

PrivacyTRACKER

iapp

A publication of the International Association of Privacy Professionals

Competitive Privacy: Towards A New Area of Privacy Litigation?

Edward McNicholas and Jennifer Tattel



An apparent afterthought in a patent case may point the way to a new type of privacy litigation, and it may offer the potential for companies to shape robust privacy practices into an offensive tool for litigation against their competitors. At the very least, the case suggests a new way for businesses to litigate over their competitors' consumer privacy practices.

In *CollegeNET, Inc. v. XAP Corp.*,¹ a federal district court relied on the

Lanham Act to enjoin an online software provider from engaging in misleading privacy practices. As is common with innovations in the law, the decision betrays little awareness that it was a signal of something potentially of very broad interest. The significance of this decision is that it suggests a way to address some of the central tensions in privacy litigation—the absence of clear damages, the consequential dearth of motivated and aggressive private enforcers, and a resulting volume of cases that is inadequate to generate defined norms for companies to rely on when setting policy.

Until now, the vast majority of private lawsuits relating to privacy have resulted from data breaches in which large amounts of consumer data were lost or stolen. In most of these cases, however, there is little or no evidence of actual injury, and as a result of the speculative nature of the damages, these cases have been routinely dismissed for lack of standing or for failure to state a claim. The absence of reliably measurable damages in turn has made this area of litigation less attractive to the plaintiff's mass tort class action bar. Industry thus has been forced to rely upon regulatory guidance and the relatively small number of cases against unfair or deceptive trade practices brought by the Federal Trade Commission (FTC) as the foundation for specific standards

See Competitive Privacy, page 3

In This Issue

Competitive Privacy: Towards A New Area of Privacy Litigation? 1

Letter from the Editor 2

Legislative Action 10

Credit Agencies & ID Theft 10

Data Security & Breach 11

Government Records, SSN & Identification 12

Internet 13

Marketing 13

Children & Education 14

Financial, Insurance & Mortgages 14

Employment 15

Medical 16

Telecommunications & RFID 18

Miscellaneous 18

Monthly Call Summary 19

Session Calendar 2008 20

¹*CollegeNET, Inc. v. XAP Corp.*, 2008 WL 1805539, No. 03-CV-1229-BR (D. Or. Apr. 17, 2008).

Competitive Privacy

of reasonableness in privacy practices.²

A suit by a competitor claiming to have been harmed by a rival company's privacy practices may avoid these issues, and thereby increase the potential stakes associated with violations of privacy policies and data breaches. Unlike the majority of data breach cases brought thus far, competitors will not assert vague notions of dignitary harm. Rather, they will have economic experts who are able to prove traditional models of business harm that could well survive judicial scrutiny. As a result of this new possibility of "competitor enforcement," any doubts about the incentives presented to address corporate privacy and data protection compliance may vanish, and a series of new, high-stakes lawsuits may emerge, particularly for companies whose business models depend on the rapid deployment of new uses of information technologies.

In light of this potential, companies are especially well advised to review whether their consumer-oriented privacy policies communicate effectively, that is, whether measuring the reaction of the target audience to the policies would demonstrate that they understand the claims being made.³ In addition, companies should consider whether their policies are sufficiently conspicuous and would survive competitor claims of being "false or misleading," defined in the Lanham Act to include material misrepresentations of actual facts.⁴ Significantly, this review is both defensive and offensive. Companies with sound practices and policies will have every incentive to use privacy violations as a means to police against less reputable competitors who are using slick privacy practices to undercut market competition.

Of course, the CollegeNET decision itself does not dictate these results, and the implications and possibilities of competitive litigation exist regardless of the specific result in the CollegeNET case. The decision, however, does provide a useful prism through which to view this potential new type of privacy litigation. Most significantly, CollegeNET indicates that the question of proper privacy norms may be solved in a traditional American way—by enlisting self-interested litigation in the service of the common good—so that commercial enterprises can become a primary

continued from page 1

enforcer of ever evolving reasonable privacy practices.

CollegeNET's Lanham Act Claim

The CollegeNET case began as a patent infringement dispute between competing providers of online college application processing software. The initial complaint in the action did not even mention the Lanham Act or the privacy policies. Plaintiff CollegeNET subsequently added a Lanham Act unfair competition claim to its suit against defendant XAP, alleging that XAP used misleading privacy statements to profit unfairly from the sale of college applicants' personal data. The result was an order of the U.S. District Court for the District of Oregon assessing \$4.5 million in damages after determining that privacy misrepresentations can amount to unfair competition. This novel use of the Lanham Act may increase companies' exposure to litigation in the event of privacy-related misrepresentations, leaving them vulnerable to suits by harmed competitors, which, in turn, could lead to injunctive measures and potentially large damage awards.

According to the opinion, Plaintiff CollegeNET earned revenue by selling its online college application software and services directly to colleges and universities. Defendant XAP did not charge colleges or universities for its services, but instead earned profits from third-party institutions, including commercial entities such as banks and other lending authorities. The Web sites operated by XAP, which allowed students to submit college applications online, contained assurances that students' personal information would not be released to third parties without the students' express consent. Specifically, the Web sites included an "account set-up screen" containing the statement: "The information you enter will be kept private in accordance with your express consent and direction." At least at the time when the litigation was initiated, XAP had a policy to deem that students had provided such "express consent and direction" if they checked the "Yes" box when asked whether they wished to receive information about student loans or financial aid. XAP's treatment of affirmative replies to this question as an "opt-in" response was key because then, without (further) expressly advising students that it

² See, e.g., *Guidance Software, Inc.*, FTC File No. 062-3057 (Nov. 11, 2006); *BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (June 16, 2005).

³ See, e.g., *Johnson & Johnson-Merck Consumer Pharmaceuticals Co. v. Rhone-Poulenc Rorer Pharmaceuticals, Inc.*, 19 F.3d 125 (3d Cir. 1994) (considering, *inter alia*, surveys of consumer to ascertain whether consumers understood the advertisers' claims).

⁴ *Id.* § 1125.

would do so, XAP allegedly sold these students' personal information to third-party institutions for a fee. CollegeNET charged that this practice constituted a false representation that amounted to unfair competition under the Lanham Act. In essence, the XAP privacy practice allowed for free the exact same services that CollegeNet was attempting to sell, thereby harming CollegeNet's business.

Although CollegeNet initially relied on the patent laws (and continues to do so) as the main thrust of its suit, it also added a claim under the federal Lanham Act, which, generally speaking, prohibits the use of false or misleading statements or representations that are likely to confuse or deceive consumers with respect to commercial goods or services.⁵ The Act authorizes awards of treble damages and disgorgement of the defendant's profits for unfair competition.⁶

During a 2006 trial on CollegeNET's claims, a jury was asked to determine whether XAP's privacy practices amounted to unfair competition under the Lanham Act. The jury answered this question in the affirmative, and assessed \$4.5 million in actual damages against XAP. In reviewing the jury's damage award, the court found "clear and convincing" evidence that XAP failed to inform student applicants that a "Yes" response to the financial aid question would be treated as express consent to the disclosure and sale of their personal data to third parties. The court emphasized that XAP could have used language to clarify the consequences of checking the "Yes" box, and that XAP chose not to do so in order to increase its revenue from the sale of student data. The court concluded "that XAP intended its privacy-policy statements to lull students into a false sense of security regarding the privacy of the[ir] personal information."⁷ These deceptive practices gave XAP an unfair competitive advantage over CollegeNET, as the sale of students' data allowed XAP to provide its services to colleges and universities for free. The court ultimately determined that the jury's award of \$4.5 million in actual damages afforded fair and reasonable compensation to CollegeNET. In light of the fact that XAP's deception was found to be willful, the court also awarded attorneys' fees to CollegeNET.

Subsequent to the court's decision awarding damages to

CollegeNET, CollegeNET filed a motion to enjoin XAP permanently from continuing its alleged deceptive practices. In this motion, CollegeNET contended that XAP had persisted in its failure to disclose clearly to students that checking the "Yes" box would constitute consent to the sale of their personal data. CollegeNET argued that any changes that XAP had made were inadequate, as XAP's privacy policy disclosure statement was vague and buried within extensive marketing statements, failed to identify the type of information subject to disclosure, and did not expressly notify students at the time of opt-in that personal information would be disclosed to third parties. The court agreed.

In weighing the factors relevant to granting injunctive relief, the court concluded that it would not be "an undue hardship to require Defendant to revise its online application system by including language that makes clear to students that a "Yes" answer to the opt-in question will result in the disclosure of their personal information to third parties."⁸ Moreover, it would serve the public interest to make students "aware unequivocally of the consequences of checking the 'Yes' box . . . by conspicuous language at the point where the opt-in question appears."⁹ The court accordingly issued a permanent injunction that required XAP "to inform student applicants in plain, concise, and conspicuous language set forth immediately preceding the opt-in question that by answering 'Yes' to that question the applicant understands he or she specifically is authorizing Defendant to disclose . . . personal information" to third parties.¹⁰ This plain language must describe the personal information to be disclosed, list the third parties that will receive the information, and state the purposes for which applicants are being asked to submit their information. At present, no appeal has been noted, and the case continues with regard to the patent claims.

The Unexpected Significance of CollegeNET

One could easily dismiss the CollegeNET decision as an interesting case about opt-in requirements, but CollegeNET may indicate a solution to some of the central problems of defenses to privacy litigation (depending on the perspective). Suits by competitors have a clearly identifiable and motivated enforcer, who has a reasonable expectation of demonstrable

⁵ 15 U.S.C. § 1125(a).

⁶ *Id.* § 1117(a).

⁷ *CollegeNET, Inc. v. XAP Corp.*, No. 03-CV-1229-BR, slip op. at 19 (D. Or. Mar. 26, 2007).

⁸ *CollegeNET, Inc. v. XAP Corp.*, 2008 WL 1805539, No. 03-CV-1229-BR, slip op. at 11 (D. Or. Apr. 17, 2008).

⁹ *Id.*

¹⁰ *Id.* at 12.

damages if they are correct in their claims. Moreover, such litigation is not limited to catastrophic breach issues, but could be targeted on compliance with specific statutory mandates, in much the same way as the recent spate of litigation over companies that printed the expiration date and the last several digits of a credit card on a receipt. Unlike the credit card receipt litigation, however, competitive privacy litigation could emerge along a path that is analogous to the constant litigation between telecommunications companies over various advertising claims.

The effects of this development may be most profound in two areas: the significance of being able to prove damages, and the scope and nature of enforcement. First, for background, we examine the significant difficulties in proving damages that have resulted in many suits being dismissed until now, and the reasons that competitor suits should not suffer from this problem. Second, we discuss the potential changes in the scope, manner, and vigor of enforcement that could result if such competitor suits become widespread.

The Damages Problem of Privacy Litigation

The lack of a coherent theory of damages has bedeviled privacy litigants for the last decade. Repeatedly, in the absence of actual identity theft, courts have refused to recognize harms from privacy violations as being adequate to support causes of action.

Conboy v. AT&T Corp.,¹¹ is emblematic of such cases. In their complaint, the Conboys alleged violations of a number of privacy and consumer protection laws, including the customer proprietary network information (CPNI) provisions of the Telecommunications Act.¹² The Conboys claimed that AT&T had illegally disclosed their unlisted contact information to AT&T's affiliate, Universal Card Service, for debt collection purposes and that they were eligible for damages. The court avoided deciding whether the disclosed information constituted CPNI and instead ruled that the plaintiffs failed to allege recoverable damages. In

Conboy, the Second Circuit Court of Appeals thus held that such a transfer of personal information does not necessarily in itself cause injury or give rise to cognizable damages. The court entertained no presumption of emotional distress or other similar damages from the disclosure of personally identifiable information, absent some concrete evidence of demonstrable harm. AT&T therefore prevailed over plaintiffs for claims of improper distribution of CPNI to AT&T's former credit card branch.

Cases involving data breaches have encountered similar damages problems, and numerous federal courts that have addressed this issue have held that the mere risk of harm due to loss of personal information is not actionable injury sufficient to confer standing.¹³ Other "lost data" cases decided at the summary judgment stage similarly support the prevailing concept that the mere risk of identity theft as a result of lost or stolen data is not a recognized "injury."¹⁴

Typical of such litigation is *Randolph v. ING Life Insurance & Annuity Co.*,¹⁵ in which the District Court for the District of Columbia rejected an argument based on speculative harms as insufficient to confer standing. There, a laptop containing personal information, including Social Security numbers, of 13,000 current and former District of Columbia government employees was stolen from an employee of the defendant insurance company. The court noted that the plaintiffs offered no evidence that the laptop was stolen for purposes of accessing the personal information thereon, or that any of the plaintiffs' personal information was actually accessed and misused.¹⁶ Indeed, the court held that plaintiffs "fail... to allege any injury that is 'actual or imminent, not conjectural or hypothetical.'"¹⁷ Furthermore, the court found that plaintiffs' claims of injury based on time and money spent monitoring their credit "was not the result of any present injury, but rather the anticipation of future injury that has not materialized."¹⁸ This was also held to be insufficiently "concrete and particularized, actual or imminent" to confer standing.¹⁹

¹¹ *Conboy v. AT&T Corp.*, 241 F.3d 242 (2d Cir. 2001).

¹² 47 U.S.C. § 222.

¹³ See, e.g., *Randolph v. ING Life Insurance & Annuity Co.*, 486 F.Supp.2d 1 (D.D.C. 2007); *Bell v. Axiom Corp.*, No. 06-485, 2006 WL 2850042 (E.D. Ark. Oct. 3, 2006); *Key v. DSW Inc.*, 454 F. Supp. 2d 684 (S.D. Ohio 2006); *Giordano v. Wachovia Sec., LLC*, No. 06-476, 2006 WL 2177036 (D.N.J. July 31, 2006).

¹⁴ See, e.g., *Stollenwerk v. Tri-West Healthcare Alliance*, No. 03-0185RHXS RB, 2005 WL 2465906 (D. Ariz. Sept. 6, 2005); *Guin v. Brazos Higher Ed. Serv. Corp.*, No. 05-668, 2006 WL 288483 (D. Minn. Feb. 7, 2006); *Forbes v. Wells Fargo Bank, N.A.*, 420 F. Supp. 2d 1018 (D. Minn. 2006).

¹⁵ *Randolph v. ING Life Insurance & Annuity Co.*, 486 F.Supp.2d 1, (D.D.C. 2007).

¹⁶ *Id.* at 7.

¹⁷ *Id.*

¹⁸ *Id.* at 8.

¹⁹ *Id.*

Randolph itself relied on the numerous cases that preceded it in which federal courts had found any alleged “risk of harm” associated with lost personal data is not a legally recognized injury. For example, in *Giordano v. Wachovia Sec., LLC*,²⁰ the court held that plaintiffs lacked standing to raise claims arising out of the loss of a report containing the personal information of bank customers. The court considered Giordano’s negligence and invasion of privacy claims, and concluded that she “lack[ed] Constitutional standing” because she “failed to allege that she suffered an injury-in-fact that was either ‘actual or imminent.’”²¹ In particular, the court found that allegations that Giordano “will incur costs associated with obtaining credit monitoring services” were insufficient, because they did “not rise to the level of creating a concrete and particularized injury.”²² In addition, the alleged injury relied on two hypothetical contingencies—the personal information “falling into the hands of an unauthorized person” and that person’s use of such information “for unlawful purposes to Giordano’s detriment.”²³ These contingencies rendered the threatened risk of future harm insufficient to confer standing.

Similarly, in *Key v. DSW Inc.*,²⁴ unauthorized persons accessed personal information maintained by defendant retailer for 96,000 customers. Although plaintiff alleged that she had been subjected to heightened risk of identity theft, the court noted that plaintiff had not demonstrated that the third-party wrongdoers intended to make use of her personal information, and if they did, the scope of the harm suffered was entirely unknown to the court.²⁵ Thus, the court found that “when the alleged injury is dependent upon the perceived risk of future actions of third parties not before the Court,” the injury is too attenuated and speculative to be sufficient for standing under Article III.²⁶

Demonstrable Damages

The CollegeNET case has potential to address the issue of damages because it does not require notions of dignitary

harm or harms from increased fear, increased risk, or increased risk of fear. Instead, competitive privacy litigation would involve traditional methods of proving harm from competitor’s inappropriate business practices. Such damages are often the subject of competing damages studies regarding market share, proximate causation, profit levels, etc., but profits are, at the end of the day, often demonstrable.

The idea that the damages issue would be solved was certainly in the air before CollegeNET, and some other recent case law was already beginning to suggest that a different theory of damages would emerge for privacy harms. In retrospect, it seems odd that this issue has been such a fearsome bar given that harms for privacy violations have always been subject to damages remedies. Even in Warren & Brandeis’ seminal article on the subject, there was the express observation that

[t]he remedies for an invasion of the right of privacy are also suggested by those administered in the law of defamation, and in the law of literary and artistic property, namely: 1. An action of tort for damages in all cases. Even in the absence of special damages, substantial compensation could be allowed for injury to feelings as in the action of slander and libel. 2. An injunction, in perhaps a very limited class of cases.²⁷

The upshot is that the availability of a remedy for harms to privacy has had readily apparent models in the literary and artistic areas where people have been competing over ephemeral but highly valuable information and ideas from time immemorial. Indeed, the concept of “substantial compensation . . . allowed for injury to feelings” in the sort of amorphous, emotional harm sought in many data breach actions.

Consistent with this common law approach, some courts have recognized that the harms of misappropriation of personal information are not necessarily contingent upon certain consequences, so that the breach of privacy itself can be considered a harm worthy of compensation in certain circumstances.²⁸ As the New Hampshire Supreme

²⁰ *Giordano v. Wachovia Sec., LLC*, No. 06-476, 2006 WL 2177036 (D.N.J. July 31, 2006).

²¹ *Id.* at *4.

²² *Id.*

²³ *Id.* at *5.

²⁴ *Key v. DSW Inc.*, 454 F. Supp. 2d 684 (S.D. Ohio 2006).

²⁵ *Id.* at 690.

²⁶ *Id.* at 689.

²⁷ Samuel D. Warren & Louis D. Brandeis, “The Right to Privacy,” 4 *Harv. L. Rev.* 193, 219 (1890) (footnote omitted) (emphasis added).

²⁸ See *Randi A.J. v. Long Island Surgi-Center*, 842 N.Y.S.2d 558, 566-67 (N.Y. App. Div. 2007) (holding that a medical center’s releasing confidential information regarding an abortion to a patient’s mother after the patient specifically requested not to be contacted at home supports a punitive damages award).

Court similarly recognized, the long-standing common law privacy torts do not require evidence of harm beyond the bare invasion of privacy itself.²⁹ Likewise, deception is not a necessary element of the common law privacy torts.³⁰ For instance, an “action for intrusion upon seclusion does not require a claimant to prove any harm beyond the intrusion itself.”³¹ Moreover, the harms experienced by violations of privacy have only increased with the advent of new forms of identity theft harm unknown at common law.³²

Just last year, the first federal appellate court decision in a data breach case also left open the possibility that courts would be amenable to such theories of damages. In *Pisciotta v. Old Nat'l Bancorp*,³³ the court dismissed a purported class action that alleged failure to protect personal information on the bank's marketing Web site. In *Pisciotta*, the bank's Web site allowed potential customers to complete online applications for accounts, loans, and other Old National Bancorp (ONB) banking services. Some of these applications required the customer to submit personal information, which was stored on ONB's Web site and was maintained by NCR, a hosting facility, which experienced a “sophisticated, intentional, and malicious” security breach in 2005. ONB sent written notice of the breach to its customers, two of whom subsequently sued the bank for negligence and breach of contract.

The significance of the *Pisciotta* decision, in addition to its being the first appellate court decision on the issue, is that the Court disagreed with several district courts and considered the fear of future identity theft to be adequate to establish an injury-in-fact for purposes of Article III standing. That is, *Pisciotta* found that the mere fear of future identity theft may be adequate to establish a legally-cognizable injury, despite noting that this conclusion was in conflict with the “no standing” decisions of a number of district courts, including *Randolph v. ING Life Ins. & Annuity Co.*³⁴ and *Bell v. Axiom Corp.*,³⁵ where purported class actions had been dismissed for failure to demonstrate sufficient injury for Article III standing.

Pisciotta, however, was a mixed blessing for plaintiffs because it also emphasized that one of the required elements of the relevant tort was “a compensable injury proximately caused by defendant's breach of duty.” The threshold question, therefore, shifted to whether state law “would consider that the harm caused by identity information exposure, coupled with the attendant costs to guard against identity theft, constitutes an existing compensable injury and consequent damages required to state a claim for negligence or for breach of contract.” Finding no statute or case law precedent to support a cause of action for such alleged injuries, the court reviewed the state data breach notification statute and held that the state would not consider monitoring expenses to constitute a compensable injury.

Although *Pisciotta* thus ultimately dismissed the idea of a claim based on merely “prospective harm,” *Pisciotta*, like *CollegeNET*, indicated that the damages issue will not enjoy such prominence in privacy litigation as it has. Indeed, in one of the most recent decisions on the subject, *Ruiz v. Gap, Inc.*,³⁶ a federal district court in California held that a mere increased risk of identity theft as a result of a security breach, without any allegation of actual or imminent harm, is sufficient to confer preliminary standing on a plaintiff. While acknowledging that plaintiff's claim of that increased risk for identity theft at some unspecified future point “seem[ed], at first blush, conjectural or hypothetical, rather than actual or imminent,” the court nonetheless felt bound to “presume ‘that general allegations embrace those specific facts that are necessary to support the claim.’”³⁷ The court therefore concluded that, for purposes of a motion for judgment on the pleadings, *Ruiz* possessed sufficient standing to pursue his claims.

The resolution of the damages issue via the *Pisciotta* line of cases—regardless of whether it is ultimately a minority or majority result—will continue to be independent of the potential for a competitor suit to rest on much more traditional, supportable damages theories.

²⁹ *Preferred Nat'l Ins. Co. v. Docusearch, Inc.*, 149 N.H. 759, 766-767, 829 A.2d 1068, 1075 (2003).

³⁰ *Restatement (Second) of Torts* § 652H.

³¹ *Docusearch*, 829 A.2d at 1075 (citing *Restatement (Second) of Torts* § 652H cmt. a at 402 (1977) (“[O]ne who suffers an intrusion upon his solitude or seclusion . . . may recover damages for the deprivation of his seclusion.”)).

³² See Federal Trade Commission, 2006 Identity Theft Survey Report, available at <http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf>.

³³ *Pisciotta v. Old Nat'l Bancorp*, Case No. 06-3817 (7th Cir. Aug. 23, 2007).

³⁴ *Randolph v. ING Life Ins. & Annuity Co.*, 486 F. Supp. 2d 1 (D.D.C. 2007).

³⁵ *Bell v. Axiom Corp.*, 2006 WL 2850042 (E.D. Ark. Oct. 3, 2006).

³⁶ *Ruiz v. Gap, Inc.*, No. 07-5739 (N.D. Cal. Mar. 24, 2008).

³⁷ *Id.* at 6 (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992)).

Competitive Privacy Litigation May Be Much More Aggressive And Pervasive Than Federal Trade Commission And Other Regulatory Actions

The presence of a supportable damages theory may well be all the more significant because commercial competitors are more numerous, more self-interested, and perhaps even more aggressive than federal regulators have been to date. Competitor cases such as *CollegeNET* may result in further development of very specific norms regarding key privacy practices because they will depend on decentralized, market-driven enforcement that will rest upon the knowledge of the participants in any industry, as opposed to relying primarily on FTC attention. Competitor privacy suits thus would stand in the tradition of solving a social problem by relying upon free market forces and self-interested competitors to expose and end harmful practices.

Unleashed competitors generally have little interest in exercising restraint in the name of the common good, and they may drive privacy practices towards an overall higher level of compliance much faster than any regulatory agency could accomplish. Suits could include those attacking the absence of a link to a privacy policy on the homepage, whether consent is valid, the degree of detail in the privacy notice, the listing of particular examples in the privacy policy, the font size of an opposing party's privacy notice, whether important information is omitted from a privacy policy, whether and affirmative statement in a privacy policy is false or misleading, the retroactivity of changes to privacy policies, the types of disclosures that can properly be deemed "allowed by law," or the vigilance exercised over third-party vendors.

The hope for moderation would be merely that competitors may also be required to comply with such restrictions themselves. Nevertheless, incentives would also exist to attempt to foist onerous rules onto competitors, especially if those rules would not apply to the given plaintiff. Indeed, some risk would exist that an industry could tacitly collude at an unreasonably low level of privacy protection until the need to share the losses resulting from such unreasonable practices raised the level of protection.³⁸ Overall, however,

the main incentive may be to create a reward for those companies able to develop structures for the least costly methods of achieving robust privacy compliance.

The contrast with the current regulatory environment for most companies could be pronounced. Overall, to the extent that the FTC has been successful in this area, it has done so by focusing its very limited enforcement resources and personnel on a few dozen high-profile adjudications of privacy policy issues, while avowing that it is attempting to avoid undue regulation. As former FTC Chairwoman Deborah Platt Majoras expressed in remarks on May 10, 2006, "the standard is 'reasonableness,' not perfection.... [T]his is not a game of 'cybersecurity gotcha' – we are not trying to catch companies with their digital pants down; rather, we are trying to encourage companies to put their data security defenses up."³⁹ Later, on October 1, 2007, she further emphasized two key points about FTC enforcement: "First, none of the cases was a close call – in each case, vulnerabilities were multiple and systemic, and in most cases simple, low cost measures were readily available to prevent them. Second, the violation in each of the cases was not the data breach itself, but the failure to take reasonable precautions to prevent it."⁴⁰

The market, however, need not be so reasonable. With the expansion of competitor suits, the scope of privacy enforcement could expand significantly without governmental oversight or direction. The FTC jurisdiction to pursue privacy litigation is of course limited in terms of jurisdiction. Although the FTC is analogized to the U.S.'s Data Protection Authority by some, large areas of the economy that deal with the most sensitive health and financial data are out of its reach.⁴¹ Employee privacy is likewise an area that is not obviously within the FTC's jurisdiction, although there has been some suggestion that the FTC is attempting to expand its oversight into this area despite the absence of an obvious trade nexus. Moreover, the FTC often must litigate through the U.S. Department of Justice, and it cannot necessarily even bring litigation in those areas where it asserts jurisdiction.

Competitors, however, lack such jurisdiction and resources

³⁸ *Cf. T.J. Hooper*, 60 F.2d 737 (2d Cir. 1932) (holding tug owner liable for unreasonably dangerous conduct in not having a radio even though most other tugs also lacked radios).

³⁹ Remarks of Chairman Deborah Platt Majoras, "Protecting Consumer Information in the 21st Century: The FTC's Principled Approach," The Progress and Freedom Foundation, Securing the Internet Project, Internet Security Summit, Washington, D.C., May 10, 2006, available at <http://www.ftc.gov/speeches/majoras/060510ProgressFreedomFoundationRev051006.pdf>.

⁴⁰ Opening Remarks of Deborah Platt Majoras, Chairman, Federal Trade Commission, "Maintaining Momentum in the Fight Against Identity Theft," National Cyber Security Awareness Summit, Washington, D.C., October 1, 2007, available at <http://www.ftc.gov/speeches/majoras/071001ncsas.pdf>.

⁴¹ See 15 U.S.C. § 46 (limitations on FTC jurisdiction).

hurdles. The sweep of competition-driven litigation across industries could be more rapid and widespread than any particular regulatory initiative of any particular agency or group of agencies. Moreover, the Lanham Act in particular offers the potential for attorneys' fees that will incentivize reasonably meritorious litigation. The natural motivation of competitors to beggar their neighbor thus could be the engine to drive increased litigation, motivated, at least in part, by the potential for attorneys' fees.

Private parties would be perhaps somewhat less vulnerable to the First Amendment challenges brought against governmental privacy regulation because the presence of the requisite state action would be far from obvious. The state action inherent in regulatory enforcement has hindered efforts to assert privacy rights. As the U.S. Court of Appeals for the Tenth Circuit in *U.S. West, Inc. v. Federal Communications Commission* observed in rejecting a privacy regulation on constitutional grounds:

Although we may feel uncomfortable knowing that our personal information is circulating in the world, we live in an open society where information may usually pass freely. A general level of discomfort from knowing that people can readily access information about us does not necessarily rise to the level of a substantial state interest under *Central Hudson* for it is not based on an identified harm.⁴²

The absence of direct state action may lessen the significance of such constitutional norms in private party unfair trade practice litigation. This effect may not be significant, however, given that private parties can frequently raise First Amendment issues in competitor suits.

Uncertain Prospects

The potential exists for this type of competitive privacy litigation to increase the scope, speed, and specificity of privacy requirements, but there are also potential counter-trends that may result in the mass tort model of regulation by class action becoming more prevalent. The establishment of statutory damages in state data breach laws alone would fundamentally shift the enforcement field by making it much more likely that people who experience psychological discomfort after a data breach will receive some tangible form of compensation regardless of their inability to prove damages by normal evidentiary standards.

Competitive privacy litigation, however, offers the distinct advantage of drawing upon the decentralized and autonomous ideas of a vast number of attorneys outside of the FTC staff. Although the FTC makes great efforts to stay in touch with the industries it regulates, other market participants will likely receive more information, faster and more accurately regarding those privacy practices that are significant to a given business model and those that are most likely to be observed in a breach if compliance is too expensive. Some news reports have indeed already indicated that competitors of Google are formulating plans to attack Google's policies which, by the very nature of Google's technologies, frequently place Google in uncharted, and therefore vulnerable, privacy waters.⁴³ Ultimately such suits will provide much-needed guidance regarding evolving privacy norms, but they could also distract and slow the innovation that has driven Google's growth.

Competitive privacy litigation, moreover, may also be a weapon for larger companies with robust privacy practices and developed privacy programs. For these companies, competitive privacy litigation could be used in organized campaigns designed to expose questionable practices by competitors. Thus, it could be a tool to force even smaller companies to be as law-abiding and transparent in their privacy policies as the best practices in the marketplace. Such litigation would level the competitive playing field by refusing to allow competitors to undercut normal market prices by sharp practice, such as XAP was alleged to have done in the CollegeNET case.

Edward R. McNicholas is a partner in the Washington, D.C., office of the international law firm of Sidley Austin LLP. His practice focuses on representing clients in complex litigation matters involving information technology, constitutional and privacy issues. Mr. McNicholas previously served as an Associate Counsel to President Clinton. He can be reached at 202-736-8010 or emcnicholas@sidley.com

Jennifer Tatel is an associate in the Washington, D.C. office of Sidley Austin LLP. Her practice focuses on litigation and counseling clients on privacy and information law issues, particularly in the communications, media, and Internet industries. She can be reached at 202-736-8038 or jtatel@sidley.com.

⁴² *U.S. West, Inc. v. Fed. Communications Comm'n*, 182 F.3d 1224, 1235 (10th Cir. 1999).

⁴³ See, e.g., Drake Bennett, "Stopping Google: With one company now the world's chief gateway to information, some critics are hatching ways to fight its influence," *Boston Globe*, June 22, 2008; Saul Hansell, "Is Google Violating a California Privacy Law?" *New York Times BITS Blog*, May 30, 2008 <http://bits.blogs.nytimes.com/2008/05/30/is-google-violating-a-california-privacy-law>.