

This massive data breach led to two private lawsuits and an FTC investigation.

Private Suits Against TJX

Two different groups filed the private suits. One was a class action of TJX consumers whose credit and debit cards were compromised due to the data breach.[36] The other was a class action by a group of financial institutions that were the issuers of the credit and debit cards, which were compromised by the breach.[37]

The consumer class action plaintiffs brought a number of counts in their complaint, including negligence, breach of both implied and third party beneficiary contracts, and two counts of unfair trade practices under the Massachusetts consumer protection law. All of the counts cen-

---

[33] Although this case was not included in the previous data coding analysis due to data complexity, we discuss this case here as it is relevant to understanding how data security cases brought by both the FTC and private parties against the same company interact and relate to one another, as we attempt to understand similarities and differences of the common law at both the FTC and Federal District court of these data security breach actions.

[34] http://www.tjx.com/about-tjx.asp

[35] http://online.wsj.com/news/articles/SB117824446226991797

[36]

[37]

tered on the fact that TJX failed to provide reasonable data security for sensitive consumer information it retained. All of the allegations were dealt with in detail in a 46-page complaint.[38]

While the class action led to a settlement agreement,[39] the complaint had several possible negligence arguments that could have been developed at trial. The first was that TJX was negligent for failing to live up to industry standards on the security of credit and debit card information. PCI standards that were allegedly violated include the failure to set up a firewall and encrypt customer data. Rules set up by Visa and MasterCard also required certain levels of data security, like limits on time for data storage, which TJX allegedly failed to provide. A second negligence argument was that TJX failed to reassess and fix its data security problems in a timely manner, allowing more breaches of consumer data to occur. A third negligence argument was that TJX failed to alert consumers of the data breach in a timely manner. A fourth negligence argument was that TJX did not reasonable data security pursuant to a special fiduciary relationship with the consumer.

The second and third counts of the consumer class action involved breach of contract claims. The second count claimed that the consumer-plaintiffs were intended third party beneficiaries of the contracts between TJX and the banks and credit/debit card companies that processed the payments. As a result, the provisions referred to in the negligence section would be actionable contract terms. The third count argued that there was an implied contract between the consumers and TJX due to the consumers giving TJX sensitive personal information.

The fourth and fifth counts of the consumer class action arose under Massachusetts' consumer protection law which is modeled after FTC Section 5. The complaint alleged that TJX engaged in an unfair or deceptive trade practice by failing to provide safeguards for the data and by retaining the data longer than necessary. Neither count specifies in detail whether they are asserting unfairness or deception, or the elements of such a claim. Count four alleges TJX acted "willfully, knowingly, and in bad faith." Both counts allege the plaintiffs suffered actual damages as a result of the unfair practices.

The consumer class action was settled, with the announcement coming on September 21, 2007. The settlement was approved, but there was some court adjudication of the issue of attorneys' fees.[40] The settlement included promises from TJX to:

> a. reimburse these customers for the documented cost of certain drivers' license replacements and, if their drivers' license or other ID numbers were the same as their social security number, for certain losses from identity theft;
>
> b. offer vouchers for use in these TJX stores in the country in which they reside for any customers who show they shopped at TJX stores located in the U.S., Canada and Puerto Rico (excluding Bob's Stores) during the relevant periods and incurred certain costs as a result of the intrusion;
>
> c. hold a future, one-time, three-day Customer Appreciation special event in which prices at all T.J. Maxx, Marshalls, HomeGoods and A.J. Wright stores in

[38]

[39] http://www.tjx.com/Press%20release%20electronic.pdf

[40] The only published opinion on the consumer track of the litigation that we found.

> the U.S. and Puerto Rico and all Winners and HomeSense stores in Canada will be reduced by 15%; and
>
> d. complete an evaluation by plaintiffs' independent security expert on the computer security enhancements made and planned by TJX and accepted by the plaintiffs' counsel.[41]

Many of the claims brought in the consumer complaint would have been whittled down if the case progressed further, as evidenced by the financial institutions track of the litigation under many of the same claims. As will be seen below, even though both lawsuits ended up in settlement, law was still created through the process of court review of the complaints.

Similar to the consumer complaint, the complaint from the financial institutions alleged negligence, breach of contract, and violation of the Massachusetts Unfair Trade Practices law.[42] Much like the consumers, the financial institutions went into considerable detail on the data breach and the alleged harms in its 32-page complaint. Unlike the consumer complaint, which ended in a settlement before any judicial opinions were issued, the complaint from the financial institutions ended up in court and many of the counts were dismissed. TJX settled with many of the plaintiffs in the financial track, but AmeriBank and SELCO continued a class action lawsuit for a considerable period of time before settling, and several decisions were issued by courts of law before they settled as well. Below, we will explain each count, whether it was dismissed, and why it was or was not dismissed.

The first count of breach of contract was based upon the theory that the financial institutions were intended third party beneficiaries of the agreements between TJX, Fifth-Third Bank, and the credit card companies. The biggest problem for this argument was that the contract between TJX and Fifth-Third Bank stated it was "for the benefit of, and may be enforced only by, Bank and Merchant… and is not for the benefit of, and may not be enforced by any third party."[43] The district court and the First Circuit rejected the idea that this agreement was superseded by the Visa and MasterCard agreements that both stated they do not constitute third-party beneficiary contracts, and dismissed the claim.

The complaint broke the negligence counts out into negligence, negligent misrepresentation, and negligence per se. The second count of negligence is based upon the theory also put forth by the consumer complaint: TJX breached its duty of care established by industry standard evidenced in the agreements mentioned above. The courts rejected this theory on the basis of the economic loss doctrine.

The third count of negligent misrepresentation argues that even if there is no contract per se, the plaintiffs justifiably relied on the promises by TJX and Fifth-Third Bank to follow industry standards for data security when issuing credit and debit cards. The courts did not dismiss this claim, since negligent misrepresentation is an exception to economic loss doctrine's bar, but said it was on "life support" if it relied only on an implied promise by conduct.

41

42

43 *In re TJX Co. Retail Sec. Breach Litigation*, 564 F.3d 489, 499 (1st Cir. 2009).

The fourth count of negligence per se was also dismissed because the defendants were not financial institutions under the GLB.

The final count alleging violations of Massachusetts' consumer protection law was much more detailed in the financial institutions' complaint than in the consumer complaint. There were several theories that would later be evaluated by courts. The first was that since TJX provided inadequate data security, under how it has defined pursuant to FTC settlements via its Section 5 authority, it could be held liable under the Massachusetts law for unfair business practices. The second argument would be also that TJX could be held liable for a deceptive business practice (similar to Section 5), since it failed to provide certain data security practices promised in its agreements with Fifth-Third Bank and the credit card companies. The third argument was that TJX failed to comply with GLB Act requirements in how they handled data, opening them up to unfair business practice liability under the Massachusetts law.

The district court only allowed the negligent misrepresentation theory to go forward, dismissing the other two. The First Circuit, though, cast doubt on the negligent misrepresentation theory (analogous to Section 5 deception) for the same reason it argued it was on "life support" as a stand-alone claim: the weakness of relying on conduct alone to imply a promise. Further, it would later rule that such a claim is not certifiable as to the class. The plaintiffs gave up on the GLB claim because TJX was not a financial institution under the GLB's definitions. Importantly, though, the First Circuit reversed the District Court and allowed the plaintiffs to go forward on the unfairness claim based upon general factors identified by the FTC as making a practice unfair. While the district court rejected reliance on FTC consent decrees because they are not binding law, the First Circuit said they could be used as persuasive authority nonetheless and decided the unfairness claim under Massachusetts law should not be dismissed.

Throughout this opinion, the First Circuit cited and discussed opinions that arose from the *BJ's Wholesale* data security litigation.[44] This shows that law can be created and precedent followed in private actions even when cases end up in settlements. Court review of claims usually occurs before settlement in private actions, even though the settlement of the consumer class action serves as a counter-example.

On September 2, 2009, about 4 months after the First Circuit's ruling, TJX would settle with the remaining plaintiffs in the financial litigation track.

The FTC's Complaint and Settlement with TJX

The FTC's complaint against TJX is a quite meager 3 pages. The most important of the complaint was summarized this way:

> Since at least July 2005, respondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its networks. In particular, respondent:
>
> a) created an unnecessary risk to personal information by storing it on, and transmitting it between and within, in-store and corporate networks in clear text;

44

b) did not use readily available security measures to limit wireless access to its networks, thereby allowing an intruder to connect wirelessly to in-store networks without authorization;

c) did not require network administrators and other users to use strong passwords or to use different passwords to access different programs, computers, and networks;

d) failed to use readily available security measures to limit access among computers and the internet, such as by using a firewall to isolate card authorization computers; and

e) failed to employ sufficient measures to detect and prevent unauthorized access to computer networks or to conduct security investigations, such as by patching or updating anti-virus software or following up on security warnings and intrusion alerts.[45]

The FTC's complaint alleges these practices together constitute unfairness because they were not "reasonable" or "appropriate." The FTC's allegation is similar, though in much less detail, to the negligence and negligent misrepresentation claims brought in the private actions. While the facts in the complaint may be enough to allege substantial injury, the FTC's complaint does not have any facts on countervailing benefits or reasonable avoidability.

The FTC's complaint and consent decree with TJX were issued on July 28, 2008, almost 10 months after TJX announced its settlement with consumers and in the middle of the ongoing financial track litigation against TJX. It is unclear how long the FTC had been investigating TJX before bringing its complaint, but the negotiated consent decree that at least some time elapsed.

Nonetheless, it does not appear that the FTC filled any gaps by bringing this case. Private actions had already led to one settlement before the FTC issued its complaint. Eventually, the private action would lead to a second settlement (as mentioned above), and on June 22, 2009, TJX would settle with 41 state AGs acting under their consumer protection laws as well for over $9.5 million.[46] This appears to be an example of the FTC piling on a defendant who already likely had sufficient incentives to be deterred from future bad behavior. This was an easy win for the FTC, though, and another settlement to put on the books.

In Re Ceridian

Ceridian Corporation is a large payroll-processing firm that processed payroll for over 20 million employees nationwide at the time of the suit. Ceridian comes into contact with sensitive personal information as a result of its business. Late December 2009, Ceridian's security system was breached, and the hacker was able to gain access to the names, addresses, dates of birth, social security numbers, and bank account and routing information of 27,000 employees. Allegedly, Ceridian kept information longer than necessary and did not provide sufficient safeguards

45

46

for the information, like encryption. This breach led to a private class action lawsuit and an FTC investigation, which culminated in a complaint and consent decree.

Reilly v. Ceridian

Reilly v. Ceridian started as a class action complaint originally brought by Kathy Reilly and Patricia Pleumacher on behalf of all those similarly situated. The complaint alleged negligence, breach of contract, breach of the covenant of fair dealing, consumer fraud, and violation of the New Jersey Identity Theft Prevention Act. The complaint was relatively short, at 20 pages, but it did assert facts and relate them to the legally actionable claims.[47]

The first count was negligence. Much like *In Re TJX*, the plaintiffs alleged Ceridian was negligent in keeping the information longer than necessary (after employees stopped working for the employer Ceridian did work for) and failing to provide reasonable data security. Unlike *In Re TJX*, the plaintiffs did not allege any violation of industry standards.

The second count was for breach of contract. The plaintiffs alleged they were intended third party beneficiaries of a promise to provide safeguards for data security, either implicitly or explicitly. The argument about the underlying contract is rather vague, based on only "information and belief" that is not spelled out in the complaint.

The third count was for breach of the covenants of good faith and fair dealing. These covenants are implied in all contracts in New Jersey and the complaint alleges that Ceridian should have taken steps to secure the private information under their care, especially in light of a previous data breach.

The fourth count was for consumer fraud, but it actually arose under a New Jersey consumer protection statute with some similarities to FTC Section 5's deception authority. The complaint alleges the inadequate data security and failure to get rid of information no longer relevant were actually deceptive practices. The complaint does not actually allege what promise was made, though.

The final count arose under New Jersey's Identity Theft Prevention Act. The Act requires timely destruction of customer's records and expedient disclosure of security breaches. The complaint alleges Ceridian failed to do either.

Ceridian's case was dismissed by the District Court of New Jersey for a lack of standing, and in the alternative, for failure to state a claim. This dismissal was affirmed by the Third Circuit Court of Appeals. The court concluded:

> 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… In data breach cases where no misuse is alleged, however,

47

> there has been no injury—indeed, no change in the status quo. Here, Appellants' credit card statements are exactly the same today as they would have been had Ceridian's database never been hacked... Finally, we conclude that Appellants' alleged time and money expenditures to monitor their financial information do not establish standing, because costs incurred to watch for a speculative chain of future events based on hypothetical future criminal acts are no more "actual" injuries than the alleged "increased risk of injury" which forms the basis for Appellants' claims.[48]

In other words, the lack of actual charges to the credit cards and mitigation efforts unconnected to any present harm are not sufficient to be actual or imminent injuries.

Despite its disposition at the motion to dismiss stage, this data security case still moved the law forward by setting an important legal precedent, offering guidance as to what does *not* count as actual injury sufficient to bring cases against businesses that have their data breached.

The FTC's Complaint and Settlement with Ceridian

Much like *In Re TJX*, the FTC's complaint is only 3 pages.[49] The FTC alleges both unfairness and deception.

The FTC's unfairness claim was based on 5 arguments; Ceridian:

1. stored personal information in clear, readable text;
2. created unnecessary risks to personal information by storing it indefinitely on its network without a business need;
3. did not adequately assess the vulnerability of its web applications and network to commonly known or reasonably foreseeable attacks, such as "Structured Query Language" ("SQL") injection attacks;
4. did not implement readily available, free or low-cost defenses to such attacks; and
5. failed to employ reasonable measures to detect and prevent unauthorized access to personal information.[50]

The FTC's complaint does not allege any facts on countervailing benefits or reasonable avoidability. Worse, the complaint does not allege any facts on substantial injury either aside from the fact of the data breach itself. This sparse and conclusory count seems unlikely to survive a *Twombly*-style challenge.

The FTC bases its deception claim on two web pages. The first stated:

> Worry-free Safety & Reliability . . . When managing employee health and payroll data, security is paramount with Ceridian. Our comprehensive security pro-

48

49

50

> gram is designed in accordance with ISO 27000 series standards, industry best practices and federal, state and local regulatory requirements.[51]

The complaint does not explain in any detail what those standards, best practices, or regulatory requirements were nor how Ceridian allegedly failed to live up to them, other than pointing to the breach itself. The second stated:

> Confidentiality and Privacy: [Ceridian] shall use the same degree of care as it uses to protect its own confidential information of like nature, but no less than a reasonable degree of care, to maintain in confidence the confidential information of the [customer].[52]

Based on just these two promises, the FTC alleges deception, based upon essentially the same criteria as the unfairness claim: unreasonable data security. At the end of the day, both the unfairness and deception claim were based upon the same underlying facts.

In light of *Reilly*, it seems unlikely that the FTC's complaint would survive a motion to dismiss. Not only did the Commission in no way show that there was an actual injury (or even an imminent injury), but it also likely failed to plead enough facts to survive even basic pleading standards, as the much more detailed complaint was dismissed on those grounds as well by the district court. Regardless, the FTC was able to impose upon Ceridian a 20-year consent decree, starting on June 8, 2011. At that point, the District Court had already granted the motion to dismiss in *Reilly* and the Third Circuit would soon after affirm that decision in December 2011.

One could perhaps argue that the FTC was fulfilling its gap-filling role in this case, since the private law market seemed to fail. The difficulty in such an argument is that the requirement for an actual injury in a case may be a feature and not a bug.

Ceridian did not settle the private case, but did settle with the FTC – even after it had won a motion to dismiss. It is possible that this illustrates how the early imposition of investigative costs without court review incentivizes defendants to settle earlier in FTC cases. Another possibility, though, is that because the FTC did not have to fulfill the same legal standards of the private plaintiffs in *Reilly* to prove its case if it came to litigation, the defendants chose to settle. Without any actual precedent on data security under Section 5 to this point, it is tough to evaluate this problem. The legal uncertainty itself may be enough to incentivize settlements in light of the investigation costs.

In Re Cardsystems

Cardsystems is a company that specializes in processing credit card transactions. Obviously, the company had a considerable amount of personal financial information on consumers, most prominently, their names, addresses, and credit card numbers. In 2004, the company was subjected to attack by hackers, and the resulting data breach compromised the security of over 40 million credit card accounts and related transaction data. This led to a private class action on behalf of consumers and retailers in California, as well as an FTC investigation, which ended in a complaint and consent decree.

51

52

Parke v. Cardsystems Solutions, Inc.

Filed on June 24, 2005, the 16-page complaint by the plaintiffs alleged only two counts and one cause of action.[53] The first count arose under the California Business & Professions Code §§ 17200, alleging unfair, deceptive, and unlawful business practices by Cardsystems. The second count was for declarative relief, but plead no separate cause of action.

While there was only one cause of action plead, the allegations were aimed at several sub-arguments under the California law on unfairness. The first was that Cardsystems stored information improperly and retained it longer than they were allowed to under Visa and MasterCard rules. The second was *res ipsa loquitor*, or the idea that since Cardsystems was in charge of the data the whole time and a breach occurred, breach could not have happened any other way than by negligence on its part. The third is that Cardsystems assumed a duty, either through the business relationship itself, or a special fiduciary relationship and were thus required to use reasonable means to protect the data. The fourth is that the California Constitution's right to privacy imposed a duty on Cardsystems that they violated by inadequate data security. Fifth, the plaintiff's point to several statutes that create the duty to inform customers of a data breach and to not share data with third parties that Cardsystems allegedly violated. Finally, the plaintiffs alleged deception, as well, stating that Cardsystems held themselves out as "fiduciaries who implement and maintain systems to ensure the security of consumers' credit card account and other nonpublic information" and violated thus by the acts already described.

Perhaps in light of this potentially huge liability or possibly because of other financial problems, Cardsystems filed for bankruptcy before trial in Arizona on May 12, 2006. This complication led to a battle over jurisdiction that led to the only reported opinion we could find in the case. The October 11, 2006 opinion granted the defendant's motion to remand and denied the motion to transfer the case to Arizona for consolidation. While this may have been a victory for Cardsystems, the company settled with the plaintiffs before the next stage of the trial could begin on February 19, 2009. Unfortunately, the court did not reach the issues of injury or pleading in its opinion, meaning no new law on data security was created before settlement.

The FTC's Complaint and Settlement with Cardsystems

On September 5, 2006, the FTC released its complaint and settlement with Cardsystems. Again, the complaint was only 3 pages. The complaint alleged an unfair business practice by Cardsystems.

The FTC listed 6 reasons why Cardsystems' data security was unfair. Cardsystems:

1. created unnecessary risks to the information by storing it in a vulnerable format for up to 30 days;
2. did not adequately assess the vulnerability of its web application and computer network to commonly known or reasonably foreseeable attacks, including but not limited to "Structured Query Language" (or "SQL") injection attacks;
3. did not implement simple, low-cost, and readily available defenses to such attacks;

53

4. failed to use strong passwords to prevent a hacker from gaining control over computers on its computer network and access to personal information stored on the network;
5. did not use readily available security measures to limit access between computers on its network and between such computers and the Internet; and
6. failed to employ sufficient measures to detect unauthorized access to personal information or to conduct security investigations.[54]

In an unfortunate trend, the FTC failed again to allege any facts on countervailing benefits or reasonable avoidability. The FTC did list some facts about substantial injury, though, stating:

> In early 2005, issuing banks began discovering several million dollars in fraudulent credit and debit card purchases that had been made with counterfeit cards. The counterfeit cards contained complete and accurate magnetic stripe data, including the security code used to verify that a card is genuine, and thus appeared genuine in the authorization process. The magnetic stripe data matched the information respondent had stored on its computer network. In response, issuing banks cancelled and re-issued thousands of credit and debit cards. Consumers holding these cards were unable to use them to access their credit and bank accounts until they received replacement cards.[55]

In light of the ongoing case (and eventual settlement) in *Parke* when the FTC finally brought its complaint and settlement, it does not appear the FTC was motivated by a gap-filling function in this case. Granted, it is not clear with our current data how long the FTC was investigating Cardsystems before bringing the complaint. While many of the allegations probably would not have survived a motion to dismiss, it appears that the bankrupt Cardsystems may have wanted to settle any civil litigation it could in a timely manner. Cardsystems, already in the red, may have appeared to be an easy target for the FTC.

In Re DSW Shoe Warehouse, Inc.

DSW Shoe Warehouse is a large seller of footwear with 190 stores throughout 32 states in the United States. DSW uses its computer network to process credit and debit card payments, as well as check payments, in its store. Wireless access points connected the cash registers and in-store scanners to the computer network. Hackers were able to breach this connection and compromise 1,438,281 credit and debit cards (but not the personal identification numbers associated with the debit cards), along with 96,385 checking accounts and driver's license numbers. This massive breach led to two private class action lawsuits and an FTC investigation, which ended in a complaint and consent decree.

Private Suits Against DSW

The data breach at DSW led to two private class action complaints, one filed in Michigan and one in Ohio. Both ended in court opinions and dismissals. Theresa Hendricks filed Michigan case on behalf of a class of similarly situated individuals. Tracy Key filed the Ohio case, also on

54

55

behalf of a class of similarly situated individuals. Both complaints came after and based themselves on facts made available due to the FTC's investigation and complaint against DSW.

The complaint in *Hendricks v. DSW* pled 3 separate counts in the plaintiff's 21-page complaint.[56] The first count was breach of contract with its customers, alleging that there was an implied term for reasonable data security when DSW assumed control over its customers' personal financial information. The second count was breach of contract with card issuers, of which the consumers were the intended third-party beneficiaries. The contracts DSW had with major credit card companies required various data security that DSW failed to fulfill, such as:

1. creating unnecessary risks to the information by storing it in multiple files when it no longer had a business need to keep the information;
2. not using readily available security measures to limit access to its computer networks through wireless access points on the networks;
3. storing the information in unencrypted files that could be accessed easily by using a commonly known user ID and password;
4. not limiting sufficiently the ability of computers on one in-store network to connect to computers on other in-store and corporate networks; and
5. failing to employ sufficient measures to detect unauthorized access.[57]

The third count arose under the Michigan's Consumer Protection Act, pleading both unfairness and deception claims analogous to what the FTC would plead under its Section 5 authority. The deception claim is that DSW omitted the material fact that it did not provide adequate data security, intending that the plaintiff trust the company to protect their data. The unfairness claim was that DSW failed to take appropriate measures to protect plaintiff's information in such manner that it would not be accessed or compromised by an unauthorized third party and that this could not reasonably be known by the plaintiff. Also, DSW failed to promptly inform Plaintiff that her personal information had been compromised by an unauthorized third party.

Hendricks v. DSW was dismissed by the Federal District Court for the Western District of Michigan for a lack of cognizable damages and a failure to establish a duty of disclosure.[58] The only injury that resulted from the data breach was the cost of a credit monitoring product. The court rejected this mitigation cost as an injury here because the facts alleged did not indicate that the plaintiff had her identity stolen or that her personal information had been used to her detriment in any way. Without an actual or imminent injury, the complaint would be dismissed for failure to state any injury for the purposes of contract law or the Michigan Consumer Protection Act. The court also ruled that DSW had no duty to disclose its data security practices, and thus a deception or implied contract claim based upon an omission could not go forward.

The complaint in *Key v. DSW* alleged six counts of wrongdoing, including negligence, breach of implied contract, breach of a third party beneficiary contract, breach of fiduciary duty, an Ohio

56

57

58

consumer protection statute, and conversion.[59] The first count which arose under the Ohio Sales Practices Act alleged DSW's failure to provide data security was unfair and deceptive. The claims essentially relied on the FTC's complaint and consent decree with DSW. The second count was negligence, alleging that DSW breached its duty of care to the plaintiffs by failing to provide a high degree of care for the sensitive information. The third count was for the breach for an implied term of reasonable data security. The fourth count was for conversion, arguing that DSW retaining and storing information longer than necessary was outside of the consent of the consumer class. The fifth count was for breach of fiduciary duty on the grounds that DSW owed such a duty because of the sensitive nature of the information given to them by consumers with the expectation of data security. The sixth count was for breach of a third-party beneficiary contract based on contracts with the major credit card companies which establish certain data security requirements that DSW allegedly failed to provide.

In *Key v. DSW*, the Federal District Court for Southern Ohio dismissed the case because the plaintiffs failed to allege an injury for standing purposes.[60] The only injury alleged was an increased risk of identity theft due to the data breach. Because there was only a speculative injury which was no imminent or actual, the court dismissed all of the allegations by Key on behalf of the class of consumers.

Again, despite the fact that there was no litigation on the merits, law was still created through these cases. DSW did not settle with the plaintiffs because plaintiffs did not allege a cognizable injury.

The FTC's Complaint and Settlement with DSW

Unlike the other cases discussed thus far, the FTC's complaint and settlement with DSW preceded the private actions started against them. Both of the complaints canvassed referred to the FTC's complaint. The FTC complaint itself was the usual 3 pages. The FTC complaint alleged DSW committed an unfair act or practice for 5 reasons. DSW:

1. created unnecessary risks to the information by storing it in multiple files when it no longer had a business need to keep the information;
2. did not use readily available security measures to limit access to its computer networks through wireless access points on the networks;
3. stored the information in unencrypted files that could be accessed easily by using a commonly known user ID and password;
4. did not limit sufficiently the ability of computers on one in-store network to connect to computers on other in-store and corporate networks; and
5. failed to employ sufficient measures to detect unauthorized access.[61]

The FTC did also connect the unfair acts to the actual breach when it said: "As a result, a hacker could use the wireless access points on one in-store computer network to connect to, and access personal information on, the other in-store and corporate networks."[62]

59

60

61

The FTC failed to allege any facts on countervailing benefits or reasonable avoidability, but it did allege facts on substantial injury, stating

> To date, there have been fraudulent charges on some of these accounts. Further, some customers whose checking account information was compromised were advised to close their accounts, thereby losing access to those accounts, and have incurred out-of-pocket expenses such as the cost of ordering new checks. Some of these checking account customers have contacted DSW requesting reimbursement for their out-of-pocket expenses, and DSW has provided some amount of reimbursement to these customers.[63]

This is the first case in which it is certain that the FTC's complaint and settlement drove private actions, both of which were dismissed. A strong argument can be made that the FTC fulfilled its gap-filling role in this case. The question remains, however, of whether it is a feature or a bug that private actions require an actual injury. The FTC may have been able to leverage its complaint and uncertain legal standards into a consent decree when private defendants could not because of the lack of judicial review. In light of DSW's consumers being reimbursed and the main harm being speculative future injuries, it is uncertain what harm the FTC could assert in a court of law.

In Re BJ's Wholesale Club

BJ's Wholesale Club, the operator of over 150 warehouses, or stores, in the eastern United States, uses its computer network to request and obtain authorization from the bank that issued the card for credit card and debit card purchases at its stores. To obtain authorization, BJ's collects information from the customer, including customer name, card number and expiration date, and certain other information. Hackers gained access to BJ's computer network and compromised personal information of its customers. This led to a private action by Sovereign Bank, an issuer of credit cards on the Visa network, and an FTC investigation that ended in a complaint and consent decree.

Sovereign Bank v. BJ's Wholesale Club, Inc.

Sovereign asserted three counts against BJ's Wholesale in its relatively short 12-page complaint: negligence, breach of fiduciary duty, and promissory estoppel.[64] The November 7, 2005 complaint lacked some of the specificity seen in other private complaints. For instance, it did not allege how the third parties came into possession of the private information.

The count of negligence was the most generally pleaded so far, simply stating:

> BJ's had a duty to exercise reasonable care in deleting or erasing Cardholder Information after a transaction had been approved and/or safeguard such information so long as BJ's retained the information to prevent the unauthorized possession and/or misuse of the information… B's retained the Cardholder Information after a transaction had been approved and/or failed to properly safeguard the information to prevent the unauthorized possession and/or misuse of

---

62

63

64

> such… By failing to delete, erase, and/or properly safeguard the Cardholder Information after a transaction had been approved, BJ's failed to exercise reasonable care… BJ's breached its duty to exercise reasonable care as aforesaid.[65]

Unlike in previous cases examined, Sovereign did not connect BJ's duty to industry standards.

The count of breach of fiduciary duty did, however, rely on Visa's Operating Regulations. Sovereign alleged there was a fiduciary relationship present created when Sovereign released its consumers information to BJ's to authorize customer purchases. According to the complaint, these Regulations meant BJ's could not retain and store cardholder information.

Relatedly, Sovereign alleged in the third count that BJ's promise to be bound by the Operating Regulations of Visa created an estoppel situation. Sovereign alleges that BJ's breach of this promise was to the detriment of Sovereign, who had relied upon it.

There are two other counts in the complaint against Fifth-Third Bank, who processed the payments. The claims were breach of contract and promissory estoppel, also based upon the Operating Regulations.

The harm for all of the counts was that BJ's retention and storage of the data allowed thieves to gain access to the information and engage in fraudulent transactions. Sovereign then had to reimburse consumers for the fraudulent charges and issue new cards to them, costing them substantial sums of money.

After the case was transferred to the Middle District of Pennsylvania, the negligence, breach of fiduciary duty, and promissory estoppel claims were dismissed, but the breach of contract claim against Fifth-Third Bank remained. On appeal to the Third Circuit Court of Appeals, the claims against BJ's Wholesale were reconsidered.[66] The Third Circuit opinion was filed on December 12, 2011 after years of litigation. The Third Circuit described the promissory estoppel claim as equitable indemnification and affirmed its dismissal. The more interesting discussion comes in the negligence section, where the economic loss doctrine is expounded and applied. Despite the court stating the losses were foreseeable results of the breach of duty, the economic loss doctrine still prevented recovery. The court also considered negligent misrepresentation, and said that while this is an exception to the economic loss doctrine, it does not apply in this case because the commercial plaintiffs did not rely on an expert supplier of information to their detriment.

With the claims against BJ's Wholesale dismissed, there was no settlement. The Third Circuit's discussion of negligent misrepresentation and the contract remedies were later cited by the First Circuit in *In Re TJX*. Important legal precedent was created that later helped hold businesses liable for bad data security, even though BJ's itself was not held liable.

The FTC's Complaint and Settlement with BJ's Wholesale

---

[65]

[66] Sovereign Bank v. BJ'S Wholesale Club, Inc., 533 F.3d 162 (3rd Cir. 2008).

[66]

On September 20, 2005, while the litigation against BJ's was still in full swing, the FTC issued it short 3-page complaint against the company along with a consent decree. The complaint alleged that BJ's Wholesale was engaged in unfair practices for 5 reasons. BJ's:

1. did not encrypt the information while in transit or when stored on the in-store computer networks;
2. stored the information in files that could be accessed anonymously -- that is, using a commonly known default user id and password;
3. did not use readily available security measures to limit access to its computer networks through wireless access points on the networks;
4. failed to employ sufficient measures to detect unauthorized access or conduct security investigations; and
5. created unnecessary risks to the information by storing it for up to 30 days when it no longer had a business need to keep the information, and in violation of bank rules. As a result, a hacker could have used the wireless access points on an in-store computer network to connect to the network and, without authorization, access personal information on the network.[67]

In other words, the FTC relied upon a negligence theory for unfairness that was rejected by the courts in *Sovereign*. The FTC did not allege any facts on countervailing benefits or reasonable avoidability. The FTC did allege facts on substantial injury, noting the millions of dollars in fraudulent purchases and the necessity of cancelling and issuing new credit cards, but it did not mention that consumers were reimbursed. The FTC also did not separate the injury to issuing banks like Sovereign or to credit card companies like Visa from injuries to consumers.

In light of how the economic loss doctrine bars so many negligence actions for poor data security like in *Sovereign*, one could argue that the FTC's action against BJ's was necessary to fill the gaps and promote better incentives. This would be a decent case for that proposition, but only if you assume BJ's poor data security was to blame for the breach. Neither complaint clearly stated how the credit card information ended up in the hands of third parties who engaged in fraudulent transactions. It seems likely that hackers took advantage of BJ's poor data security, but both cases essentially operate on a theory of *res ipsa loquitur* with no factual explanation of how the hackers gained access to the sensitive information. Tellingly, the FTC was able to leverage its complaint into a consent decree on basically the same theory that failed in *Sovereign*. The long litigation period and even some discovery done in *Sovereign* without settlement shows that those costs do not always lead to settlement in private actions. It is difficult to determine if it was the costs of the FTC's investigation or some other factor that led BJ's to agree to a consent decree.

FTC v. Wyndham

It takes little more than a quick glance to see how different the FTC's complaint in *Wyndham* it is than previous FTC complaints. This may be because the FTC was not able to get Wyndham to agree to a consent decree and decided to bring the case in a court of law. The complaint is

---

67

much more detailed and comes in at 22 pages, rather than the usual 3. Even so, the FTC's complaint still fails to allege any facts on countervailing benefits or reasonable avoidability.

The FTC does do a considerably better job of alleging substantial injury in this case, but even here it is not perfect. The FTC alleged both unfair and deceptive practices by Wyndham. The deception is based on two promises. Wyndham promised to provide firewalls, which the FTC alleges it failed to provide. Wyndham also promised commercially reasonable data security, which the FTC also alleges it failed to provide, as the basis for both the deception and unfairness claims. The reasons the FTC alleges Wyndham's data security was unreasonable are that Wyndham:

> a. failed to use readily available security measures to limit access between and among the Wyndham-branded hotels' property management systems, the Hotels and Resorts' corporate network, and the Internet, such as by employing firewalls;
>
> b. allowed software at the Wyndham-branded hotels to be configured inappropriately, resulting in the storage of payment card information in clear readable text;
>
> c. failed to ensure the Wyndham-branded hotels implemented adequate information security policies and procedures prior to connecting their local computer networks to Hotels and Resorts' computer network;
>
> d. failed to remedy known security vulnerabilities on Wyndham-branded hotels' servers that were connected to Hotels and Resorts' computer network, thereby putting personal information held by Defendants and other Wyndham-branded hotels at risk. For example, Defendants permitted Wyndham-branded hotels to connect insecure servers to the Hotels and Resorts' network, including servers using outdated operating systems that could not receive security updates or patches to address known security vulnerabilities;
>
> e. allowed servers to connect to Hotels and Resorts' network, despite the fact that well-known default user IDs and passwords were enabled on the servers, which were easily available to hackers through simple Internet searches;
>
> f. failed to employ commonly-used methods to require user IDs and passwords that are difficult for hackers to guess. Defendants did not require the use of complex passwords for access to the Wyndham-branded hotels' property management systems and allowed the use of easily guessed passwords. For example, to allow remote access to a hotel's property management system, which was developed by
>
> software developer Micros Systems, Inc., Defendants used the phrase "micros" as both the user ID and the password;
>
> g. failed to adequately inventory computers connected to the Hotels and Resorts' network so that Defendants could appropriately manage the devices on its network;

> h. failed to employ reasonable measures to detect and prevent unauthorized access to Defendants' computer network or to conduct security investigations;
>
> i. failed to follow proper incident response procedures, including failing to monitor Hotels and Resorts' computer network for malware used in a previous intrusion; and
>
> j. failed to adequately restrict third-party vendors' access to Hotels and Resorts' network and the Wyndham-branded hotels' property management systems, such as by restricting connections to specified IP addresses or granting temporary, limited access, as necessary.[68]

The FTC also described in considerable detail how the three different breaches into Wyndham's networks by hackers led to the compromised data.

The FTC took the time to allege substantial injury in detail, as well, describing it as:

> [T]he compromise of more than 619,000 consumer payment card account numbers, the exportation of many of those account numbers to a domain registered in Russia, fraudulent charges on many consumers' accounts, and more than $10.6 million in fraud loss. Consumers and businesses suffered financial injury, including, but not limited to, unreimbursed fraudulent charges, increased costs, and lost access to funds or credit. Consumers and businesses also expended time and money resolving fraudulent charges and mitigating subsequent harm.[69]

Though some of these may not count as cognizable injury under some of the private causes of action, the FTC survived a Twombly-style motion to dismiss in Wyndham.[70]

On the question of fair notice, the court held that the FTC's interpretations of the FTC Act "while not controlling upon the courts by reason of their authority, do constitute a body of experience and informed judgment to which courts and litigants may properly resort for guidance."[71]

Interestingly, in quoting *General Electric Co. v. Gilbert*, Judge Salas omitted the very next sentence which stated "[t]he weight of such a judgment in a particular case will depend upon the thoroughness evident in its consideration, the validity of its reasoning, its consistency with earlier and later pronouncements, and all those factors which give it power to persuade, if lacking power to control."[72] The court seemed to suggest that the complaints and consent decrees described above attain to those qualities.

On the contrary, most of the complaints we looked at from the FTC would not likely be able to survive a motion to dismiss, even though they had already had substantial opportunities for

---

[68]

[69]

[70] FTC v. Wyndham, no. 13-1887 (D.N.J. Apr. 4, 2014), *available at* http://ashkansoltani.files.wordpress.com/2014/04/ftc-v-wyndham-opinion.pdf.

[71] *Id.* at 24 (quoting Gen. Elec. Co. v. Gilbert, 429 U.S. 125, 141-42 (1976)).

[72] Gilbert, 429 U.S. at 142.

"discovery" before bringing the complaints. While the FTC's complaint in *Wyndham* survived a motion to dismiss, it is still unlikely to be strong enough to win on summary judgment without more development of the facts and better application of the facts to the law, *despite the fact* that the FTC already investigated Wyndham pursuant to its investigative powers. If the FTC's complaints and consent decrees are supposed to act as common law sufficient to give notice of Section 5's demands to plaintiffs, much more should be said than what has been presented about applying the law to the facts. Even the FTC's considerably better complaint in *Wyndham* would give businesses little to work with aside from a list of practices that the FTC does not think sufficient to count as "reasonable" data security.

Conclusion