2006

Virtual Espionage: Spyware and the Common Law Privacy Torts

Don Corbett
North Carolina Central University (NCCU) School of Law

Follow this and additional works at: http://scholarworks.law.ubalt.edu/ublr
Part of the Computer Law Commons, and the Torts Commons

Recommended Citation
Available at: http://scholarworks.law.ubalt.edu/ublr/vol36/iss1/2

This Article is brought to you for free and open access by ScholarWorks@University of Baltimore School of Law. It has been accepted for inclusion in University of Baltimore Law Review by an authorized administrator of ScholarWorks@University of Baltimore School of Law. For more information, please contact snolan@ubalt.edu.
VIRTUAL ESPIONAGE: SPYWARE AND THE COMMON LAW PRIVACY TORTS

Don Corbett†

INTRODUCTION

Like any working mother with children, time always seemed to be an obstacle for Danielle.¹ Her schedule seemed endlessly divided between preparing presentations at work, fixing breakfast, lunch, or dinner, and running between activities for the kids. She had never been computer savvy, but by helping her children complete some homework assignments, Danielle was introduced to the wonders of the Internet. She realized she could use her home computer to pay her bills, shop, read various newspapers, and keep up with her favorite television shows more quickly and easily than ever before.

After several months of heavy Internet usage, Danielle noticed her computer was not operating as quickly as it had in the past. She also saw a large increase in the number of advertisements that appeared on her screen as she tried to either read material or pay her bills. On two occasions, when Danielle connected to the Internet, she found her home page had been changed. She thought these incidents were slightly peculiar, but paid them little attention since she did not know much about computers. The Internet still seemed like a godsend.

One day, Danielle went online to pay another bill and was shocked to see her account showing a zero balance. Since she had just gotten paid the previous week, she knew this was inaccurate. Moreover, when she looked at a more detailed version of her transactions, she noticed a number of sizable purchases charged to her account that she did not recognize. Horrified, Danielle called the bank and was notified that not only were all the purchases made in the last week, but also several even larger purchases were standing by waiting to be cleared by the bank. Danielle informed the bank that she had no idea how the purchases happened because

† Assistant Professor of Law, North Carolina Central University School of Law, Durham, North Carolina. The author would like to thank colleagues Mary Wright, David Green, and Cheryl Amana for their edits, suggestions, and support. I would also like to thank my outstanding research assistant Leah Thompson, as well as my parents, brothers, and sister for always encouraging me. Last but not least, I’d like to thank my wife Wendy, who despite her questionable taste in men, showed me once again through her suggestions for the article that she is far brighter than I.

¹ While Danielle is a fictional character, the idea for her presence was influenced by Spyware Center Spyware Horror Stories: The Pitfalls of Pornography, http://www.download.com/1200-2023-5139045.html (last visited Dec. 30, 2006).
no other person possessed her account information and she had never made them. When she told bank representatives about her online activity, they informed her that due to possible infiltration of her computer, she might not be the only one with access to her account.

Danielle called a computer repair company. After a thorough inspection, the company’s employees informed Danielle she had several dozen software applications commonly known as “spyware” loaded on to her computer. The spyware enabled someone in cyberspace to watch every move Danielle made on her computer. The computer repair employees told her that one or more of these spyware programs had likely gathered her bank account information and shared it with a third party, paving the way for the unauthorized purchases.

Like Danielle, thousands of other computer owners are unaware of the perils of spyware, a form of advertising-supported software. The term “spyware” is Internet slang that describes technology which “takes up residence” on a personal computer, usually without the owner’s knowledge or consent. Its purpose is to gather information about “the activities and preferences of the computer’s users,” and to retrieve data stored on a computer so it can be forwarded to a third party. While some of these programs are fairly harmless, other more nefarious spyware programs can lead to problems ranging from those suffered by Danielle all the way to the theft of one’s identity.

If Danielle is lucky, she will recover the majority of her money lost based on unauthorized purchases. Still, the monitoring of one’s computer use can result in not just financial harm. It can also produce a significant breach of another important, but less tangible interest—the person’s right to privacy. One of the fundamental principles related to our general understanding of what constitutes privacy is a person’s ability to retreat to a space where he or she cannot be troubled, interrupted, or viewed by the

3. Id. at 6-7.
4. The Federal Fair Credit Billing Act allows parties to contest charges for purchases that account holders did not receive or accept. See 15 U.S.C. § 1666 (2000). The Act requires that the creditor either clarify the charge or “make appropriate corrections in the account of the obligor,” id. at § 1666(a)(B), but the creditor who fails to do so only forfeits a maximum of $50.00. Id. at § 1666(e). Also, the Act is limited to “billing errors.” See id. at § 1666. This does include a variety of activities, such as mathematical problems or a failure to properly credit an account for returned merchandise. Id. at § 1666(b)(4)-(5). For a good summary of the Federal Fair Credit Billing Act, see Credit Cards: What’s Wrong With This Bill?, Consumer Reports, Feb. 2004, http://www.consumerreports.org/cro/personal-finance/creditcard-billing-errors-204/overview/index.htm.
5. See infra Part II.
outside world. However, as our dependence on computer technology and our Internet usage become more extensive, it is also clear that our sense of personal privacy is potentially under attack in novel ways.

This Article will discuss whether the common law torts that protect one's privacy rights—intrusion upon one's seclusion, public disclosure of private facts, appropriation of one's likeness, and placing a party in an objectionable false light in the public eye—can properly and effectively combat the new privacy threats potentially caused by advertising-supported software. Part I chronicles the rise of spyware as a problem, focusing particular attention on how it works and how it potentially endangers people like Danielle. Part II will discuss the evolution of the torts that comprise the rights of action protecting a plaintiff's privacy interests. Part III will analyze the applicability of these torts to the possible privacy hazards associated with advertising-supported software. The Article concludes with the premise that under some circumstances, courts can and should recognize spyware-related incidents as actionable invasions of privacy for plaintiffs.

PART I

American dependence on technology extends to our daily lives in ways that could not have been imagined thirty years ago. For many of us, as we head to work, we cannot do so without our Blackberries or tablet computers. When we leave work for home, we make a direct path to the Xbox, iPod, or TiVo. We can no longer envision our lives without cell phones or home computers. Our technological addictions have created a new type of arms race that now allows people to store, transmit, and access more information in more ways than at any other time in human history.

But for every electronic advance, there is collateral risk. Our dependence is not lost on those who wish to profit from our reliance. Third-parties, like advertisers, marketing professionals, and hackers, have also benefited from the recent technology boom. The more we use personal computers, the more “they”
can see us.\textsuperscript{13} By using the science available to track Internet activity, often via spyware or adware, these third-parties can personalize their marketing in a way that other traditional advertising media cannot.\textsuperscript{14} While much of the marketing use of spyware can be relatively harmless,\textsuperscript{15} computer hackers can also use this technology for malevolent purposes.\textsuperscript{16} Each time a computer user clicks on an unsolicited Web site or advertisement, he or she potentially creates an avenue for spyware to infect one’s system.\textsuperscript{17}

\textit{A. Advertising and the Internet}

While not all can afford the latest scientific wizardry, most people can place much of the world at their fingertips via the Internet, a global, interconnected network of computers that provides a pathway to information of any and all types.\textsuperscript{18} From its humble origins as a small collection of computer networks used by the Department of Defense for military communications,\textsuperscript{19} the Internet now allows users to easily find and use data regarding virtually any subject from any part of the world.\textsuperscript{20} The term “Internet” is often inaccurately used interchangeably with the term “World Wide Web.”\textsuperscript{21} The Internet refers to the technology that enables information to be retrieved online through computers, servers, and cables, while the Web is the compilation of text, audio, and photographs that can be accessed via the Internet.\textsuperscript{22} Semantics aside, people like Danielle now use the Internet and the World Wide Web to shop, do all of their banking, and keep up with current events. The Pew Internet and American Life Project estimated that on an average day in 2005, 94 million Americans

\begin{footnotesize}
\begin{itemize}
  \item \textsuperscript{13} See supra notes 2-3 and accompanying text.
  \item \textsuperscript{14} See PCmag.com, Definition of: Spyware, http://www.pcmag.com/encyclopedia_term/0,2542,+spyware&i=51898,00.asp (last visited Dec. 30, 2006).
  \item \textsuperscript{15} See What is Spyware?, http://www.spywaredetectiontips.com (last visited Dec. 30, 2006).
  \item \textsuperscript{18} The Internet has been defined in many ways. This is only one example. See \textit{In re Doubleclick, Inc.}, Privacy Litig., 154 F. Supp. 2d 497, 501 (S.D.N.Y. 2001).
  \item \textsuperscript{19} Id.
  \item \textsuperscript{20} HARLEY HAHN & RICK STOUT, THE INTERNET COMPLETE REFERENCE 497 (1994).
  \item \textsuperscript{21} \textit{In re Doubleclick, Inc.}, 154 F. Supp. 2d at 501.
  \item \textsuperscript{22} See id.
\end{itemize}
\end{footnotesize}
used the Internet.\textsuperscript{23} It is also estimated that in 2006, approximately 1.043 billion people across the planet will access the Internet.\textsuperscript{24}

As it became evident that increasing numbers of people were spending larger amounts of time on the Web, advertisers began to direct more resources toward Internet marketing.\textsuperscript{25} This online advertising comes in several models.\textsuperscript{26} “Banner” advertisements are bars that resemble billboards that either run across the top of the Web page or down one of its sides.\textsuperscript{27} Then, there are “pop-up” advertisements, which are separate advertising windows.\textsuperscript{28} When users click on the advertisement, they are then connected to the advertiser’s Web page.\textsuperscript{29} While banner advertisements do not necessarily interfere with the user’s ability to read the substantive content of the Web site, pop-up ads jump to the top of the screen and require the user to close them in order to continue working on whatever is beneath the ad.\textsuperscript{30} Many advertisements also now use real-time videos on the Web to display their wares, giving them more of a look and feel of traditional television commercials.\textsuperscript{31}

When Web browsers began to develop programs that allowed users to block pop-up ads, software developers created “pop-under” ads, which appear behind the page the user views as opposed to on top of it.\textsuperscript{32} Yet another form is the “floater,” which uses a Macromedia Flash program to display the ad in front of the user’s screen for as long as 30 seconds before the desired Web page is finally accessible.\textsuperscript{33} Floater ads do not create a separate window like pop-up ads, so although they do have “close” options on them, they still obscure the entire page beneath them.\textsuperscript{34}

\begin{enumerate}
\item\textsuperscript{23} Daily Internet Activities, \url{http://www.pewinternet.org/trends/Daily_Activities_12.05.05.htm} (last visited Dec. 30, 2006).
\item\textsuperscript{24} World Internet Usage and Population Statistics (June 30, 2006), \url{http://www.internetworldstats.com/stats.htm}.
\item\textsuperscript{25} Interactive Advertising Bureau, Internet Advertising Revenues Close to $4 Billion for Q1 2006 (May 30, 2006), \url{http://www.iab.net/news/pr_2006_05_30.asp}.
\item\textsuperscript{26} See TITTEL, supra note 2, at 12-15.
\item\textsuperscript{27} Id. at 12.
\item\textsuperscript{28} Id.
\item\textsuperscript{29} What is Spyware?, supra note 15.
\item\textsuperscript{30} TITTEL, supra note 2, at 12. Pop-up ads tend to be favored by marketers because it is more likely that web visitors will click on them as opposed to banner advertisements. See Ronald R. Urbach & Gary A. Kibel, Adware/Spyware: An Update Regarding Pending Litigation and Legislation, 16 INTELL. PROP. & TECH. L.J. 7, 12 (2004), available at \url{http://www.dglaw.com/images/TJjournal.pdf}.
\item\textsuperscript{31} See Hyun Ju Jeong, Development of Internet/WWW Ad, \url{http://www.ciadvertising.org/SA/fall_02/adv391k/jeong/page4_2.html} (last visited Dec. 30, 2006).
\item\textsuperscript{32} Steven J. Vaughan-Nichols, Pop-Up Ads Shed Blocks, Tackle Consumers, WASH. POST, June 26, 2005, at F5.
\item\textsuperscript{33} Id.
\item\textsuperscript{34} Id.
\end{enumerate}
While traditional advertising used polling and research to best predict what viewers might read or see, online advertisers are now able to accomplish the same goal by using technology to track the habits of users. For example, when users visit certain Web pages, the site may place textual records called “cookies” on the hard drive. These very small text files record information like user names, passwords, or account numbers, so the user does not have to enter the same information every time they access that particular site. Cookies are also capable of tracking the user’s movements on the Web, allowing those who receive the information to calculate what type of advertising that particular user may find attractive so they can send users targeted advertisements in the future. Cookies are fairly harmless because they often are easy to block by privacy controls that exist on most Web browsers.

B. Defining and Understanding Spyware

Spyware tends to be difficult to precisely characterize because it can encompass anything that resides on your computer that has the ability to report on the preferences and activities of the user once it is installed. Spyware is regularly grouped with another term called “adware,” but although the two terms share certain traits, they are not identical. Adware is designed to display advertising on your computer while it is running, and is generally attached to larger software applications like music file-sharing programs, which typically come at no financial cost to the user. Many of these free software applications contain end-user licensing agreements. These agreements, in very cumbersome language, inform the user that certain other programs may be attached to the free application the user is downloading. Upon downloading the program, users may unknowingly attach adware to their systems, which collects the data of the Web sites the users visit, and enables advertisers to target future ads toward particular users.

36. Id.
37. Id.
38. TITTEL, supra note 2, at 8.
39. Id.
40. Id. at 7.
41. Compare id. at 7 with id. at 10. Contra Urbach & Kibel, supra note 30, at 12.
42. TITTEL, supra note 2, at 10.
44. This is a common tactic in peer-to-peer file sharing programs, such as popular music download sites like KaZaa. See Urbach & Kibel, supra note 30, at 12.
45. Id.
Similarly, users often inadvertently download spyware applications by simply clicking on pop-up advertisements, visiting certain Web sites, or opening unsolicited electronic-mail messages. But, the installation comes without the user’s consent because the spyware programs do not provide the same notice that the end-user licensing agreement does. While some precautions can be taken to guard against spyware infecting one’s computer, inexperienced parties like Danielle often do not protect themselves against these software programs because they are unaware of their existence until it is too late. Moreover, spyware has proven to be flexible, versatile, and resourceful. Once it is on your computer, it is notoriously difficult to uninstall or delete.

The danger of spyware fluctuates according to the type of tracking device in the software. Some forms are merely designed to watch your Web activity and track the sites you visit, much like cookies. There is also the Browser Highjacking Object (BHO), which is designed to take over the user’s Internet browser. The BHO can reset the user’s home page to the vendor’s Web page or even alter the results one sees when conducting searches through more traditional engines like Google.

One of the most hazardous forms of spyware is the “keystroke logger.” It can come in the form of a battery-sized plug that is physically inserted into the computer, or it can be downloaded on to your system as software. It has the ability to record keystrokes that it saves as text on its own hard drive, allowing the party who installed it to collect the information by physically removing it or reading the data when it is uploaded periodically over the Internet. The key logger tool provides some beneficial uses, such as allowing parents to monitor the Internet activity of their children, but it can also be used to access sensitive personal

46. Generally, the underlying Web site has no relationship with either the pop-up provider or the advertiser. See id.
48. Id. at 34.
49. Id. at 33.
51. Slutsky & Baran, supra note 47, at 33.
52. Id.
54. See What is a Keylogger? (June 8, 2005), http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci962518,00.html.
55. Id.
information, such as Social Security numbers, e-mail passwords, bank account transactions, or credit card numbers.\textsuperscript{56} Criminal use of programs like the keystroke logger has led to a sharp rise in consumer complaints of Internet-related fraud and identity theft.\textsuperscript{57} In 2004, the federal government estimated total losses related to identity theft and credit card fraud at $52.6 billion to individuals and businesses.\textsuperscript{58}

The arrangement between those who provide spyware or adware and Web site operators is mutually advantageous. Web site operators receive much-needed revenue by selling advertising to those who are interested, which offsets the costs associated with product development.\textsuperscript{59} Conversely, while advertisers may not know for certain if their television commercials or print advertisements are being seen by their target audience, pop-up ads, pop-under ads, and floaters ensure that their ad displays are at least being seen by their audiences, even if not every user clicks on the advertisement.\textsuperscript{60} While marketers may have been initially slow to realize the potential of the Internet, this is no longer the case.\textsuperscript{61}

While marketers may have been initially slow to realize the potential of the Internet, this is no longer the case.\textsuperscript{61} In the third quarter of 2005, Internet advertising revenues reached a

\begin{footnotes}
\item[56] Slutsky & Baran, \textit{supra} note 47, at 33. For example, Specter Pro, which describes itself as “the world’s best selling software for monitoring and recording every detail of PC and Internet activity,” enables those who purchase it to use its key logger to document every key typed on the keyboards of their personal computers.

\textit{SpectorSoft, http://www.spectorsoft.com/products/SpectorPro_Windows/entry.asp?refer=6940} (last visited Dec. 30, 2006). It is designed to intercept alphanumeric keystrokes and hidden characters, like the shift and control key. \textit{Id.} It allows users to also record instant messages, all electronic mail (both sent and received), Web sites visited, and keystrokes entered, and it offers keyword detection and Internet access blocking. \textit{Id.} It retails anywhere from $99.95 to $149.95. \textit{Id.}


\item[58] \textit{Id.}

\item[59] \textit{See} TITTEL, \textit{supra} note 2, at 4.

\item[60] \textit{See} Urbach & Kibei, \textit{supra} note 30, at 12.


Claria used to broadcast its advertisement messages through software applications that tracked the users’ online behavior, often doing so as a part of free software packages. Claria Corporation, \textit{http://www hoovers.com/claria/-ID_106214--/free-co-factsheet.xhtml} (last visited Dec. 30, 2006). In 2003, it generated $90.5 million in sales, a one-year increase of 122.9% over the previous year. Claria Corp., Registration Statement (Form S-1) (Apr. 8, 2004), \textit{available at http://knobias.10kwizard.com/filing.php?repo=tenk&doc=1&ipage=2723312}. Claria’s net income for 2003 was $34.9 million, a one-year growth rate of 38,203%. \textit{Id.}
\end{footnotes}
record $3.1 billion, the highest quarter reported and a 33.9 percent increase over the previous year. The estimated annual Internet advertising revenue projection for 2005 was $12 billion, a nearly $3 billion increase over 2004. It is precisely this desire to move product that is, at a minimum, causally connected to some of the injuries caused by spyware.

The prevalence of spyware and adware is far from isolated. In October 2004, America Online and the National Cyber Security Alliance conducted a study involving 329 randomly selected personal computers. The study found that 80 percent of the computers contained some form of spyware. The average "infected" computer had 93 spyware or adware programs, providing a small snapshot of the risk to the average user. In response, several anti-spyware bills have been introduced in both the United States House of Representatives and the Senate, but none have yet gained the traction necessary for passage in both bodies. The Securely Protect Yourself Against Cyber Trespass Act (SPY ACT), sponsored by Representative Mary Bono (R-Calif.), was backed by the Energy and Commerce Committee in March 2005. The SPY ACT precludes any person who is not an authorized user or owner of a protected computer from engaging in any deceptive act categorized as taking control of the computer, modifying settings related to use of the computer or to the

63. Id.
65. Id. at 2.
66. One computer in the study contained 1,059 spyware or adware programs. Id. at 2.
67. There are already a number of federal laws aimed at protecting privacy rights of individuals. The Electronic Communications Privacy Act, for example, precludes the interception or disclosure of the contents of any electronic communication, ranging from electronic mail to telephone conversations, but it is riddled with exceptions and does not appear applicable to spyware. See 18 U.S.C. §§ 2510–2522 (2000).
70. See H.R. 29, § 2(a)(1).
computer's ability to access or use the Internet, 71 or collecting personally identifiable information through the use of a keystroke logger. 72 The SPY ACT prohibits several other activities as well, but part of the problem with any state or federal legislation is that it runs the risk of being overinclusive. Because spyware has been difficult to label, any number of legitimate advertising Web features could be rendered inoperable by statutory language that is too broad or sweeping. 73 While the SPY ACT does allow for hefty fines for any company that engages in a pattern and practice of spyware-related activity, 74 such legislation would no doubt be vigorously contested by those with lawful marketing and advertising interests.

In summary, it is clear that now more than ever, unassuming consumers are at greater risk for divulging private information. The proliferation of spyware and adware is evidence that the information available online is worth large amounts of money to those who obtain it, whether they are selling information to another party, using that information for marketing purposes, or getting it to pilfer funds or make purchases from the personal accounts of others. 75 This points to only one conclusion: If you use your PC to go online, there is an excellent chance someone is monitoring you without your consent.

PART II

Of all the things most Americans do on a daily basis, few joys rival that of returning to our homes at the end of the day. Being able to shut the door on the rest of the world and retreat to our own space is often the chief incentive for working our way through the rigors of work, school, or in some cases, socializing. But what is it about our privacy that we cherish so much? Clearly, the independence involved with being able to choose your own path of movement presents one rationale. 76 The freedom to select when you want to engage in discussion and when you wish to retreat from such provides us with needed self-autonomy and empowerment in ways that the bulk of our daily activities do not

71. See id. § 2(a)(2).
72. See id. § 2(a)(3).
73. See McGuire, supra note 69.
74. See H.R. 29, § 4(b)(1)(A) (stating that the proposed fine to be paid to the Federal Trade Commission for repeated violations of deceptive acts or practices relating to spyware is $3 million).
75. See TITTEL, supra note 2, at 4.
allow. Much of the disparate range of human natural emotion, be it pleasure, sadness, grief, or anger, would be stifled considerably if people could not express such feelings behind closed doors, leading one to conclude that our right to be left alone is essential to our personal and emotional development.

Although the law was slightly delinquent in recognizing the high societal value in maintaining one's right to be left alone, the limits and threshold of our right to privacy—tortious, constitutional, or otherwise—have engendered considerable debate. As we head further into an information age that is sure to see the reach of technology's tentacles extend to more areas of life, it will get increasingly difficult to retreat without someone having access to one's person. Spyware is only one small element in this equation, but in many ways, it is a microcosm of the larger tension between the present-day societal interest in data collection and the individual's right to withdraw from the world when he or she chooses to do so.

A. Privacy: A Brief Background

Before pinpointing some of the particulars of the tort of invasion of privacy, the wide spectrum and scope of what constitutes privacy in the United States merits a brief background discussion. Though a uniform definition of privacy is somewhat elusive, both the federal and state branches of the American judicial and legislative wings of government have consistently attempted to protect the right of individuals and groups to have

---

77. Finkin, supra note 76, at 952-54; Gormley, supra note 76, at 1374; Makdisi, supra note 76, at 987-90.
78. Finkin, supra note 76, at 952-54; Gormley, supra note 76, at 1374; Makdisi, supra note 76.
79. Gormley, supra note 76, at 1339-40.
81. Webster's Dictionary defines privacy as: "1. the state of being private; retirement or seclusion. 2. freedom from the intrusion of others in one's private life or affairs: the right to privacy. 3. secrecy." RANDOM HOUSE WEBSTER'S COLLEGE DICTIONARY 979 (2d ed. 2001).
82. While the vast majority of privacy cases involve individuals, the U.S. Constitution guarantees both freedom of religion and freedom of association, which are more likely to affect groups of people. See U.S. CONST. amend. I. The word "privacy," however, makes no appearance in the Constitution.
their own autonomy, freely express themselves, and retreat from society, if and when necessary.\textsuperscript{83} Additionally, an individual’s right to privacy is, to some degree, protected by cultural, social, and ethical norms as well.\textsuperscript{84}

To the extent that it can be categorized, Professor Anita Allen-Castellitto and other scholars have succinctly divided United States privacy law into four distinct classifications: informational privacy, physical privacy, proprietary privacy, and decisional privacy.\textsuperscript{85} Informational privacy protects a person’s right to preclude others from either gaining access to, or publishing information that that person would consider private or confidential.\textsuperscript{86} Plaintiffs have successfully argued that disclosure of medical records\textsuperscript{87} and other confidential matters\textsuperscript{88} violated their right to keep personal information from being disclosed to the public. Physical privacy rights safeguard a person’s interest in his or her own bodily autonomy and emotional tranquility.\textsuperscript{89} Physical privacy cases cast a wide net across areas ranging from constitutional issues, such as a party’s Fourth Amendment protection from illegal searches and seizures by the government\textsuperscript{90} to improper “viewing intrusions.”\textsuperscript{91} The home is often the benchmark of a person’s physical privacy rights.\textsuperscript{92} Proprietary privacy rights shield our interest in keeping others from exploiting our likeness\textsuperscript{93} for monetary gain or other business purposes.\textsuperscript{94}

\begin{flushleft}


85. Id.

86. See id. at 19 tbl. 1.

87. See, e.g., Pachowitz v. Ledoux, 2003 WI App. 120, ¶ 24, 265 Wis. 2d 631, ¶ 24, 666 N.W.2d 88, ¶ 24 (finding that disclosure of plaintiff’s private medical records by emergency medical technician to one person constituted invasion of privacy under state law).

88. See, e.g., Urbaniak v. Newton, 277 Cal. Rptr. 354, 360 (1991) (finding that defendant’s disclosure of plaintiff’s human immunodeficiency virus (HIV) status violated plaintiff’s privacy rights when plaintiff only revealed information to protect other health care workers who may come into contact with him).

89. See Allen-Castellitto, supra note 84, at 19 tbl. 1.

90. See, e.g., Katz v. United States, 389 U.S. 347, 353 (1967) (holding that citizens have reasonable and legitimate expectations of privacy under the Fourth Amendment, even in areas as small as a public phone booth).


92. See Allen-Castellitto, supra note 84, at 19 tbl. 1.


94. See Allen-Castellitto, supra note 84, at 19 tbl. 1.
\end{flushleft}
Decisional privacy protects one’s right to make personal choices free from government interference or restriction. This type of privacy has proven to be a lightning rod for controversy due to the complex social overtones associated with protections concerning abortion, contraception, homosexuality, and one’s "constitutionally protected right to refuse lifesaving hydration and nutrition." Privacy rights are not absolute and frequently must be weighed against other interests that may be at stake during litigation. Still, because of their essential underlying principles of self-autonomy, acceptance, and independence, privacy rights are exceedingly important to most Americans.

The development and evolution of the four branches that currently comprise the tort of invasion of privacy probably can be traced to a pair of law review articles: Louis Brandeis and Samuel Warren's article, The Right to Privacy, which was published in the Harvard Law Review in 1890, and Dean William Prosser's article Privacy, which was published seventy years later in the University of California Law Review. Since then, the origins and development of the right to privacy have been among the most discussed topics in American jurisprudence.

B. Warren and Brandeis: The Inspiration

Legend has it that around 1890, Samuel Warren, who graduated at the top of his class at Harvard Law School but had ceased practicing law, became exasperated at the Boston press for its

95. See id.
96. See Roe v. Wade, 410 U.S. 113, 153 (1973) (holding that the right to privacy protected by the Fourteenth Amendment supersedes laws that criminalize abortion).
97. See Griswold v. Connecticut, 381 U.S. 479, 485 (1965) (holding that fundamental rights to marital privacy exist with the "penumbra" of liberties within the Constitution's Bill of Rights and thereby prohibit any legislation that attempts to criminalize contraception).
98. See Lawrence v. Texas, 539 U.S. 558, 578 (2003) (holding that a Texas statute prohibiting intimate acts between members of the same sex is unconstitutional due to infringement upon liberty interests provided by the Fourteenth Amendment).
100. See Allen-Castellitto, supra note 84, at 13.
104. See, e.g., Joshua Herman, Identifying Privacy: An Introduction, 54 DEPAUL L. REV. 657 (2005) (discussing symposium on modern applications of privacy law to several areas based on historical development).
According to Prosser, events "came to a head when the newspapers had a field day on the occasion of the wedding of a daughter, and Mr. Warren became annoyed." Warren contacted Louis Brandeis, his former law partner, and the two crafted a law review article that became the foundation for privacy rights in the United States. While the urban legend of what exactly precipitated the article has since been debunked somewhat, it is clear that the authors were motivated at least in part by concern about journalism tactics that became more pronounced with the advent of the technological changes that threatened individual solitude. They wrote:

Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge [Thomas] Cooley calls the right "to be let alone." Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."

Prior to the article, American courts had not affirmatively recognized an individual right to privacy that was enforceable via civil court, but had on occasion crafted legal remedies using

105. See Prosser, supra note 103, at 383.
106. Id. (citing ALPHEUS THOMAS MASON, BRANDEIS: A FREE MAN'S LIFE 70 (1946)).
107. Prosser, supra note 103, at 383-84.
109. Warren and Brandeis wrote:

The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers. To occupy the indolent, column upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle.

Warren & Brandeis, supra note 102, at 196.
110. For an excellent synopsis of the historical context that provided the backdrop for the article of Warren and Brandeis, see Gormley, supra note 76, at 1350-53.
111. See Warren & Brandeis, supra note 102, at 195 (footnote omitted). The technological advances at issue in this excerpt from the article are not far removed from the same types of issues facing society today.
112. The Fourth Amendment of the U.S. Constitution guarantees individuals the "right . . . to be secure in their persons, houses, papers and effects," but these rights only curtailed the government's ability to intrude on one's home or property; private
existing law to safeguard such a right. For example, an aggrieved party could file a trespass action to protect his or her privacy rights, but the plaintiff had to prove that a physical invasion took place in order to be successful. It was also possible for parties to be prosecuted criminally for invading the privacy of another, but such laws were often substantively ineffective. Although courts had not yet gone far enough to positively ensure that one did indeed have the right to be left alone, Warren and Brandeis were able to successfully mold such an argument around a fundamental premise: creating a right to privacy was far from legal overkill because so many other areas of law already implicitly supported such a right.

The authors explained that one court had already held that the author of any private letter, literary product, or other artistic work “possesses such a right of property in them, that they cannot be published without his consent, unless the purposes of justice, civil or criminal, require the publication.” Another court had precluded student publication of a teaching surgeon’s lectures on the grounds that making the material public would be a breach of confidence that was tantamount to breach of an implied contract. Warren and Brandeis argued that while such matters clearly deserved legal protection, to do so by stretching the areas of contract law or trusts was not legally sound. By recognizing the
more general right of privacy, it would no longer be necessary to contort existing areas of the law to create just results for wronged parties. Moreover, since the law permitted compensation for mental distress, Warren and Brandeis contended that the private person who chose to keep personal concerns removed from the public eye also deserved compensation for whatever emotional harm may emanate from having such matters exposed without his authorization. Accordingly, the pair deemed it sensible to broaden the law in order to meet the “political, social, and economic changes” that were inevitable in a growing society.

Warren and Brandeis also clearly understood, however, that such a right needed limitations, and suggested several possible areas of privilege: (1) The right to privacy should not prohibit any publication of any matter which is of public or general interest; (2) the right to privacy should not prohibit the communication of any matter, even if private in nature, when the publication is made under circumstances that would make it privileged under the law of defamation; (3) any right to privacy would not likely grant redress for invasion of privacy by oral publication if there was no special damage; and (4) the right to privacy would cease upon the publication of the facts by the individual himself, or with his consent. The authors also noted that neither the truth of the matter nor the absence of any malice on the part of the publisher would afford a defense to a privacy action.

Despite the cogency and lucidity of the article’s arguments, the right to privacy “revolution” was somewhat slow to materialize in the courts. It was not until fifteen years after the article’s time when the abuse to be guarded against could rarely have arisen without violating a contract or a special confidence; but now that modern devices afford abundant opportunities for the perpetration of such wrongs without any participation by the injured party, the protection granted by the law must be placed upon a broader foundation.

Warren & Brandeis, supra note 102, at 209-11.
120. Warren & Brandeis, supra note 102, at 213-14.
121. See id.
122. Id. at 193.
123. See generally id.
124. Id. at 214.
125. Id. at 216.
126. See id. at 217.
127. Id. at 218.
128. Id.
129. For example, in Roberson v. Rochester Folding Box Co., 64 N.E. 442 (N.Y. 1902), the New York Court of Appeals rebuffed the claim of a plaintiff who had alleged that the defendants invaded her privacy by using her picture without her consent in an advertisement for flour. The court justified its decision based on concerns that:
publication that the first American court recognized a common law right to privacy.\textsuperscript{130} In \textit{Pavesich v. New England Life Ins. Co.},\textsuperscript{131} Paolo Pavesich, an artist, sued New England Mutual, a life insurance company; Thomas Lumpkin, a general agent of New England Mutual; and photographer J.Q. Adams after a picture of Pavesich appeared in \textit{The Atlanta (Ga.) Constitution}.\textsuperscript{132} The plaintiff’s photo appeared next to a person the court described as “ill-dressed and sickly looking.”\textsuperscript{133} The words, “Do it now. The man who did.” appeared above the plaintiff’s photograph, while the words, “Do it while you can. The man who didn’t.” appeared above the other picture.\textsuperscript{134} The advertisement also included text implying that Pavesich had bought life insurance from New England Mutual, and that his life had prospered from that decision.\textsuperscript{135} New England Mutual received the picture from a negative from Adams, but while Adams knew why the photograph would be used, Pavesich, who never had a life insurance policy with New England Mutual, did not consent to the use of his likeness.\textsuperscript{136} He sued the defendants for libel and for invading his right to privacy.\textsuperscript{137}

After the lower court sustained the demurrer of the defendants,\textsuperscript{138} Pavesich found a receptive audience for his claims in the Georgia Supreme Court. While acknowledging there had been no specific right to privacy in any prior decision, the court found that such a right did indeed exist:

The right of privacy has its foundation in the instincts of nature. It is recognized intuitively, 

\begin{quote}
The attempts to logically apply the principle will necessarily result, not only in a vast amount of litigation, but in litigation bordering upon the absurd, for the right to privacy, once established as a legal doctrine, cannot be confined to the restraint of the publication of a likeness but must necessarily embrace as well the publication of a word-picture, a comment upon one’s looks, conduct, domestic relations or habits.
\end{quote}

\textit{Id.} at 443. In response, the New York legislature enacted a statute that made it a criminal misdemeanor and a possible tort action for any person, firm, or corporation to use another’s name, portrait, or picture for commercial purposes without the consent of the subject. \textit{See} 1903 N.Y. Laws 308 (codified as amended at N.Y. CIV. RIGHTS LAW §§ 50-51 (McKinney 1992 & Supp. 2006)).

\textsuperscript{131.} \textit{Id.}
\textsuperscript{132.} \textit{id.} at 68.
\textsuperscript{133.} \textit{Id.}
\textsuperscript{134.} \textit{Id.}
\textsuperscript{135.} Under Pavesich’s picture, the text of the advertisement said: “In my healthy and productive period of life I bought insurance in the New England Mutual Life Insurance Co., of Boston Mass., and to-day my family is protected and I am drawing an annual dividend on my paid-up policies.” \textit{Id.} at 69.
\textsuperscript{136.} \textit{Id.}
\textsuperscript{137.} \textit{Id.}
\textsuperscript{138.} \textit{Id.}
consciousness being the witness that can be called to establish its existence. Any person whose intellect is in a normal condition recognizes at once that as to each individual member of society there are matters private, and there are matters public so far as the individual is concerned. Each individual as instinctively resents any encroachment by the public upon his rights which are of a private nature as he does the withdrawal of those of his rights which are of a public nature. A right to privacy in matters purely private is therefore derived from natural law.  

The Pavesich decision recognizing the plaintiff’s right to privacy produced more debate from American courts as to the legitimacy of such a right. After the American Law Institute recognized such a right in the 1939 edition of the Restatement of Torts, however, the vision of Warren and Brandeis began to establish a permanent foothold.

C. Clarification from Dean Prosser

While the Warren-Brandeis article made the case for establishing a right to privacy, Prosser’s article illuminated the interests such a right protected and what conduct should be precluded to further defend such rights. Prosser’s study of the reported privacy decisions led him to conclude that the right to privacy was not one independent tort, but actually four different torts, each of which safeguarded a different privacy interest. He categorized them as an "intrusion upon the plaintiff’s seclusion or solitude," "public disclosure of embarrassing private facts about the plaintiff," "publicity which places the plaintiff in a false light in the public eye," and "appropriation, for the defendant’s advantage, of the plaintiff’s name or likeness." Prosser’s work led to the categorization of privacy torts in the Restatement (Second) of Torts, which has been exceedingly

139. Id. at 69-70.
140. See Gormley, supra note 76, at 1353-54.
141. "A person who unreasonably and seriously interferes with another’s interest in not having his affairs known to others or his likeness exhibited to the public is liable to the other." RESTATEMENT OF TORTS § 867 (1939).
142. Prosser, supra note 103, at 389.
143. Id.
144. Id.
145. Id.
146. Id.
147. Id.
influential in helping states determine whether, and to what extent, privacy rights should be recognized.

1. Intrusion Upon Seclusion

Prosser described this class of privacy cases as those which protected a plaintiff's mental interests when causes of action like trespass and nuisance did not do so sufficiently. \(^{149}\) While the early cases focused on physical intrusions into a plaintiff's space, \(^{150}\) the cases began to eventually encompass any type of prying or intrusion into anything the plaintiff would consider private. \(^{151}\) Prosser was careful to note that intrusion cases, like the other privacy torts, were subject to limitations. \(^{152}\) For example, Prosser felt plaintiffs could not expect to recover for any perceived slight or interference with their solitude. \(^{153}\) Plaintiffs also could not state a claim for alleged intrusions that took place in public, where the plaintiff had no right to be left alone, or if there were disclosures that were required to comply with existing law. \(^ {154}\)

The Restatement (Second) of Torts followed Prosser’s lead, defining the tort as follows: “One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.” \(^ {155}\) The Restatement further stated that the intrusion could be harmful to the plaintiff’s person, “his private affairs or concerns,” \(^ {156}\) and could be accomplished “by the use of [a] defendant’s senses, with or without mechanical aids.” \(^ {157}\) Today, intrusion is probably the branch that best represents the goal of privacy torts—the protection against “affront[s] to individual dignity.” \(^ {158}\)

2. False Light

Just as intruding upon one’s seclusion was a possible invasion of privacy, it was similarly clear that when a party placed the

---

149. Prosser, supra note 103, at 392.
150. See, e.g., Byfield v. Candler, 125 S.E. 905 (Ga. Ct. App. 1924) (allowing a cause of action because defendant ventured into woman’s stateroom on a steamship).
151. Prosser, supra note 103, at 390-91.
152. Id.
153. Id. at 390 (“It is clear, however, that there must be something in the nature of prying or intrusion, and mere noises which disturb a church congregation or bad manners, harsh names and insulting gestures in public, have been held not to be enough.”).
154. Id. at 391.
156. Id. at cmt. a.
157. Id. at cmt. b.
plaintiff in a false light in the eye of the public, that too comprised a viable privacy claim. Prosser contended that American courts recognized three different contexts of successful false light actions: (1) When the defendant falsely attributed an opinion or statement to the plaintiff; (2) when the defendant used the plaintiff's likeness or picture to highlight books or articles that were not connected to the plaintiff; or (3) the defendant used the plaintiff's image, name or physical characteristics among images including convicted criminals when the plaintiff was innocent of any crime. Prosser also underlined that false light claims could also lead to defamation claims in some, but not all instances, and that like intrusion cases, supersensitive parties did not merit false light protection.

The Restatement presently defines false light claims thusly:

One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if (a) the false light in which the other [person] was placed would be highly offensive to a reasonable person, and (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.

In order for plaintiffs to be successful, they must prove the matter published is not true.

Of the four privacy torts, courts have viewed the "false light" branch with the most cynicism. Currently, only two-thirds of the states affirmatively recognize false light as a theory of recovery. A number of states expressly reject it, including Colorado, Massachusetts, Minnesota, North Carolina, Ohio, South Carolina, Texas, and Virginia.

159. Prosser, supra note 103, at 398.
160. Id.
161. Id. at 399.
162. Id.
163. Id. at 400.
164. Id.
166. Id. at cmt. a.
167. See supra notes 148-155 and accompanying text.

Although Warren and Brandeis advocated for a general right to privacy, they appeared to be most disturbed at the increasing proclivity of the press to make public information which most would consider private. Prosser characterized this type of invasion as public disclosure of private facts. He explained that the prior cases were consistent in that liability could only be imposed if the facts at issue could be categorized as private and if the disclosure was made publicly. These limitations eliminated idle gossip between individuals as actionable, as well as anything that the plaintiff held out to the public for consumption.

The Restatement (Second) again followed Prosser’s lead, calling publicity claims permissible if the matter publicized is of the type that: “a) would be highly offensive to a reasonable person and b) is not of legitimate concern to the public.” The disclosure cases are designed to protect the community standing of the plaintiff and can be construed as “an extension of defamation.” Unlike defamation, however, the truth of the facts disclosed is not a defense to disclosure claims because a statement’s falsity is not necessary to state a claim. Disclosure cases are vulnerable to constitutional limitations, specifically those related to freedom of the press and freedom of speech.
4. Appropriation

The final category of privacy cases concerned the "exploitation of the plaintiff's identity," i.e., using the likeness or name of the plaintiff for the benefit of the defendant, without the plaintiff's consent. The Restatement (Second) mirrored Prosser's language in defining appropriation, calling it viable when one "appropriates to his own use or benefit the name or likeness of another." Defendants have also been able to contest appropriation claims by successfully arguing that the use of one's likeness is permissible when made in the context of, or in reasonable relation to, a publication that is both newsworthy and of legitimate public concern.

Although Prosser concluded that appropriation cases also fell under the rubric of privacy, the interest shielded by appropriation does not on its face seem to be aimed at protecting the plaintiff's mental tranquility in the same fashion as the other branches of this tort. Prosser acknowledged that it instead appeared to protect the plaintiff's right to control the exploitation of his image in the same way one protects a copyright or trademark, giving appropriation claims both personal and economic texture. For this reason, this branch is often overlapped with the right to a publicity cause of action, which celebrities periodically pursue when someone else uses their name without their consent for commercial purposes. Still, because of the possible mental distress that can emanate from having one's image or likeness exposed to the public without consent, appropriation has survived as a practical extension of one's right to be left alone.

magazine that revealed he was living in a rooming house because the facts were "newsworthy".

185. Prosser, supra note 103, at 401-02. The Pavesich case, which first recognized a right to privacy, could in theory have also been characterized as an appropriation case because of the insurance company's attempt at using the alleged testimonial from Mr. Pavesich to generate more business. See generally Pavesich v. New England Life Ins. Co., 50 S.E. 68 (Ga. 1905).


187. See, e.g., Zacchini v. Scripps-Howard Broad. Co., 433 U.S. 562, 569 (1977) (holding that an entertainer's claim against defendant for filming his circus-like act and broadcasting it on the evening news was not viable because of defendant's right to broadcast matters of public concern).

188. See Prosser, supra note 103, at 406.

189. Id.

190. See, e.g., Carson v. Here's Johnny Portable Toilets, Inc., 698 F.2d 831, 835-36 (6th Cir. 1983) (holding that a former entertainer's commercial identity was potentially appropriated by defendant's use of phrase "Here's Johnny" in association with defendant's product).

191. While it has survived, appropriation has not done so unscathed. One court has called it "misleading" to attach the privacy label to appropriation claims because the interest protected is not really private in the same sense as the tort's other claims. Joe Dickerson & Assoc., L.L.C. v. Dittmar, 34 P.3d 995, 999-1000 (Colo. 2001). For similar reasons, other courts have affirmatively distinguished
Prosser’s four-fold categorization of what comprised the single
tort of invasion of privacy covered the areas of physical,
informational, and proprietary privacy, described by Professor
Allen-Castellitto and others.192 Although Prosser’s article
acknowledged that more than one theory could be used under the
same set of facts, the article also concluded that it was not sound to
lump all four theories together without distinguishing them.193
Prosser explained that while intrusion upon one’s seclusion and
public disclosure of private facts both necessitated the invasion of
something confidential, this was not the case with the false light or
appropriation torts.194 Appropriation required something the
defendant could use to his or her own advantage, making it distinct
from the other three forms,195 and false light claims needed proof
of falsity or fiction in a way the other forms did not.196 Each
covers a distinct mode of invasion and addresses slightly different
affronts to one’s personal dignity.197

Prosser also concluded that the right to privacy is generally a
personal one that does not extend to others unless their privacy is
invaded along with the plaintiff.198 It is also generally not
actionable after the plaintiff’s death unless expressly provided for
by statute.199 Today, most courts limit the right to privacy to
individuals and do not grant corporations a similar right.200 Only
two states do not currently recognize some form of the privacy
rights first espoused by Warren and Brandeis and later crystallized
by Prosser: North Dakota and Wyoming.201

PART III

The functionality of the Internet relies on the acquisition and
accumulation of copious amounts of data. Because more and more
corporations like financial banking institutions and health care
organizations are keeping client records online,\textsuperscript{202} sensitive information is more vulnerable to those with the ability, technology, and desire to access such records without permission.\textsuperscript{203} This naturally creates new concerns about whether the privacy of individuals is adequately protected against these somewhat non-traditional intrusions.\textsuperscript{204} Advertising-supported software has already forced courts to assess the boundaries of existing copyright and trademark laws.\textsuperscript{205} It seems only a matter of time before an individual, who may not have initially understood the potential infringement of spyware programs brings suit, too.\textsuperscript{206}

A. Making the Case for the Plaintiff

On occasion, plaintiffs have been able to argue that several of the four privacy theories—intrusion, appropriation, false light, and disclosure—were simultaneously pertinent to their claims.\textsuperscript{207} This would not be as likely to occur in suits related to spyware. For example, a disclosure theory requires the public disclosure of facts that would generally be considered private.\textsuperscript{208} The applicability of disclosure to spyware-related claims would hinge on how broadly the court would interpret the term “public.”\textsuperscript{209} Spyware providers typically only offer the mechanism by which data can be accessed.\textsuperscript{210} There is usually no “publication” of the information received about the user; it is collected by a third party for future use. Still, if the collection of this information reached a significant number of parties, a court could find that sufficient to satisfy the

\textsuperscript{202} Gillian Flynn, Privacy in an Age of Online Record-Keeping, WORKFORCE MGMT., Aug. 2001, available at http://findarticles.com/p/articles/mi_m0FXS/is_8_80/ai_77612539.

\textsuperscript{203} See supra notes 58-66 and accompanying text.

\textsuperscript{204} See GEORGE B. DELTA & JEFFREY H. MATSUURA, THE LAW OF THE INTERNET § 1.07 (2d ed. 2006).


\textsuperscript{206} Through August 2006, there were no reported cases where a plaintiff has alleged a common law invasion of privacy action due to spyware-related concerns.

\textsuperscript{207} See, e.g., Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231 (Minn. 1998) (finding that intrusion, appropriation, and disclosure theories potentially applied to a case where defendant’s employee circulated photos of plaintiffs naked); see also RESTATEMENT (SECOND) OF TORTS § 652A cmt. d (1977).

\textsuperscript{208} Cox Broad. Corp. v. Cohn, 420 U.S. 469, 489, 495 (1975).


\textsuperscript{210} See supra note 3 and accompanying text.
requirement that the fact be released to the public at large. If, however, the plaintiff’s claim focused on the privacy infringement created by the presence of spyware, neither the theory of public disclosure of private facts nor the theory of painting one in a false light would be actionable because of the lack of publication.

Appropriation claims, although a slightly better match than disclosure and false light, are still an inexact fit. Plaintiffs could argue that information collected by spyware about their perceived personal preferences is done for the commercial benefit of targeted advertising, generating potential profit for the defendant, either by using the information directly or selling it to another party. The Restatement, however, clearly says the purpose of appropriation claims is to shield an individual’s interest in the exclusive use of his own identity. Accordingly, appropriation suits characteristically require manipulation of the plaintiff’s name or likeness, such as publishing a person’s photograph without consent in an advertisement, as was the case in Pavesich, or impersonating an individual to obtain information about another party. Spyware programs only gather data to forecast user behavior and Web tendencies.

This leaves intrusion as the most viable avenue for spyware claims. Intrusion cases typically require that plaintiffs clear two hurdles to state a claim, both of which are consistent with the

211. See generally infra note 212 and accompanying text.
212. See generally supra notes 208-210 and accompanying text. If the plaintiff’s lawsuit focused on the party who provided information to a third party without the plaintiff’s knowledge, the theories of disclosure and false light could be more applicable. Plaintiffs would still have to show the information accessed and distributed was private, which at least one court found to be problematic. See, e.g., Busse v. Motorola, Inc., 813 N.E.2d 1013 (Ill. App. Ct. 2004) (holding that no privacy claim existed against defendant who transferred information of cell-phone customers to research firm because information obtained was not private).
213. See supra notes 189-192 and accompanying text; see also infra notes 216-223 and accompanying text.
217. RESTATEMENT (SECOND) OF TORTS § 652C cmt. b.
218. See supra note 3 and accompanying text. In Dwyer, the plaintiffs, as part of a class action, sought to recover on an appropriation theory because of the defendant’s practice of renting cardholder information about their spending habits to other merchants. 652 N.E.2d at 1356. The defendant, American Express, successfully argued that the practice did not adversely affect the interest of cardholders under the language of the Restatement. Id. The court found that while each cardholder's name did possess value for the defendants, an individual name had value only “when it is associated with one of defendants’ lists. Defendants create value by categorizing and aggregating these names. Furthermore, defendants’ practices do not deprive any of the cardholders of any value their individual names may possess.” Id. The court rejected the plaintiffs’ appropriation claim.
Restatement approach. First, there must be an intentional intrusion into what would normally be considered an area of seclusion or privacy. Second, although intrusion claims seek to protect an individual’s subjective right to be left alone, courts have used an objective standard to assess liability. Therefore, the intrusion must be highly offensive to a reasonable person. Predictably, there has been considerable discussion over these fairly rudimentary requirements.

Plaintiffs must first have a reasonable expectation of privacy in the area allegedly violated by the defendant. While absolute and complete privacy is not necessary, there must usually be a showing that the defendant penetrated some zone of physical or sensory privacy surrounding the plaintiff. This can entail a wide variety of activity, encompassing physical intrusions on to one’s property, psychological intrusions created by reading or copying one’s mail, wiretaps, and persistent late-night phone calls. Without a reasonable expectation of privacy, the alleged intrusion does not impact one’s seclusion, which is why courts have repeatedly rebuffed plaintiffs who attempt to seek recovery for intrusion while in fairly public venues. Moreover, the plaintiff’s

219. See supra notes 215-217 and accompanying text; see also infra notes 220-221 and accompanying text.
221. See Mo. Court of Appeals v. The Jewish Hosp. of St. Louis, 795 S.W.2d 488, 504 (Mo. 1990).
223. See infra notes 224-237.
225. See, e.g., Sanders v. Am. Broad. Co., 978 P.2d 67, 69 (Cal. 1999) (holding that where elements of intrusion are proven, the cause of action is not defeated as a matter of law simply because the events intruded upon were not completely and totally private).
226. See Shulman v. Group W Prods., Inc., 955 P.2d 469, 489-90 (Cal. 1998). The Shulman court extended privacy rights much further than many courts have, finding that individuals do not lose all privacy rights merely by being at work. Id. at 490-91. This allowed an employee to state a privacy claim against a defendant who had utilized a helmet camera and audio tape recorder to tape conversations involving the plaintiff in his workplace without the plaintiff’s consent. Id. at 474-77.
228. Id. at 355.
231. See, e.g., Muratore v. M/S Scotia Prince, 656 F. Supp. 471 (D. Me. 1987), rev’d on other grounds, 845 F.2d 347 (1st Cir. 1988) (finding that passenger on cruise ship could not state privacy claim when ship’s employees took photographs of
privacy expectations must be measured in such a way so they do not encroach upon the possible rights of the defendant. 232

Second, the intrusion must be one that is objectively unreasonable and offensive. 233 While ultimately this is a question of fact, courts customarily intervene in these types of claims to determine if the alleged offensive act sufficiently states a claim. 234 No consistent litmus test exists nationwide, and courts have differed upon how the intrusion has to offend sensibilities. 235 Courts do, however, regularly consider "the degree of intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder's motives, and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded." 236 The social expectations of a society also influence an assessment of the defendant's behavior. 237

Despite the dearth of litigation over spyware, the software does contain central characteristics that courts have seen many times over: (1) Despite its rapidly evolving development, spyware is really just another form of electronic surveillance; 238 and (2) it is designed to collect information for the benefit of third-parties. 239 Both of these traits have been the subject of privacy litigation in the past, and can therefore offer some clues as to how privacy suits related to spyware may be received. 240

---

233. See infra notes 234-237 and accompanying text.
235. In Carter, the Alabama Supreme Court found that the plaintiffs properly stated a claim for intrusion upon seclusion. Id. at 1178. The plaintiffs, a married couple, stayed on the defendant's premises, unaware that a peephole had been drilled behind a mirror in their room. Id. at 1177. The plaintiffs were in various states of undress before discovering the peephole. Id. The court allowed them to state a claim even though they could not prove that anyone had actually observed them in the room. Id. at 1178-79. The court instead focused on the method of potential intrusion and allowed them to state a claim. Id. Conversely, in Galella, the former wife of President John F. Kennedy counter-claimed under an intrusion theory against a photographer who was suing her for interference with trade, and was granted an injunction against the photographer. 487 F.2d at 998. The appellate court held that the injunction was too broad, and as long as the photographer did not act in an inconspicuous manner, he had the right to take pictures of Ms. Onassis. Id.
237. Id. at 1281.
238. See O'Brien v. O'Brien, 899 So. 2d 1133 (Fla. Dist. Ct. App. 2005) (finding that a spyware program was included under legislation that ensured privacy for electronic communications).
239. See supra note 3 and accompanying text.
240. For example, in Miller v. Brooks, 472 S.E.2d 350 (N.C. Ct. App. 1996), the plaintiff-husband and defendant-wife separated after five years of marriage. The defendant made arrangements to have a surveillance camera placed in the plaintiff's home. Id. at 352. Although the plaintiff discovered the camera and
 Plaintiffs can first point to the *Restatement*, which many states follow very closely,241 for common sense support for an intrusion claim. Section 652B, in discussing intrusion upon seclusion, says that one’s seclusion can be invaded “by the use of the defendant’s senses, with or without mechanical aids, [or] by some other form of investigation or examination into his private concerns.”242 Moreover, it is the intrusion itself that makes the defendant subject to liability, making publication or any other use of the information irrelevant.243 Spyware can be classified as a mechanical aid used for the purpose of monitoring one’s Web habits. Defendants could argue that there are no “senses” used with spyware, but because the overall goal is to watch the user’s habits, spyware appears to fall within the parameters of this *Restatement* language.

For example, in *O’Brien v. O’Brien*,244 the plaintiff-husband, embroiled in a difficult break-up with the defendant, his wife, moved to enjoin her from using communications she obtained from his personal computer as evidence in their divorce proceedings.245 When the couple began having marital problems, his wife installed a spyware program on his computer without his knowledge.246 The husband had engaged in private online conversations with another woman, and the spyware program captured and recorded all of the conversations, instant messages, and e-mails sent and received by the user.247 The husband did not sue under an invasion of privacy theory, but he was able to successfully enjoin his wife from disclosing the intercepted data in their divorce proceeding, a decision that was affirmed by the Florida District Court of Appeal.248 The plaintiff alleged that the e-mails and instant messages were illegally obtained in violation of the Florida Security of Communications Act, making them inadmissible in the divorce.249 Although the court focused much of its discussion on matters of statutory interpretation, it did find the purpose of the

---

243. Id.
244. 899 So. 2d 1133 (Fla. Dist. Ct. App. 2005).
245. Id. at 1134.
246. Id.
247. Id.
248. Id. at 1137.
249. Id. at 1134.
Florida Act to be the protection of every person’s right to be free from intrusion into their private conversations and communications. Because the court agreed that the spyware-generated information was illegally obtained in violation of the Act, O’Brien can be fairly read to infer that information exchanged on the Internet is just as private as more traditional communication mediums.

O’Brien provides evidence that plaintiffs should be able to favorably compare spyware with other surveillance tools that have been deemed to violate a plaintiff’s privacy rights. In Black v. City & County of Honolulu, the United States District Court of Hawaii overturned a summary judgment motion and held that the plaintiff likely stated an intrusion claim when the defendant placed a wiretap on the plaintiff’s personal pager in potential retaliation for her filing a sexual harassment claim. In Tompkins v. Cyr, a doctor stated an intrusion claim against anti-abortion activists by showing that the defendants regularly sat on a street near the doctor’s home and watched him by using binoculars and a camera. In both cases, the defendants were unable to argue that because there was not a physical intrusion or trespass on to the plaintiff’s property, there could be no privacy claim. Similarly, spyware providers, while not physically entering the plaintiff’s domain, still may use devices that create the tortious activity. The methodologies may differ, but the objective is still the same—the surveillance of the plaintiff’s movements.

Despite the seemingly direct tie between an invasion of privacy and the primary goal of spyware, plaintiffs are still only likely to find viable claims in very specific contexts. First, plaintiffs would probably need to be in their home using their own personal computers for the best chance of recovery. As Warren and Brandeis suggested 115 years ago, “[t]he common law has always recognized a man’s house as his castle, impregnable, often, even to its own officers engaged in the execution of its commands.” Courts would likely be more receptive to the theory that a plaintiff, while in his home, using a server connection he or she believed to

250. Id. at 1135.
252. Id. at 1053-54.
254. Id. at 684.
258. See infra notes 263-265 and accompanying text.
259. Warren & Brandeis, supra note 102, at 220.
be secure, out of the view of others, had a legitimate and reasonable expectation of privacy. Plaintiffs who lose access to personal information due to spyware while on the job are likely to have more difficulty because courts have generally held that there is a reduced expectation of privacy in the workplace.

Second, plaintiffs would likely need to show they were negatively impacted by a more aggressive spyware application like the keystroke logger to be able to state a meritorious claim. Because all intrusions are not actionable, an application that merely monitors user activity is not as likely to be deemed "highly offensive" by a court. But applications like keystroke loggers are easier to categorize as such because of the surreptitious manner and conduct associated with their installation, and the generally disreputable motives and purposes of those who install them.

If possible, plaintiffs should also attempt to identify both the installer/provider of the spyware program and the party that harvested the data, and then sue both parties simultaneously. This is problematic for practical reasons because like Danielle, users often have no idea who has accessed their computer data. Moreover, many spyware providers can operate from overseas locations without difficulty, well beyond the purview of U.S. law. But ideally, a plaintiff would want to sue both installer and provider for damage purposes. Plaintiffs are typically entitled to receive general damages from harm that stems from the wrongful act and special damages from all harm that proximately results, but the dignitary harm that stems from spyware intrusions is harder.


262. See infra notes 263-264 and accompanying text.


265. See infra notes 269-275 and accompanying text.

266. See supra Part I.


to quantify.\textsuperscript{270} It is therefore unclear as to the extent of damages one could receive from the mere application of spyware programs because it is the third-party’s use of information harvested by the spyware—credit card numbers, bank account information, and Social Security numbers—that results in the most serious harm.\textsuperscript{271} Since some courts have held that such information is not private if it can be obtained from public sources,\textsuperscript{272} the mere placement of spyware may only result in nominal damages at best if all the spyware program did was provide information to a third party.\textsuperscript{273}

Without those fundamental components present in a lawsuit, bringing individual privacy claims may not be financially viable for the party who is victimized by spyware because the expense of litigation is likely to outweigh the recovery.\textsuperscript{274} Class action lawsuits could possibly yield more success against these software providers, but they too are far from a guarantee.\textsuperscript{275}

\textbf{B. Making the Case for the Defendant}

Defendants have proven to be very resilient in intrusion cases, and have received favorable results across the country in a variety of contexts where privacy violations have been alleged.\textsuperscript{276} Defendants can first contend that the Internet and World Wide Web are both, in essence, public locales, albeit in a divergent form. Users can engage in conversations online, play poker, and shop in much the same way they can in any other public venue. Because so many other people are online simultaneously, there is likely to be support for the defendant’s contention that plaintiffs cannot realistically call the Web a place of isolation or seclusion, regardless of where they are physically when they connect to the Internet.\textsuperscript{277}

\begin{footnotesize}
\textsuperscript{270} See, e.g., Mathias v. Accor Econ. Lodging, Inc., 347 F.3d 672, 676-77 (7th Cir. 2003).


\textsuperscript{273} See id. at 1018.


\textsuperscript{277} See Four Navy Seals, 413 F. Supp. 2d at 1146-47.
\end{footnotesize}
Additionally, a great deal of spyware is delivered when users seek the benefits of “free” software applications that can be downloaded without financial cost. The licensing agreements that accompany this software regularly contain language that allows the software provider to install other applications on an individual’s computer. By clicking “I accept” or “OK,” users consent to all the terms of the agreement. Plaintiffs would therefore not be able to successfully contend that they had no notice of the additional programs, despite the linguistic obfuscation that frequently characterizes these licensing agreements. With such consent, defendants can argue the subsequent activity on one’s computer is no longer secluded because by consenting to the other programs, the user has agreed to be observed, negating a central element of intrusion. Plaintiffs could conceivably argue that the consent was invalid because they were unaware of what they were agreeing to do, but that is unlikely to be convincing in most cases.

Courts have also rejected intrusion claims where defendants took previously collected information and subsequently sold it or shared it with a third party. In Dwyer v. American Express Co., the plaintiffs, as part of a class action, sued the defendants for invasion of privacy under both intrusion and appropriation theories. The defendants had a business practice of renting out lists containing its customer names and other information to other merchants and giving the merchants data about the spending habits of particular cardholders. Since this was done without the consent of the plaintiffs, they alleged this constituted an intrusion upon their seclusion. The court held that because cardholders provided the information voluntarily, the plaintiffs could not successfully argue that the intrusion was unauthorized. “Defendants rent names and addresses after they create a list of cardholders who have certain shopping tendencies; they are not

279. See id.
280. See id.
281. See id.
282. See Poe, supra note 271, at 348-50.
283. Most who use computers have gotten very accustomed to clicking “Next” or “OK” in working with new software applications. Users often do so without reading all of the language attached to the agreement. Individual carelessness with regard to accepting these terms likely trumps any argument that parties did not know to what they were consenting.
284. See supra notes 235-239 and accompanying text; see also infra notes 285-289 and accompanying text.
286. Id. at 1353.
287. Id.
288. Id.
disclosing financial information about particular cardholders. These lists are being used solely for the purpose of determining what type of advertising should be sent to whom.\(^{289}\)

The majority of spyware tools are most regularly used to determine what type of advertisements should be sent to users.\(^{290}\) Since spyware programs generally only collect data and pass it to other parties,\(^{291}\) defendants could argue that any invasion of privacy claim should fail under the logic followed in *Dwyer.*\(^{292}\) Even if plaintiffs should clear these obstacles, the level of intrusiveness must still reach the "highly offensive" threshold.\(^{293}\) Dozens of courts have rejected plaintiffs at the summary judgment stage, finding that the conduct was not "highly offensive."\(^{294}\) The combination of any or all of these arguments provides defendants with formidable ammunition in defending such claims.

In summary, one of the major obstacles to any technology-based lawsuit is the lack of complete understanding as to how the Internet operates and how its applications are changing the way people live, communicate, and relate to one another.\(^{295}\) This deficiency of appreciation is likely to produce cynicism in some legal circles with regard to these types of lawsuits. Still, the author supports the position that acknowledging such claims requires neither overhaul nor renovation of existing tort principles.\(^{296}\) With better insight into how Internet-driven applications like spyware can affect individual rights, it is likely that courts would more rapidly find invasions upon individual solitude in ways that are not in keeping with traditional paths to liability for privacy violations.

\(^{289}\) *Id.* at 1355.

\(^{290}\) See *supra* Part I(A)-(B).


\(^{292}\) See *supra* notes 285-289 and accompanying text; see also Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1009 (N.H. 2003) (rejecting plaintiff's intrusion claim where investigator provided address information to third party, who later shot and killed plaintiff's daughter).

\(^{293}\) *Restatement (Second) of Torts* § 652B (1977).

\(^{294}\) See, e.g., Plaxico v. Michael, 735 So. 2d 1036 (Miss. 1999) (finding that defendant-father's act of secretly taking nude photographs of plaintiff-mother with her lesbian lover for use at future child custody hearing did not rise to level of gross offensiveness because of his concern for minor child).

\(^{295}\) DELTA & MATSUURA, *supra* note 204, at § 1.07.

\(^{296}\) Delta and Matsuura argue that:

[The legal community] should strive to understand fully the facts associated with the development of the Internet and its associated products and services. Based on an accurate factual understanding of today's Internet and its potential capabilities, the legal community can effectively apply existing legal rights, obligations, and remedies to the network in a manner consistent with the public interest yet conductive [sic] to the Internet's ability to realize its positive commercial, social, and political potential.

DELTA & MATSUURA, *supra* note 204, at § 1.07.
CONCLUSION

When Ian Fleming’s legendary book series detailing the adventures of British super-agent James Bond started being made into movies in the 1960s, nearly every film devoted at least one scene to the “toys” Bond might need to combat his enemies.297 His briefcase alone came equipped with tear gas, a sniper’s rifle, and a flat-bladed throwing knife.298 Four small leather cases could be instantly turned into a one-man helicopter, complete with machine guns and rocket launchers.299 Bond’s watches might contain poison darts or plastic explosives.300 All of these items were typically needed to save the world on-screen, but at the time, it is doubtful even the inventive screenwriters of those 007 films could have foreseen today’s arsenal of electronic gadgets, an assortment varied enough to make de facto “James Bonds” out of otherwise ordinary people. The question still remains, however, as to whether society’s increasing dependence upon technology demands a decreased expectation of individual privacy.

To date, courts have adhered to the current four branches of privacy torts quite faithfully.301 This, however, has produced some results that at minimum, seem in considerable tension with the stated goals of this area of the law. In Busse v. Motorola, Inc.,302 for example, the plaintiffs represented a class of cellular phone users who filed suit against several defendants for acts associated with epidemiological studies investigating the connection between mortality and cellular phone use.303 Defendants Wireless Technology Research, LLC and Cellular Telecommunications & Internet Association funded two of the studies, which were completed by Epidemiology Resources, Inc. (ERI).304 To create a database, two other defendants, Southwestern Bell Mobile Systems and Comcast Cellular Communications, provided ERI with customers’ names, street addresses, cities, states, Social Security numbers, and cellular phone account numbers, among other things.305 ERI then mailed the customers a survey about their

297. See, e.g., FROM RUSSIA WITH LOVE (United Artists 1963); OCTOPUSSY (United Artists 1983).
298. See FROM RUSSIA WITH LOVE (United Artists 1963).
300. Id.
303. Id. at 1015.
304. Id.
305. Id.
cellular phone usage and published the results. The customers had not given any permission to forward the information to ERI and filed suit, using a number of theories.

The court rejected the plaintiffs' privacy claim for intrusion, finding that Social Security numbers, names, and telephone numbers were not "private" information standing alone. The court found that because such information could be found in public records, and the data was neither compromising nor embarrassing, the defendants did not violate the privacy rights of the plaintiffs. Such a finding undercuts the basic privacy rights that Brandeis and Warren advocated for so skillfully. Merely providing information for others to access in a context where it must be given in order to receive use of the product or benefit of a service does not necessarily mean the information should no longer be thought of as confidential at all. Because of the rise in identity theft, most people would consider data like Social Security numbers to be private information, and would likely not approve of the unauthorized sharing of such data. Busse offers a classic example of not being able to find the ocean because of all the water, and is illustrative of how some courts have bypassed what should be the fundamental matter of all privacy cases—whether the release of the information without the consent of the plaintiffs infringed on their individual independence.

The Minnesota Supreme Court has described the right to privacy as "an integral part of our humanity; one has a public persona, exposed and active, and a private persona, guarded and preserved. The heart of our liberty is choosing which parts of our lives shall become public and which parts we shall hold close." Courts have already recognized privacy intrusions caused by wiretaps, binoculars, and video cameras. It therefore follows that allowing claims based on spyware intrusions protects the vital interests expressed by the Minnesota Supreme Court. Recognizing such claims may require courts to expand the parameters of what privacy may mean in a society with such rapidly evolving technological capability. But it is clear that future tools will be devised to gather information about us for myriad purposes, ranging from selling cookware to consumers to

306. Id.
307. Id. at 1014-15.
308. Id. at 1017.
309. Id. at 1018.
310. See Warren & Brandeis, supra note 102.
311. See Busse, 813 N.E.2d at 1014-15, 1018.
313. See supra notes 229, 240 & 254 and accompanying text.
314. Lake, 582 N.W.2d at 235.
protecting our national security. These scientific gains, combined with our post-September 11, 2001 interest in data collection, represent considerable challenges to safeguarding the principles stated by the Minnesota Supreme Court. Still, given that the chief question in privacy claims tends to be whether the plaintiff suffered a loss of his or her right to be left alone because of a third-party’s activity, it makes sense that courts recognize claims against providers of spyware. Such lawsuits would certainly face definitive challenges, but could be illustrative of the need to see existing law through a different prism because we live in a different era.

Until then, spyware will likely continue to evolve and mutate, as programmers on both sides of the fence take turns playing leapfrog. Web browsers will keep developing software applications that block spyware, while spyware programmers will devise new methods of installation to keep their programs from being impeded. At least for now, consumers like Danielle are probably best served by taking precautions to ensure their own privacy, such as installing anti-spyware programs on their personal computers, treating free software programs with healthy skepticism, and avoiding all unsolicited advertisements and e-mail attachments. Although it may be a cliché, an ounce of prevention may indeed be worth a pound of cure.