Home Is where the Internet Connection Is: Law, Spam and the Protection of Personal Space

Andrea Slane*

THE ARTICLE EXAMINES HOW IMAGES of home internet access have informed two prominent strands in the development of anti-spam law, namely property-based and autonomy rights-based approaches. Through a comparison of legislative and common law attempts to legally articulate and address the wrongs inflicted by unsolicited bulk email in both the United States and Canada, the article traces slow and halting progress away from an exclusively property-based approach to one which considers part of the wrong to be the invasion of the personal autonomy rights of spam recipients. The internet-connected home thereby becomes a visual stand-in for the less materially bound personal space within which an individual can exert a right not to receive unwanted messages. Solutions able to address this right directly are therefore most capable of getting at the underlying popular complaint against spam, while validating a larger cultural trend toward more portable notions of privacy.

L'ARTICLE EXAMINE COMMENT LES IMAGES de l'accès Internet à domicile ont inspiré deux courants dominants dans le développement de la législation anti-pourriel : l'une fondée sur la propriété et l'autre, sur les droits à l'autonomie. En comparant les démarches prises par les législateurs et en common law, tant au Canada qu'aux États-Unis, afin d'énoncer des règles en matière des préjudices résultant de l'envoi massif de messages électroniques non sollicités, l'article décrit le progrès accompli, bien qu'à petits pas et sporadiquement, afin de s'écarter de l'approche fondée exclusivement sur la propriété et de considérer le préjudice en partie comme une atteinte aux droits à l'autonomie personnelle des récipiendaires de pourriels. Le branchement à l'Internet du domicile devient donc une sorte d'entrée visuelle dans l'espace personnel physiquement moins délimité où l'individu peut exercer le droit de ne pas recevoir de messages non désirés. Les solutions qui tiennent compte de ce droit directement sont donc plus susceptibles de régler le vrai malaise général qu'engendrent les pourriels et de nourrir le courant culturel plus vaste vers des notions de vie privée de portée plus large.

* Andrea Slane is an Associate in the National Intellectual Property Department of Osler, Hoskin, Harcourt LLP in the Toronto office.

Home Is where the Internet Connection Is: Law, Spam and the Protection of Personal Space

Andrea Slane

1. INTRODUCTION

IN THE 1998 ROMANTIC COMEDY *You've Got Mail*, the hero and heroine know one another both online and offline: they fall in love from the comfort of their separate homes in the simplified world of decontextualized text-based communications, while they do political and economic battle in the public physical world where context is everything.[1] The material drama where the corporate hero drives the small family business heroine into bankruptcy is ultimately relegated to the background and resolved through the romantic union of the store owners, made possible by an idealized, domesticated world of internet communication.[2]

The fall 2004 broadcast advertising campaign of internet service provider (ISP) America Online (AOL) features a related though very different image of internet communications. As in *You've Got Mail*, the television commercial promotes domestic space as the seat of the pleasant online experience. A woman dressed comfortably in casual clothes sits at her internet-connected home computer, situated in a well tended, middle-class single family home. Outside, a horde of unitard-clad beings run headlong towards the house, each bearing bold white lettering on its back signifying the various threats to the

1. Nora Ephron (director) & G. Mac Brown (producer), Home Video: *You've Got Mail* (United States: Warner Studios, 1998) [*You've Got Mail*].

2. The film is a remake of the 1940 film *The Shop Around the Corner*, directed by Ernst Lubitsch. In the earlier film, the lead characters exchange letters anonymously, while unbeknownst to them, they work together in a shop that sells fancy gifts. The original film does not perform the same ideological work as the remake, since both characters are originally clerks (though the hero, played by Jimmy Stewart, is the lead clerk and is promoted to manager in the course of the film). The romantic drama more centrally revolves around traditional tensions arising from gender conflict, and the desire of men to provide for their wives and wives to be economically taken care of: a theme which is not banished from the idealized love letter writing world in the way that the economic and political conflict between the characters in the remake is banished from their email correspondence (Ernst Lubitsch (director): *The Shop Around the Corner* (United States: Warner Home Video, 1940)).

woman's experience: spam, "XXX" (pornography), viruses, hackers and so forth. The horde is suddenly stopped by an invisible barrier—the figurative stand-in for AOL's various filtering and security software—just as it reaches the boundary of the home's neat green lawn. As the beings smash their faces against the transparent wall, the woman smiles, then carries on with her peaceful, domestic online activity.

This article will examine how these images of home internet access have informed two prominent strands of anti-spam law—that is, legal attempts to curtail bulk commercial unsolicited email—namely property-based and privacy rights-based approaches. While access to email has been increasingly uncoupled from particular static locations as Web and wireless technologies have evolved, the historical evolution of the legal understanding of the rights affronted by intrusive behaviours has been replicated in efforts to combat spam through legal means. The use of images of the home, in both popular and legal contexts, illustrates this historical tendency to obscure the distinction between property rights and autonomy rights. As our legal understanding of privacy rights moves haltingly away from property and toward autonomy rights, the image of home in anti-spam contexts comes to serve more as a figure for the portable autonomy interests associated with personal space. The article maps progress toward clarification of these privacy interests through the features of anti-spam law that either succeed or fail to address the personal affront of spam. These are features that derive from the right to exclude unwanted communications, an area of law that aptly illustrates the move from property to autonomy-based rights. But their evolution also derives from the right to a legal means of redress for a wrong, where autonomy interests have always been central.

Cyberspace consists of a variety of forums: some public, some private, and some in between. In his influential book, *City of Bits,* Professor of Architecture and Planning William Mitchell marked out public and private forums in 1995, noting that "Many of the places in cyberspace are public, like streets and squares; access to them is uncontrolled. Others are private, like mailboxes and houses, and you can enter only if you have the key or can demonstrate that you belong."[3] Dan Hunter has argued that the notion that cyberspace is an actual place is perpetuated by the prominent use of such place-oriented metaphors, which has had negative consequences for the legal treatment of internet phenomena. He writes that "Thinking of cyberspace as a place has led judges, legislators, and legal scholars to apply physical assumptions about property in this new, abstract space"—assumptions which, as this article will go on to argue, often limit or delay the ability of law to effectively address affronts to autonomy interests raised by internet communications.[4]

Although Hunter's discussion of the ways that analogy and metaphor operate to help us cognitively understand new phenomena is astute, there is

3. William J. Mitchell, *City of Bits: Space, Place, and the Infobahn* (Cambridge, MA: The MIT Press, 1995) at p. 23.

4. Dan Hunter, "Cyberspace as Place and the Tragedy of the Digital Anticommons" (2003) 91 California Law Review 439 at p. 443.

more to the spatial conceptualization of cyberspace than his analysis acknowledges. Metaphors of place are ubiquitous in discussions of cyberspace in large part because social phenomena are often *spatially* conceived, which should be distinguished from a phenomenon being located in a particular place. The application of the public forum doctrine to online forums, for instance, depends on the social functions that characterize the terms public and private, which only in turn correspond to places described with these terms. The close association of these social functions with places points to the spatial aspect of social relations. However, it is important to conceptually distinguish references to these spatial aspects from uses of metaphors of place, which convert the amorphous network that is the internet into something governable by place-based legal concepts, like those associated with real property. Hunter's analysis almost says as much when he writes, "The ideal of a public forum suggests a place where citizens can congregate, air their grievances, debate public policy, and be confronted with new thoughts and arguments."[5] The suggestion of a place in this instance primarily points to the social capacity to communicate certain kinds of ideas to certain kinds of audiences, rather than necessitating physical co-presence in a particular kind of located arena. Similarly, the social space of the home stands in for the types of interactions which often take place there, namely intimate communications featuring heightened levels of personal control over who will have access to this level of intimacy (the realities of domestic life notwithstanding). Mitchell's characterization of online private spaces, such as mailboxes and houses, should therefore be read as invoking these social features of the personal autonomy exercised in the home, rather than the physical place itself.

The use of the home as simile for online personal space is of course frequently confounded by the actual location of computers in physical domestic spaces. But even when the home appears as the physical locus of an internet connection, the substance of the issues raised bear much more profoundly on intangible social issues.[6] On the one hand, home internet-access further uncouples privacy values from the home *per se*, contributing to the trend toward portable personal space, less aligned with property and instead aligned with autonomy rights. On the other hand, the process of moving from property-based towards autonomy-based meanings of the home produces anxiety, relating primarily to the disaggregation of families into collections of individuals,

---

5. *Ibid.* at p. 488.

6. There are other social factors that also complicate the public/private organization of the home, especially insofar as home computing and the Internet make possible a reversal of the historical division between the home and the workplace which was brought on by the Industrial Revolution and the rise of the middle class in the 19th century. For an optimistic view of the reintegration of the home and workplace see Alvin Toffler, *The Third Wave* (New York: William Morrow & Company, Inc., 1980) at chapter 16 "The Electronic Cottage"; for a critical view see Tom Forester, "The Myth of the Electronic Cottage" (1988) 20 Futures 227.

perceived to be hastened by technological means.[7] The idealized home therefore sometimes works as an architectural image of social order, clearly marking the boundary between public and private life.[8] The internet connected home, however, cannot as clearly sustain the boundaries so fundamental to that image, and so the invocation of images of home in the internet context is fraught with contradiction.

Mitchell marks the spatial reorganization inspired by the internet as having created

> Places where you can hear and be heard, or see (on a display) and be seen (via a video camera) without completely relinquishing the privacy and controllability of the home. But these places need not be positioned (like the old urban stoops lauded by nostalgic planning theorists) at the boundary between private property and the street; they can just as easily be internal, thus restructuring the traditional public-to-private hierarchies of domestic space.[9]

While behaviour formerly contained in the home can now be broadcast to the public, so too can formerly public behaviours be experienced within the home, inspiring further social anxieties about the ways that what one does online is not subject to public scrutiny. As historian Philip Jenkins writes in his book on child pornography on the internet, "On the Internet, rules are made to be broken. This attitude is facilitated by the user's psychological sense that whatever occurs in a computer transaction takes place within his or her own private space… The attitude seems to be that it is my home, my desk, my computer, and my business what I do with it."[10] In other words, images of the internet-connected home mostly shore up the home's significance as the seat of private life, but the experience of going online is simultaneously not private enough and too private, counter-tendencies that inform the conflicts arising from spam.

A third example joins *You've Got Mail* and the AOL commercial to flesh out the consequences of spam's disruption of distinctions between public and private communications, bringing the underlying autonomy right into sharper

---

7. Another line of cultural studies scholarship examines consumer technologies that have disturbed both the home environment and public spaces by individualizing the consumption of entertainment (through the use of personal listening devices and headphones, and through handheld video games, for instance). These technologies are feared to fragment family life by detracting from collective experiences. Other concerns have been raised pertaining to the privatization of public places through the use of cellular phones and again personal listening devices, raising fears that non-interacting, self-isolating individuals will populate public spaces. See Paul du Gay *et al.*, *Doing Cultural Studies: The Story of the Sony Walkman* (London: Sage Publications, 1997).

8. For a discussion of television's impact on domestic space see Lynn Spigel, *Make Room for TV: Television and the Family Ideal in Postwar America* (Chicago: University of Chicago Press, 1992). Many films have dramatized the ways that television alters home life (for instance David Cronenberg (director), Home Video: *Videodrome* (United States: Universal Studios, 1983); Tobe Hooper (director) & David Spielberg and Frank Marshall (producers), Video: *Poltergeist* (United States: MGM, 1982); Peter Weir (director) & Andrew Niccol *et al*. (producers), Video: *The Truman Show* (United States: Paramount, 1998)); but few have dramatized the impact of internet access on home life. The short film *eMale* (Bryan Harston (director/producer), Video: *eMale* (United States: Idea Ranch, 2001)) dramatizes how the promise of recreating your home life over the internet can destroy the home life you currently enjoy.

9. Mitchell, *supra* note 3 at pp. 99-100.

10. Philip Jenkins, *Beyond Tolerance: Child Pornography on the Internet* (New York: New York University Press, 2001) at p. 97.

focus. In the fall of 2003, California computer programmer and encryption specialist Charles Booher was charged with eight counts of uttering threats of bodily injury in the course of international communications when he retaliated against a Canadian direct email marketing company he thought was spamming him.[11] The threats, uttered over email and voicemail, are undeniably graphic, promising dismemberment, castration, anthrax attacks and many more imaginative tortures.

Booher believed that the company (DM Contact Management, Inc. of Victoria, BC) and its president were responsible for sending him numerous email advertisements on behalf of another company, hawking "VigRX," a penile enlargement medication.[12] He made the calls and sent the messages sometimes identifying himself by his real name, other times mimicking the tactics of spammers, using email addresses such as Satan@hell.org, SatanLordofHell666 @yahoo.com, and Fuckyou@fuckyou.com.[13] In the course of the investigation, Booher revealed to John A. Carney, the FBI agent who filed the criminal complaint, that he uttered the threats because, as a testicular cancer survivor, he felt that the penile enlargement messages were "frustrating."[14] In other words, he took messages sent indiscriminately to millions of email account holders *personally*.[15] His case illustrates that the invasiveness of spam is not linked to the home *per se* but rather is linked to what the home stands for in the other examples above: namely, the right to protect your most intimate matters from public address, commonly grouped in legal terms under the concept of privacy.

---

11. The criminal complaint against Booher was filed in the US District Court for the Northern District of California on 19 November 2003, *United States v. Booher* (5 03 292). Booher was charged with several counts of violating 18 U.S.C. s. 875(c), <http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00000875----000-.html>, which holds that "Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both." The indictment was filed 25 November 2003, case no. CR 03 20170 JF.

12. DM Contact Management denied being responsible for these advertisements, sent on behalf of Albion Medical (also known as Leading Edge Marketing, Inc.) although some internet discussion of the case suggested that there were strong inter-connections between the companies that accounted for Booher's placing the blame with DM. See for instance, Dan Pulcrano, "Raging Against the Machine" *Metro: Silicon Valley's Weekly Newspaper* (4-10 December 2003), <www.metroactive.com/papers/metro/12.04.03/booher-0349.html>.

13. Booher, *supra* note 11 at para. 4.

14. *Ibid.* at para. 8.

15. The profile article on Booher by Pulcrano, *supra* note 12, features a photograph of Booher wearing a "Free Charles Booher" T-shirt and "No Spam" hat, and contains the following quote from a letter Booher allegedly sent to DM Contact Management's president: "I have survived testicular cancer three times. The spam messages were coming to my computer every 15 minutes in either pop up or spam form and no other spammer on the Internet is as horrible to deal with as the penis enlargement industry. If you had only sent me a few spams once in a while, and not filled my computer screen with pop up ads every 15 minutes I would not be so pissed off. I work on my computer. I do things that require concentration. I am working on real scientific research… Please… act in a responsible and ethical manner, and stop harassing people."

Booher's case was widely reported in the news media all over the world,[16] and he became an online folk hero.[17] His actions were quickly dubbed "spam rage," thereby marking them as an emblem of the larger societal frustration with spam, which, like road rage and air rage, represents an infuriating state of affairs (like traffic or travel delays) which brings some people to the point of snapping. Such "rage" behaviour is not condoned, but it is popularly perceived as understandable and sometimes cynically applauded as someone finally having the "guts" to do something about the annoying phenomenon.[18] The level of public frustration escalates the more people feel like they have no legal means to address their grievances. While legal remedies for spam are accumulating through the enactment of legislation and the initialization of civil lawsuits by ISPs (especially in the US), the individual spam recipient still feels largely powerless in the face of spam, and in particular powerless to address spam's affront to privacy.

Law is a favoured instrument for achieving social objectives, so complaints about spam from individual citizens call for a legal response. But while court decisions, legislation, and government policies attempt to address publicly articulated complaints about spam, those aspects of complaints about spam concerning personal affront and interference with personal space are largely subsumed under more dominant legal doctrines pertaining to the legal management of business relationships and the protection of property rights, especially concerning the interests of the ISP industry and the damages it suffers from spam. Personal complaints persistently resurface, however, at the margins of anti-spam cases, and are central to offences created by anti-spam statutes. As such they form a prominent subtext to law's current approach to spam.

Teasing out this subtext in Canadian and US anti-spam law allows us to assess how and why current anti-spam policies in these jurisdictions either succeed or fail to address the personal aspects of the spam problem. Surveying these regimes will enable the analysis of those features of existing and proposed

---

16. See for instance Howard Mintz, "Man Pleads Not Guilty in Spam Rage" *San Jose Mercury News* (December 12, 2003); "Upset with Spam" *Japan Times* (23 November 2003), <http://www.freelists.org/archives/computertalkshop/12-2003/msg00421.html>; "Desejo de eliminar spam pode lever homem à prisão" *Terra* (27 November 2003); "Spam Krieg eskaliert" *Politikforum* (9 March 2004), <http://politikforum.de/forum/showthread.php?s=6a09135520abed127caacc7534384e10&postid=1208712>; Adam Tanner, "Spam rage: Man arrested for threats to company" *Reuters News Service* (21 November 2003), <http://www.globalaffairs.org/forum//showthread.php?t=17696>; and Lester Haines, "US man threatens anthrax attack on spammers" *The Register* (24 November 2003), <http://www.theregister.co.uk/2003/11/24/us_man_threatens_anthrax_attack/>.

17. Pulcrano, *supra* note 12, notes that Booher lives in a "two-story, cream-colored Sunnyvale home" in a "Brady Bunch neighborhood"—a theme of domestic normalcy that pervades the article. See also discussion thread "Free Charles Booher" *Shark Blog: Current Events, Smarter Investing and Fatherhood* (25 November 2003), <www.usefulwork.com/shark/archives/001276.html>.

18. See for instance Jon Swartz, "Spam rage sparks extreme reactions" *Seattle Times* (17 February 2004). Swartz quotes anger-management expert Gilda Carle explaining the phenomenon of spam rage as inspired by the fact that "This is an invasion of personal space, intrusion with a capital I." Pulcrano, *supra* note 12, also notes in his profile

> Ok, Booher may be a little nuts, but mostly because he was crazy enough to ignore the consequences of saying aloud what many people have been thinking to themselves. And he didn't hurt anybody. He only struck a little fear in the heart of a disingenuous Canadian penis-pill spamster who's been making millions off male insecurity while damaging the Internet as a business and personal productivity resource.

anti-spam legislation which most effectively address the value of individual autonomy which informs the desire for an individual means of legal redress. The defence of this value should be a central component of any anti-spam strategy, and inattention to it is a grave but correctable flaw in Canada's current legally passive anti-spam policy. Since Canadian anti-spam policy is currently under active review,[19] the article concludes by endorsing the adoption of those features of existing anti-spam regimes that successfully address these complaints and by suggesting some guiding principles that should inform the further development of Canada's approach to the spam problem.

*

2. PERSONAL SPACE IN CYBERSPACE: THE RIGHT TO EXCLUDE UNWANTED COMMUNICATIONS

A BRIEF SURVEY OF ARTICLES ON SPAM in the late 1990s that appeared in the *Toronto Star* shows that spam was being regularly discussed in highly vexed terms such as "the most annoying aspect of the Internet,"[20] "viscerally offensive to the general public,"[21] "the equivalent of dumping untreated sewage into the environment,"[22] and "a grease stain on E-commerce."[23] Columnist K.K. Campbell writes, it is "the Net's version of the telemarketing call at dinnertime. It is an annoyance. The potential for it to become a plague is real," and "while governments try to figure it all out, people still get it. And they hate it because they don't know where it comes from, why it comes to them, and what to do about it."[24] By 2001, one *Toronto Star* writer was calling the phenomenon "public nuisance number 1."[25] Yet visions of an internet experience untainted by intrusions persist, as in the AOL commercial described above, inspiring public demands for legal interventions which will prop up the ideal of a perfectly individualized email experience and at least facilitate the development of tools to defend that private communication space.

Senator Oliver responded to this popular call to defend private communications space in his comments to the Senate of Canada upon the introduction of the first version of his bill, the *Spam Control Act.*[26] Oliver

---

19. Industry Canada, *An Anti-Spam Action Plan for Canada* (Ottawa: May 2004), <http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00246e.html>. See also two previous SPAM discussion papers: Industry Canada, *Internet and Bulk Unsolicited Electronic Mail* (Ottawa: July 1997), <http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/gv00188e.html>, and Industry Canada, *E-mail Marketing: Consumer Choices and Business Opportunities* (Ottawa: January 2003), <http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/gv00189e.html> [*E-mail Marketing*].
20. Peter Krivel, "Net Rage" *Toronto Star* (18 February 1999) at pp. K1, K8.
21. K.K. Campbell, "Web advertising in search of a model" *Toronto Star* (10 April 1997) at p. G5.
22. Myles White, "Spam ain't just mysterious pink meat" *Toronto Star* (2 October 1997) at p. H3.
23. K.K. Campbell, "'Spamming' a grease stain on E-commerce" *Toronto Star* (18 June 1998) at p. G7.
24. K.K. Campbell, "Waging war on Internet spammers" *Toronto Star* (26 August 26 1999) at p. L5.
25. Peter Krivel, "You've got spam" *Toronto Star* (28 June 2001) at pp. J1, J2.
26. The bill was most recently re-introduced as *the Spam Control Act* on 20 October 2004 (Bill S-15, *An Act to prevent unsolicited messages on the Internet*, 1st Sess., 38th Parl., 2004, <http://www.parl.gc.ca/38/1/parlbus/chambus/senate/bills/public/S-15/S-15_1/S-15_cover-e.htm> [*Spam Control Act*]).

explicitly invoked the image of the home as the locus of internet access when he said:

> I do not believe Canadians would tolerate pornographic magazine subscriptions or free edible underwear samples turning up in their traditional post each morning. I do not believe they would appreciate seeing their pre-teen daughter's name on the address box of a coupon book for diet pills and breast enhancements. I do not believe for a second Canadians would allow such damaging messages to enter their homes, yet this is precisely what occurs over the Web.[27]

This strong statement of what Canadians will not tolerate in their homes implies a right to exclude unwanted communications from the home (and the related right of parents to protect their children from exposure to materials of which they do not approve), an example of the use of images of the home as a stand in for the broader concept of personal autonomy.

The right to exclude unwanted communications derives from a number of legal sources: constitutional limits to freedom of expression and the government's power to conduct surveillance (the origins of the reasonable expectation of privacy); property-based common law rights of action (trespass and nuisance); and statutory regimes addressing specific means of communication (regulating telemarketing and of course spam itself). The interplay of these sources leads to the conceptual confusion as to whether the right to avoid spam (if there is such a right) is a property right or a human right involving the preservation of human dignity and personal autonomy. Examining each source in turn will afford an opportunity to map the shape of legal approaches to spam in the US and Canada, in order to suggest that the underlying issue remains autonomy rights, and so only approaches that take these rights into account can truly address popular complaints about spam.

2.1 Freedom of Expression, the Reasonable Expectation of Privacy and the Protection of Personal Spaces: Constitutional Law and Email Communications

The US has a long history of constitutional jurisprudence dealing with the sanctity of the home as a privileged locus of autonomy rights, justifying the limitation of the speech rights of others. Jurisprudence that deals with section 2(b) of the *Canadian Charter of Rights and Freedoms*, coming later as it does, is less specifically place-oriented and more consistently expressed in terms of human dignity and autonomy, a shift also visible in more recent US First Amendment jurisprudence dealing with communications media. The history of US thinking on the sanctity of the home is relevant to the Canadian context because the gradual American transition from place-based to autonomy-based principles in the face of evolving communications technologies helps to clarify that autonomy interests infuse images of domestically-situated internet access.

---

27. See *Debates of the Senate (Hansard)*, Volume 140, Issue 77 (24 September 2003) at 1530 (Hon. Donald H. Olivier), <http://www.parl.gc.ca/37/2/parlbus/chambus/senate/deb-e/077db_2003-09-24-e.htm?Language=E&Parl=37&Ses=2#54>.

The issue of whether a speaker has a right to address people in their homes has come up in a variety of contexts in US case law. In *Frisby v. Schultz* (1988), for instance, the US Supreme Court reversed trial and appellate court decisions which had struck down a municipal by-law that forbade picketing directed at a private residence, even when the picketers stayed on public streets.[28] O'Connor J, writing for the Court, cites numerous cases that protect the sanctity of the home, noting that "One important aspect of residential privacy is protection of the unwilling listener."[29] O'Connor J elaborates that "a special benefit of the privacy all citizens enjoy within their own walls, which the State may legislate to protect, is an ability to avoid intrusions. Thus, we have repeatedly held that individuals are not required to welcome unwanted speech into their own homes and that the government may protect this freedom."[30]

In *Rowan v. US Post Office* (1970), the US Supreme Court upheld a section of the *Postal Revenue and Federal Salary Act of 1967*, which requires businesses to remove people from mailing lists if they file a request to that effect with the Postmaster. Burger CJ, writing for the Court, held that a vendor does not have a constitutional right to send unwanted material into someone's home, and that a "mailer's right to communicate must stop at the mailbox of an unreceptive addressee," going so far as to say that "[t]o hold less would tend to license a form of trespass."[31] The idea that continuing receipt of communications after objection is a "form of trespass" illustrates the blurriness of property and personal autonomy rights in this line of cases. The home is not inviolable because it is real property, but rather because it is a location that is socially constructed to represent the domestic, intimate space of private life, where intrusions into personal space are consequently more serious affronts to personal autonomy than they are in public spaces.

The blurriness extends to the Court's controversial decision in *Federal Communications Commission v. Pacifica Foundation* (1978), where the Court found (by a narrow majority) that people have a right to avoid receiving

---

28. *Frisby v. Schultz*, 487 U.S. 474 <http://www.law.cornell.edu/supct/html/historics/USSC_CR_0487_0474_ZS.html> (1988) [*Frisby*]. This case concerned the rights of anti-abortion protestors to picket the home of a doctor who performed abortions.

29. *Ibid.* at p. 484. O'Connor J quotes *Carey v. Brown*, 447 U.S. 455, <http://justia.us/us/447/455/case.html> (1980) at p. 471 [*Carey*] for the principle that "The State's interest in protecting the well-being, tranquility, and privacy of the home is certainly of the highest order in a free and civilized society." She notes that many prior decisions have taken note of the unique nature of the home, "the last citadel of the tired, the weary, and the sick" (*Gregory v. Chicago*, 394 U.S. 111 <http://justia.us/us/394/111/case.html> (1969) at p. 125) and that "preserving the sanctity of the home, the one retreat to which men and women can repair to escape from the tribulations of their daily pursuits, is surely an important value" (*Carey, supra* note 29 at p. 471).

30. *Frisby*, *supra* note 28 at pp. 484-485. O'Connor J notes that in public spaces people must tolerate hearing unwanted speech, but, quite plainly, "the home is different" (*Frisby*, *supra* note 28 at p. 484), citing *Rowan v. United States Post Office Department*, 397 U.S. 728 <http://supct.law.cornell.edu/supct/html/historics/USSC_CR_0397_0728_ZS.html> (1970) [*Rowan*]; *FCC v. Pacifica Foundation*, 438 U.S. 726 <http://justia.us/us/438/726/case.html> (1978) [*Pacifica*]; and *Kovacs v. Cooper*, 336 U.S. 77 <http://justia.us/us/336/77/case.html> (1949). She further notes that even where the court has invalidated by-laws that enact complete bans on expressive activities like the distribution of handbills (*Schneider v. New Jersey*, 308 U.S. 147 <http://justia.us/us/308/147/case.html> (1939) or door-to-door solicitation (*Martin v. Struthers*, 319 U.S. 141 <http://justia.us/us/319/141/case.html> (1943)), the Court has consistently stressed that a person's right to distribute literature is limited to a right to distribute to those willing to receive that literature.

31. *Rowan*, *ibid.* at pp. 736-737.

unwanted speech in their homes via radio.[32] This right justifies broadcasting regulations which restrict programs containing offensive language to the later hours of the day, when most people can more readily avoid listening and when children are less likely to be in the audience. Stevens J writes for the majority that

> broadcasting—unlike most other forms of communication—comes directly into the home, the one place where people ordinarily have the right not to be assaulted by uninvited and offensive sights and sounds…although the First Amendment may require unwilling adults to absorb the first blow of offensive but protected speech when they are in public before they turn away…a different order of values obtains in the home.[33]

The home-as-sanctuary image informs both the right to exclude unwanted communications and the concern over protecting children from exposure to materials some parents find objectionable, since the Court has also held elsewhere that the presence of children in an audience does not justify stricter limits on speech in public places.[34]

The distinction between places and the social and subjective interest in privacy is better articulated in cases dealing with the Fourth Amendment right to be free from unreasonable search and seizure. The transition from a property-based notion of the protected right to a more abstract, autonomy-based notion of privacy occur from *Olmstead et al. v. United States* (1928) to *Katz v. United States* (1967).[35] In *Olmstead,* the US Supreme Court holds that a wire tap on a phone line does not violate the Fourth Amendment when government agents do not have to physically trespass onto either business or residential property to install it.[36] In *Katz,* the Court overturns the "trespass doctrine" in *Olmstead*, holding instead that a person has a reasonable expectation of privacy even in a public telephone booth, enough to require a warrant to intercept and record a telephone conversation occurring there.

The Fourth Amendment proclaims the people's right "to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures," and the reference to houses is part of what causes the interpretive confusion, since, as the *Katz* Court acknowledges, it appears to be common ground that the home is one place where the expectation of privacy generally holds. The reasoning in *Katz* depends on a change in posture toward the right

---

32. *Pacifica*, *supra* note 30.

33. *Ibid.* at p. 759. Justice Brennan's dissent argues that radio is a public forum, and the mere fact that radios and televisions are often found in homes does not turn broadcasting into a private communication. He argues that it is easy for an offended listener to merely change the channel and so "avert their ears" from the offending language.

34. *Erznoznik v. City of Jacksonville*, 422 U.S. 205 <http://supct.law.cornell.edu/supct/html/historics/USSC_CR_0422_0205_ZD.html> (1975); *Cohen v. California*, 403 U.S. 15 <http://www.justia.us/us/403/15/case.html> (1971).

35. *Olmstead v. United States*, 277 U.S. 438 <http://www.justia.us/us/277/438/case.html> (1928) [*Olmstead*]; *Katz v. United States*, 389 U.S. 347 <http://justia.us/us/389/347/case.html> (1967) [*Katz*].

36. Taft CJ writes for the Court, "The language of the Amendment can not be extended and expanded to include telephone wires reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office any more than are the highways along which they are stretched." *Olmstead, supra* note 35 at p. 465.

at issue, which protects people and their intention to preserve a communication as private rather than implicating the physical places where the communication occurs.[37] The shift in *Katz* from place-based to an autonomy-based understanding of the right to privacy is a great advance for autonomy rights and as such should be more explicitly echoed in the case law regarding the right to not receive unwanted communication.

US Supreme Court decisions dealing with media regulation and the right to exclude unwanted speech after *Pacifica* seem to be moving in the direction of autonomy rights, reinforcing those aspects of the *Rowan* decision which stress that the government's role is to empower individuals to exclude speech depending on personal tolerance and the privacy expectations of the context rather than to make decisions about which speech to exclude for everyone in a blanket manner. Hence in *United States v. Playboy Entertainment Group, Inc.* (2000) the Court struck down a provision of the *Telecommunications Act 1996* which required cable operators to ensure that they fully scrambled sexually-oriented material or else limited its transmission to night time hours (the industry practice was to partially scramble the signal, in order to entice viewers to order the materials).[38] The difference from *Pacifica* for the Court, deciding via another slim majority, was that other provisions of the Act already made signal blocking available free of charge on a household-by-household basis. Individual householders can choose not to receive the partially scrambled signals and therefore their autonomy rights are protected, making further regulation of those signals not justifiable as a protection of the individual's right to control which signals reached him over his cable account.

The US Supreme Court turned its attention to the internet quite early in the internet's history with *Reno v. ACLU* (1997), a case which dealt with a challenge to two provisions of the *Communications Decency Act of 1996* which broadly prohibited the transmission of obscene or indecent materials to minors over any of the myriad applications which utilize the internet.[39] As Timothy Wu has argued, the constitutional treatment of the internet in the *ACLU* decision

---

37. *Katz*, *supra* note 35 at p. 352.

38. *United States v. Playboy Entertainment Group, Inc.*, 529 U.S. 803, <http://www.law.cornell.edu/supct/html/98-1682.ZS.html> (2000).

39. *Reno v. American Civil Liberties Union*, 521 U.S. 844 <http://straylight.law.cornell.edu/supct/html/96-511.ZS.html> (1997) [*ACLU*]. The first impugned provision prohibited someone from initiating the transmission of "any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age." 47 USC s. 223(a)(1)(B), <http://www4.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000223----000-.html>. The second provision prohibited someone from knowingly using an interactive computer service to send any "comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs" to a particular minor, or to display such materials "in a manner available to a person under 18 years of age." 47 USC s. 223(d). The anti-spam bills proposed in Canada contain higher penalties for sending spam to children, a more specific focus than the provisions of the *Communications Decency Act*. The *Spam Control Act*, for instance, greatly increases the penalties for sending sexually explicit or fraudulent messages to children, where the spam was designed to be attractive to children, directed at an educational institution (that is not a post-secondary institution) or "directed to an address at which the sender had reason to believe children were likely to see the spam." *Spam Control Act*, *supra* note 26 at cl. 13(3). The latter restriction is too vague to be useful but the first two prohibitions have potential. An Ontario bill introduced in April 2004 by MPP Marsales as Bill 69, the *Anti-Spam Act* (Bill 69, *Anti-Spam Act*, 1st Sess., 38th Leg., Ontario, 2004, <http://www.ontla.on.ca/documents/Bills/38_

suffers from its simplification of the network into one unified "medium," when the network is actually more properly characterized by the specific features of the applications it enables.[40] As Hunter has pointed out, the Court wisely declined to explicitly apply the public forum doctrine to the internet in general "since to do so would lead to overbroad protection for some types of content"[41]—namely unsolicited email. But the Court's failure to distinguish between applications based on each application's varying expectations of privacy leads to flawed reasoning, making the decision unable to properly deploy the underlying autonomy interest at the core of the right to exclude unwanted communications.

The Court delineates the differences between the internet (as a whole) and broadcast media in order to distinguish the case from *Pacifica* and so to find that any restrictions on speech over the internet deserve the highest level of First Amendment scrutiny. Stevens J, writing for the Court, consequently makes some generalizations about the features of the internet which do not hold for every application, stating that unlike broadcast media, the risk of encountering material by mistake is remote "because a series of affirmative steps is required to access specific material," and while in broadcasting "warnings could not adequately protect the listener from unexpected program content," the same could not be said for the internet.[42] Stevens J concludes that "the Internet is not as 'invasive' as radio or television," supporting the District Court's finding that "communications over the Internet do not 'invade' an individual's home or appear on one's computer screen unbidden. Users seldom encounter content 'by accident.'"[43]

As the Court's yardstick of the invasiveness of a communication appears to measure a recipient's capacity to avoid seeing unwanted material, these observations may apply to the Web (except where deliberately deceptive practices are used), but not to spam email (where deceptive subject lines and transmission information are regularly used). As Wu has pointed out, "Junk email is invasive in ways that the World Wide Web is not, and hence *ACLU*'s simplified treatment of the internet has little resonance for anyone who suffers under an invasion of thousands of "get rich quick" schemes (and worse) in their inboxes."[44] The problem arises for the Court in trying to align the reasoning in *Pacifica*, which

---

Parliament/Session1/b069_e.htm>) [*Anti-Spam Act*], contains a similar provision at s.8(3). The US federal law, *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003*, Pub. L. No. 108-187, <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:s877enr.txt.pdf>, 117 Stat. 2699 [CAN-SPAM Act] does not contain any provisions regarding children.

40. Timothy Wu, "Application-Centered Internet Analysis" (1999) 85 Virginia Law Review 1163.

41. Hunter, *supra* note 4 at p. 491.

42. *ACLU*, *supra* note 39 at p. 867.

43. *Ibid.* at p. 869, citing the lower court decision of the District Court for the Eastern District of Pennsylvania, *American Civil Liberties Union et. al. v. Janet Reno,* 929 F. Supp. 824, <http://www.aclu.org/FilesPDFs/copa%20district%20court%20opinion.pdf> (ED Pa 1996) at p. 844.

44. Wu, *supra* note 40 at pp. 1167-1168. Wu argues that junk email legislation should more appropriately be subject to intermediate scrutiny rather than the highest level of scrutiny the Court applies here, on the basis that spam control measures are time, place and manner restrictions rather than content restrictions, or that they deal with a captive audience, or that they deal only with commercial speech.

is stated by reference to physical homes, with the issues raised by the internet, where the autonomy issues persist but are not tied to real property.

US district courts that have specifically considered the features of spam email have also declined to apply the public forum doctrine to email communications, although without much further development of the autonomy rights-based interests involved.[45] The reliance of the Courts on property rights rather than autonomy rights is largely dictated by the context of the cases, which involve the action of private companies against spammers and are concerned with the degree to which email systems owned by these companies are "quasi-public forums" rather than public forums. In *Cyber Promotions v. America Online* (1996), for instance, the District Court for the Eastern District of Pennsylvania declared that the plaintiff spammer does not have a right under the First Amendment to send unsolicited email advertisements to members of defendant ISP AOL, and so AOL is entitled to block any attempts by Cyber Promotions to do so.[46] The decision is primarily based on the dual rationale that AOL is not a state actor and that AOL's email system is private property, entitling the company to exclude any speakers it wants to.[47]

Among the factual stipulations upon which the court's decision is based is that:

> Although the Internet is accessible to all persons with just a computer, a modem and a service provider, the constituent parts of the Internet (namely the computer hardware and software, servers, service providers and related items) are owned and managed by private entities and persons, corporations, educational institutions and government entities, who cooperate to allow their constituent parts to be interconnected by a vast network of phone lines.[48]

The court consequently rules that the privately owned nature of AOL's facilities precludes Cyber Promotions' claim that the company is a state actor to whom the Constitution should apply. This characterization has a strong impact on the rights of email system proprietors to exclude messages, since the court further rejects the argument that by opening up its email system to public

---

45. *Cyber Promotions, Inc. v. America Online Inc.*, 948 F. Supp. 436 (ED Pa 1996) at p. 447 [*Cyber Promotions*], motion for reconsideration denied; *Compuserve Inc. v. Cyber Promotions*, 962 F. Supp. 1015 (SD Ohio 1997) [*Compuserve*].

46. *Cyber Promotions*, *ibid.* Cyber Promotions, the spammer, filed the suit against AOL seeking an injunction against AOL's practice of compiling all the undeliverable spam email that Cyber Promotions sent to AOL accounts and sending it back to Cyber Promotions' ISP in one bulk email "bomb," a tactic designed to compel the ISP to terminate Cyber Promotions' account. Cyber Promotions claimed, *inter alia*, that it had a right to send unsolicited email and that AOL was interfering with its freedom of expression rights.

47. Weiner J states this most adamantly upon denying Cyber Promotions' motion for reconsideration: "Because AOL is a private company and its e-mail servers are AOL's private property and because neither the Internet nor AOL's accessway to the Internet are public systems within the meaning of the First Amendment, a private company such as Cyber simply does not have the unfettered right under the First Amendment to invade AOL's private property with mass e-mail advertisements. Put another way, the First Amendment does not prevent AOL from using its PrefferedMail System to protect its private property rights by blocking Cyber's mass e-mail advertisements from clogging AOL's system and damaging AOL's reputation while at the same time not receiving any compensation whatsoever from Cyber." (*Ibid.* at p. 456).

48. *Ibid.* at p. 448.

communications, AOL had created a quasi-public forum.[49] Instead the court relies on *Lloyd Corp. v. Tanner* (1972),[50] which establishes that there is no right to speak on privately owned property open to the public (there, a shopping mall), where alternative avenues of expression exist.[51] Because corporations cannot have autonomy rights, only property rights-based aspects of the spam problem arise.

Canada has not had any cases dealing with freedom of expression rights via email nor on the internet more generally. Jurisprudence that deals with section 2(b) of the *Canadian Charter of Rights and Freedoms* is generally autonomy rights-based, and the limitation of expression rights on private property open to the public turns on the "wrongful action approach" rather then on any special protection for property rights.[52] In other words, if a Canadian approach to anti-spam policy is primarily property based, the degree to which the *Charter* will protect the expression rights of people *sending* spam emails against the property interests of ISPs—assuming email systems to be private property, as in the US—depends on whether the expressive activity can be considered to involve a wrongful action at either common law (including nuisance, defamation, inducing breach of contract and so forth) or criminal law (threats, intimidation, etc). If so, then courts are free to issue injunctions that limit expression rights, regardless of the nature of the location of the speech. If not, then expressive activity may be protected even on private property open to the public depending on other interests that government regulation seeks to protect.

Anti-spam legislation should not be based only on the property interests of email system owners, and should instead be geared to protect the autonomy and privacy interests of email recipients, the protection of which is a valuable objective. Wu similarly predicts that in the future the primary issue affecting the constitutional treatment of different internet applications in the US will be whether they are privacy-invasive or not:

> This perennial tension between privacy interests and the First Amendment seems destined to play a starring role in the story of Internet regulation. And since the Internet, as a whole, cannot be branded privacy-invasive or noninvasive, the distinction has to be made where the variability lies: the application. The tension between these two big rights seems likely to play out in a distinction between applications that in usage are privacy-invasive and those that are not.[53]

---

49. Specifically, the court rejected Cyber Promotions' argument that "by providing Internet e-mail and acting as the sole conduit to its members' Internet e-mail boxes, AOL has opened up that part of its network and as such, has sufficiently devoted this domain for public use. This dedication of AOL's Internet e-mail accessway performs a public function in that it is open to the public, free of charge to any user, where public discourse, conversations and commercial transactions can and do take place." *Ibid.* at p. 442.

50. *Lloyd Corp. v. Tanner*, 407 U.S. 551 <http://straylight.law.cornell.edu/supct/html/historics/USSC_CR_0407_0551_ZO.html> (1972).

51. *Cyber Promotions*, *supra* note 45 at p. 443.

52. See *Retail, Wholesale and Department Store Union, Local 558 v. Pepsi-Cola Canada Beverages (West) Ltd.*, 2002 SCC 8, <http://www.lexum.umontreal.ca/csc-scc/en/pub/2002/vol1/html/2002scr1_0156.html>, [2002] 1 S.C.R. 156.

53. Wu, *supra* note 40 at p. 1176.

The future of Canadian constitutional treatment of anti-spam regulation is likewise likely to turn on this tension, pointing Canadian anti-spam policy in the direction of more explicit protection of autonomy-based privacy interests.

2.2 Common Law Actions in Trespass and Nuisance: from Property to Autonomy Rights

The nature of the wrong in common law actions can be either autonomy-based or property-based. The US has led the attack on spam through common law actions, and has tilted the approach in favour of property-based approaches, although that need not be the case. The spectre of domestic space continues to haunt the US cases, but since email systems have been determined to be the property of ISPs, concerns for the protection of individual users' personal space only appear at the margins of actions generally initiated by ISPs.[54]

Property-based rights of exclusion that specifically address email have centered on ISP rights in their chattels (where the chattels are the physical facilities of the ISP).[55] Legal scholarship dealing with these cases has been critical of the apparent slippages between trespass to chattels (where damage to the interest in the chattel must be proven) and trespass to real property (where damage does not have to be proven) in the various court decisions.[56] The slippage stems from the problems associated with defining the precise chattel at issue and from distinguishing that chattel from the spatial characteristics ascribed to "cyberspace."[57]

The debate has been judicially considered by the Supreme Court of California's ruling in *Intel Corporation v. Hamidi* (2003), overturning Court of Appeal and trial court decisions, where a trespass to chattels action was brought

---

54. In *Compuserve*, supra note 45 at p. 1027, for instance, the court cited *Tillman v. Distribution Sys. of America, Inc.*, 224 A.D.2d 79 (NY App Div 1996) [*Tillman*], where "the plaintiff complained that the defendant continued to throw newspapers on his property after being warned not to do so. The court held that the defendant newspaper distributor had no First Amendment right to continue to throw newspapers onto the property of the plaintiff." So far an individual's proprietary interest in his or her inbox has not been specifically explored by any courts, since individuals generally only access the internet by subscribing to an access provider, who in turn owns the system on which the email account is based.

55. See for instance *America Online, Inc. v. GreatDeals.net*, 49 F. Supp. 2d 851 (ED Va 1999); *America Online v. LCGM, Inc.*, 46 F. Supp. 2d 444 (ED Va 1998); *America Online v. IMS*, 24 F. Supp. 2d 548 (ED Va 1998); *Compuserve*, *supra* note 45.

56. *Restatement (Second) of Torts* (1965) at s. 218.1.e states that

> The interest of a possessor of a chattel in its inviolability, unlike the similar interest of a possessor of land, is not given legal protection by an action for nominal damages for harmless intermeddlings with the chattel. In order that an actor who interferes with another's chattel may be liable, his conduct must affect some other and more important interest of the possessor. Therefore, one who intentionally intermeddles with another's chattel is subject to liability only if his intermeddling is harmful to the possessor's materially valuable interest in the physical condition, quality, or value of the chattel, or if the possessor is deprived of the use of the chattel for a substantial time, or some other legally protected interest of the possessor is affected... Sufficient legal protection of the possessor's interest in the mere inviolability of his chattel is afforded by his privilege to use reasonable force to protect his possession against even harmless interference.

As quoted in *CompuServe Inc. v. Cyber Promotions, Inc.*, *supra* note 45, at 1023.

57. Dan L. Burk, "The Trouble with Trespass" (2002) 4 Journal of Small and Emerging Business Law 27; <http://www.isc.umn.edu/research/papers/trespass-ed2.pdf> Hunter, *supra* note 4 at pp. 486-489; Mark A. Lemley, "Place and Cyberspace" (2002) 91 California Law Review 521, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=349760> at pp. 527-528.

not against a spammer, but against a labour organizer who sent about 200,000 emails to current Intel employees over the course of two years (a small amount, considering how many emails are typically sent by spammers).[58] The majority of the divided Court reversed the trend that legal scholars had lamented, confirming that no action in trespass to chattels should be available where the volume of emails is not high enough to likely cause damage to a plaintiff's computer system.

The majority decision aims to correct the drift toward making trespass to chattels provide a means of seeking redress for more intangible damages, like loss of goodwill or loss of productivity of employees. Consequently, it is unlikely that trespass to chattels would be an appropriate cause of action to seek redress for invasion of an individual user's personal space, since these are intangible wrongs. The *Hamidi* court does discuss the interests of homeowners in excluding unwanted communications however, mainly through addressing or distinguishing the line of constitutional cases discussed above.

Sliding toward concepts of real property despite efforts to clear up that confusion, Werdegar J, writing for the majority, finds that the defendant had no tangible presence on Intel's property, since he was speaking from his own home computer: "He no more invaded Intel's property than does a protester holding a sign or shouting through a bullhorn outside corporate headquarters, posting a letter through the mail, or telephoning to complain of a corporate practice."[59] Werdegar J thereby counters the US Supreme Court position in *Rowan*, which held that to not allow people to reject further mail from unwanted sources would be "to condone a form of trespass." Werdegar J thus confuses the fairly straightforward issue of whether damages must be proven in trespass to chattels actions with issues that are more real property based. The decision therefore still grapples with the problem of how to talk about the autonomy-based rights implied in trespass actions, and ultimately fails to find a coherent way to do so.

Brown J's dissent in *Hamidi* takes on the problem of domestic and personal space more directly in an effort to argue that there are some types of trespasses to chattels which do not require proof of damages. Brown J also slides back towards real property, however, by arguing that the plaintiff company is entitled to exclude whatever messages it likes, since "a private property owner may choose to exclude unwanted mail for any reason, including its content."[60] Freedom of expression of the speaker is curtailed by the "principle of respect for personal autonomy" once a recipient of a message has refused further communication.[61] Brown J's observations draw the analogy described at the start of the paper between a company's interest in its computer system with a

---

58. *Intel Corporation v. Hamidi*, 71 P.3d 296 (Cal Sup Ct 2003) [*Hamidi*].
59. *Ibid.* at p. 312.
60. *Ibid.* at p. 314. Brown J cites *Rowan*, *supra* note 31; *Frisby*, *supra* note 28; *Pacifica*, *supra* note 30; and *Tillman*, *supra* note 54, among other cases that establish that individuals are not required to welcome unwanted speech into their homes. Brown J also cites *Loving v. Boren*, 956 F. Supp. 953 (WD Okla 1997), where the University of Oklahoma was held to be entitled to restrict the use of its computer system to exclude pornographic messages.
61. *Hamidi*, *supra* note 58 at p. 318.

householder's interest in his home, where the home represents a locus of heightened expectation of respect for principles of personal autonomy which includes a right to exclude unwanted communications.

The problem with both the majority and dissenting positions in *Hamidi* is that they have difficulty articulating the interest wronged by unwanted email, and whether this wrong is properly addressed by an action in trespass to chattels. As argued in the above section, the personal autonomy interest violated by the ongoing receipt of unwanted communications is heightened in the location of the home, but the property interests vested in private property should not be substituted for the underlying autonomy interest. Brown J comes close to stating the problem this way, but is constrained by the property-based trespass to chattels action before the court. The majority is right to conclude that trespass to chattels is not the appropriate legal wrong to use to make such a claim, but the decision as written does little to clarify the interest at stake.

Several legal scholars have suggested that actions in nuisance could provide a ground for redressing the annoying aspects of spam in a manner more cognizant of the multiple interests involved.[62] Mark Lemley, for instance, notes that

> under the law of nuisance, certain more intangible intrusions onto private space—the playing of loud music next door, say, or the emission of pollutants—are only actionable if the harm they cause the property owner exceeds the benefits associated with the conduct. … [I]t would allow us to ask whether, in the context of the Internet, the defendant's conduct intrudes on some fundamental right we want to confer on the owner of a web server.[63]

Among the factors considered in a nuisance action is the social value that the law attaches to both the type of use or enjoyment of property invaded, and to the purpose of the defendant's conduct.[64] While there has been but one case to date where a court has considered the liability of a spammer in nuisance, nuisance actions could potentially take into account the plaintiff's autonomy interests as a factor in the assessment of the intrusion.[65]

Some conceptual difficulties remain in the use of nuisance to address spam, in particular the muddiness of who suffers the harm (the ISP or the individual email user) and whether a proprietary interest in either real property or chattels is necessary to claiming that harm. If so, individual spam email

---

62. Steven Kam, "Intel Corp. v. Hamidi: Trespass to Chattels and a Doctrine of Cyber-Nuisance" (2004) 19 Berkeley Technology Law Journal 427; Jeremiah Kelman, "E-Nuisance: Unsolicited Bulk E-Mail at the Boundaries of Common Law Property Rights" (2004) 78 Southern California Law Review 363; Adam Mossoff, "Spam—Oy, What A Nuisance!" (2004) 19 Berkeley Technology Law Journal 625, <http://btlj.boalt.org/data/articles/19-2_spring-2004_1-mossoff.pdf>.

63. Lemley, *supra* note 57 at p. 540.

64. *Restatement (Second) of Torts*, *supra* note 56, ss. 827-828.

65. *Parker v. C.N. Enterprises & Chris Nowak*, No. 97-06273 (Tex Dist Ct Travis County, 10 November 1997) at para. 5. The case involved a spammer's use of the plaintiff's domain name as a return address so that

> Because many thousands of the Internet addresses were not valid addresses, thousands upon thousands of copies of junk mail were "returned" to Ms. Parker and her business associates ... This massive, unwanted delivery of the Defendants' garbage to the Plaintiffs' doorstep inflicted substantial harm, including substantial service disruptions, lost access to communications, lost time, lost income and lost opportunities.

recipients will not likely be able to claim nuisance, since, as described above, most do not hold actual proprietary interests in the server space which houses their inboxes, though they certainly hold a social, autonomy-based interest in the privacy of that inbox.

Some legal scholarship has continued to map the nuisance of spam via the proprietary interests in the home. Jeremiah Kelman, for instance, writes that

> More than any other virtual space on the Internet, the inbox has an exclusive quality (at least in the perception of Internet users) comparable to the absolute dominion traditionally bestowed on one's home.[66]

Since excessive telephone calling has been deemed to constitute a nuisance,[67] Kelman reasons that "the inbox can be viewed either as a fixed (or at least, semi-fixed) conduit into real property or an inherent part of residential use itself."[68] While this reasoning more clearly highlights the centrality of the protection of personal space to complaints about spam, it shifts too far in the direction of property rights and away from autonomy interests. It remains unclear whether nuisance law is useful to expressing autonomy interests at some distance from property interests.

The creation of an individual cause of action in nuisance in the Oliver and Marsales anti-spam bills in Canada seems to suggest just such an independent, non-property-based variation. The provisions in the federal[69] and provincial[70] bills are nearly identical, both versions creating an individual cause of action in nuisance for sending quantities of email causing "significant inconvenience." While the bills themselves do not offer up any explanation for why nuisance would be the chosen type of action, Oliver's comments to the Senate quoted above make it clear that the protection of autonomy interests reflected in the sanctity of domestic space is certainly among his motivations for introducing the bill.

While Canada has not seen any trespass or nuisance actions against spammers so far, Canada does have a stronger jurisprudence pertaining to the right to go about one's business in peace than the US, which may contribute to a less property-based and more personal rights-based approach to nuisance.[71] The "collective right of every subject to peace and tranquillity" has been discussed by the Supreme Court of Canada in *R. v. Lohnes* (1992),[72] a case

---

66. Kelman, *supra* note 62 at p. 372.
67. *Wiggins v. Moskins Credit Clothing Store*, 137 F. Supp. 764 (ED SC 1956); *Macca v. Gen. Tel. Co. of the Northwest*, 495 P.2d 1193 (Oreg 1972); *Brillhardt v. Ben Tipp, Inc.*, 297 P.2d 232 (Wash 1956).
68. Kelman, *supra* note 62 at p. 389.
69. *Spam Control Act*, *supra* note 26, s. 17.
70. *Anti-Spam Act*, *supra* note 39, s. 12.
71. The landmark case on disturbing the peace in the US is *Cohen v. California*, *supra* note 34, , where a man was charged for wearing a jacket bearing the message "Fuck the Draft" in a courthouse where women and children were present. The US Supreme Court concluded that a written message did not amount to speaking "in a loud and boisterous manner" despite the possible offence to those who read it, and so the audience was not captive and offended individuals could avert their eyes. The case has subsequently been interpreted more broadly to mean that individuals must tolerate the offensive speech of others in a public place. *Rosenfeld v. New Jersey* 408 U.S. 901, <http://justia.us/us/408/901/case.html> (1972).
72. *R. v. Lohnes*, [1992] 1 S.C.R. 167 at 172 <http://www.lexum.umontreal.ca/csc-scc/en/pub/1992/vol1/html/1992scr1_0167.html>.

dealing with the degree of outwardly manifested disturbance required to qualify for the criminal charge of "causing a disturbance."[73] While this is clearly a different legal context, the fact that the interpretation of this section of the *Criminal Code*, later upheld in the face of a s. 2(b) *Charter* challenge,[74] protects people from interference with their "normal activities" even in public places speaks to strong support for the underlying value of personal autonomy manifest in a right to be left in peace.[75]

The only Canadian case dealing with spam is *1267623 Ontario Inc. v. Nexx Online Inc.* (1999), a rather singular case revolving around the question of whether ISP Nexx Online was entitled to terminate service to the numbered company which had been sending spam.[76] The contract between the parties required subscribers to adhere to generally accepted principles of "netiquette," which the court essentially interpreted to mean polite behaviour or "good neighbour principles."[77] The invocation of neighbourliness implies adherence to social norms which nuisance actions are designed to legally enforce, but it also implies the more intangible ways that neighbours should respect the rights of others to peace and tranquility—a more autonomy-rights-based concept. While this case is certainly not strong precedent for much of anything since it revolves around such a fine contractual point, Wilson J (of the Ontario Superior Court of Justice) appears again to be grasping for a way to legally express the personal interests which are affronted by spam.

Since the common law has not been particularly helpful so far in articulating the personal interests at stake in the face of spam, statutory regimes, whether existing or specially created, emerge as the primary hope for legal articulation and redress of these more personal features of the spam problem.

2.3 Statutory and Regulatory Regimes that Protect Interests in Personal Space

Analysts of consumer culture have characterized the evolution of some recent consumer technologies as a struggle between advertisers and consumers, where the advertiser strives to find new strategies to capture the attention of consumers,[78] even if only for a few seconds, while consumers strive to find ways to avoid advertising, including purchasing devices that help them do so.[79] A

---

73. *Criminal Code*, R.S.C. 1985, c. C-46, <http://laws.justice.gc.ca/en/c-46/42339.html>, s. 175(1)(a)(i).
74. *R. v. Lawrence* (1992) 74 C.C.C. (3d) 495 (Alta. Q.B.), aff'd (1993) 81 C.C.C. (3d) 159 (Alta CA), leave to appeal to S.C.C. refused, [1993] 3 S.C.R. vii.
75. McLachlin J (as she then was) describes an important limit on the parameters of the right to be left in peace, where she states that the purpose of the *Criminal Code* provision is "not the protection of individuals from emotional upset, but the protection of the public from disorder calculated to interfere with the public's normal activities" (*R. v. Lohnes, supra* note 72 at p. 179). The right to go about your business in peace extends into the home, as in the case where a woman had to go into her house to calm down her children when a neighbour was making a ruckus outside (*R v. Swinimer* (1978) 40 C.C.C. (2d) 432 (NS CA)).
76. *1267623 Ontario Inc. v. Nexx Online Inc.* (1999) 45 O.R. (3d) 40 (SCJ).
77. *Ibid.* at p. 45.
78. Advertisers are aware that television viewers often walk away from the television during the commercials, for instance, and so the sound volume of commercials is much higher than that of the programs, in an effort to force viewers to hear their message even if they've gone to the kitchen or the washroom.
79. Part of the appeal of the videocassette recorder, for instance, is that a consumer can fast forward through the commercials in taped television programs, a feature that also makes digital television appealing.

related trend in advertising strategies is to capture the attention of consumers when they are a captive audience, via place-based advertising at bus stops, on movie theatre screens, and in the stalls of public washrooms. Other strategies attempt to reach a consumer personally, through mail or telephone calls to residential homes, and so to garner the attention of consumers for at least as long as it takes to figure out what the message is and to discard it. Spam appears in this context as an extension of these larger trends, reaching an internet user both personally through his or her email account and at a captive moment, sitting in front of the computer screen.[80]

The statutory regimes regulating telemarketing, as well as the US Postal Service regime upheld in *Rowan*, discussed above, most overtly invoke the sanctity of the home as a rationale for intervening in advertisers' struggle for consumer attention. These regimes convert the cultural value of personal autonomy inhabiting domestic space into a statutory right to be left alone by persistent advertisers. To this end, telemarketing restrictions in both the US and Canada limit the hours within which telephone solicitations can be made, require marketers to maintain do-not-call lists when recipients request not to be called again, and, most powerfully, establish a National Do Not Call Registry in the US, or the framework for a Do-Not-Call Registry in Canada, where a telephone subscriber can place his or her number on a master list containing numbers which telemarketers are forbidden to call.[81] The rationale for these restrictions, as stated in the *Telecommunications Consumer Protection Act of 1991*, is "to protect residential telephone subscribers' privacy rights to avoid receiving telephone solicitations to which they object."[82] The reference to privacy rights here is the autonomy-based right to be left in peace that haunts the constitutional and common law approaches above, which here, as in these other legal contexts, is closely associated with the home, but not identical to the property rights vested there.

The US Federal Communications Commission's (FCC) website for the National Do-Not-Call Registry prominently foregrounds the disruption to home and family life caused by dinnertime telemarketing calls, as is graphically illustrated by the logo for the Registry, which features a receiver lifted off of a telephone shaped like a single family home.[83] Other illustrations on the FCC

---

80 For an analysis of the trends in other forms of advertising besides on the internet, see Matthew P. McAllister, *The Commercialization of American Culture: New Advertising, Control and Democracy* (Thousand Oaks, CA: Sage Publications, 1996).

81. In Canada, see Telecom Decision CRTC 94-10, <http://www.crtc.gc.ca/archive/eng/decisions/1994/DT94-10.htm>, Order CRTC 2001-194, <http://www.crtc.gc.ca/archive/eng/orders/2001/O2001-194.htm>, and Bill C-37, *An Act to Amend the Telecommunications Act, R*.S.C. 2005, c. 50, <http://www.parl.gc.ca/38/1/parlbus/chambus/house/bills/government/C-37/C-37_3/C-37-3E.html>, which received royal assent on 25 November 2005 [not in force]; in the US, see *Telecommunications Consumer Protection Act of 1991*, 47 U.S.C. 227, <http://uscode.house.gov/download/pls/47C5.txt>.

82. 47 U.S.C. 227 (c)(1), <http://www.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000227----000-html>. Upon filing the first state suit for violation of the National Do Not Call Registry, the office of the California Attorney General stated that "it's our intention to protect the privacy rights and family time of the millions of Californians who signed up for the registry" ("State Sues Hayward Company in Enforcing Do-Not-Call Law, 44 Complaints Have Been Filed Against American Home Craft" *The Mercury News* (7 November 2003) 1E).

83. Federal Communication Commission National Do-Not-Call Registry website, <https://www.donotcall.gov/default.aspx>.

website feature a nuclear family eating a meal while the mother reaches for the phone, next to the caption:

> Has your evening or weekend been disrupted by a call from a telemarketer? If so, you're not alone. The Federal Communications Commission (FCC) has been receiving complaints in increasing numbers from consumers throughout the nation about unwanted and uninvited calls to their homes from telemarketers.[84]

Canada, on the other hand, does not have a similar national registry, instead only requiring individual marketers to maintain lists of people who, upon talking to a telemarketer at least once, have requested not to be called again. This method places the enforcement burden on consumers, who must record their requests and keep track of further calls in order to determine if the same people are calling again. In both regimes, the hours of call restrictions themselves are not designed to protect family time (since calls are not forbidden during dinner hours) but rather merely to protect people when they are likely to be asleep. While the Canadian Radio-television and Telecommunications Commission (CRTC) has not chosen to implement regulations that more explicitly protect domestic space and family time, the *Telecommunications Act* clearly permits regulations which protect the underlying autonomy rights at issue, as long as they are designed "to prevent undue inconvenience or nuisance, [and] giv[e] due regard to freedom of expression."[85]

The telemarketing regime is able to articulate the affront to autonomy interests which telemarketing shares with spam, that is, the violation of privacy understood as a zone of tranquility which is often, though not necessarily, associated with the home. Of course, the telemarketing regime lends itself to the clear articulation of these interests since it applies only to residential phone lines which require a person to answer the phone at a particular time and location. While ISP access services still distinguish between residential and business services, accessing one's inbox is not confined to the home and receipt of email is not disruptive of other activities. The statutory anti-spam regimes enacted in the US and proposed in Canada consequently have a more tenuous connection with the image of family time within the home, although the underlying autonomy interests at the core of both problems are related.

Parallels between telemarketing and spam continue to inspire legislative solutions to spam modelled on the telemarketing regime. The popularity of the National Do-Not-Call Registry led US legislators to include a mandate to study the viability of a Do-Not-Email Registry in the *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003* (CAN-SPAM Act), built on the same model.[86] The potency of the parallel apparently also led Senator Oliver to

---

84. Federal Communications Commission National Do-Not-Call Registry website, <http://www.fcc.gov/cgb/donotcall/>.

85. *Telecommunications Act,* 1993, c. 38, <http://laws.justice.gc.ca/en/T-3.4/105521.html>, s. 41. The reference to nuisance here appears to lean towards the autonomy-based rather than property-based variant, serving once again as a marker for a wrong against the right to be left alone.

86. CAN-SPAM Act, *supra* note 39, s. 9.

include the creation of a Canadian "no-spam list" in his anti-spam bill, but, unlike the US legislation, Oliver's bill does not require a government commission study.[87] The fact that parallel solutions are being suggested speaks to the at least conceptual similarity perceived between telemarketing calls disturbing home life and the more portable interest disturbed by unsolicited commercial email. After conducting the mandated study, however, the US Federal Trade Commission (FTC) advised against the implementation of a Do Not Email registry at this time, noting that "in light of the current lack of authentication, [it] would be costly, potentially counter-productive, and without any appreciable benefit from spam reduction or increased law enforcement capabilities."[88]

The appeal of these registries is that they allow individuals to categorically reject unsolicited commercial calls or emails before a marketer even makes first contact. In other words (if it works), the registry fortifies the boundaries around the home as personal space (in the case of telemarketing) and the inbox as personal space (in the case of email), and so more clearly demarcates the division between public and private space.[89] A similarly boundary-fortifying result is achieved by requiring telemarketers and senders of commercial email to obtain prior consent from individuals, an "opt-in" regime such as that currently in place in the European Union, which further de-locates the right at issue from the home and more properly orients it as an individual autonomy right.[90] Some US states also implemented an "opt-in" regime in their anti-spam legislation, but these provisions are now superseded by the CAN-SPAM Act's "opt-out" regime, which is still based in the principle of autonomy rights, though in a weaker form.

In other words, with an opt-out regime, the boundaries around personal space are more permeable. The opt-out features of the CAN-SPAM Act, many of them replicated in the bills in Canada, require that each unsolicited commercial

---

87. *Spam Control Act, supra* note 26, s. 8.

88. Federal Trade Commission, *National Do Not Email Registry: A Report to Congress* (June 2004), <www.ftc.gov/reports/dncregistry/report.pdf>, at p. 34.

89. *Spam Control Act, supra* note 26. Senator Oliver's *Spam Control Act* (Bill S-15) is not merely addressed to unsolicited commercial email, but rather applies to all unsolicited email. Non-commercial email can also cause intrusions into the domestic ideal, and indeed filtering software is not designed to distinguish commercial from non-commercial email. However, since other forms of speech are more central to core freedom of expression values than commercial speech, the US has chosen to limit application to commercial solicitations. The National Do-Not-Call Registry has come under constitutional scrutiny in *Mainstream Marketing Services Inc. et al. v. Federal Trade Commission*, 358 F.3d 1228 (Memorandum and Order filed by US District Court for Colorado, 25 September 2003), where its limited application to commercial solicitations (exempting charitable and political solicitations) has resulted in the court ruling declaring that the distinction is contrary to the First Amendment. Nonetheless, the court reiterates the substantial government interest "in protecting the well-being, tranquility, and privacy of the home" which is "of the highest order in a free and civilized society" (citing *Frisby v. Schultz*, *supra* note 28, in turn citing *Carey v. Brown*, *supra* note 29) but finds that unlike the statutory regime at issue in *Rowan*, individuals are not given "unfettered discretion" to reject speech, and so the government has gotten into the business of content discrimination. It should be noted that some non-commercial unsolicited email violates other public policies, for instance spam used to disseminate hate speech. See David McGuire, "German-Language Spam Bears Racist Message" *The Washington Post* (11 June 2004), <http://www.washingtonpost.com/wp-dyn/articles/A34391-2004Jun11.html>.

90. The European Union's opt-in regime includes limited exceptions for pre-existing business relationships: EC, *Council Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*, [2002] O.J. L. 201/37, <http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf>, art. 13.

email contain a mechanism for requesting not to receive any further email from that sender.[91] As other commentators have pointed out, the result is that a spammer can legally send at least one email to every inbox, a feature which effectively affords no protection at all to recipients, since spammers can easily avoid appearing to send repeat emails from the same source.[92] The right to exclude unwanted communications is thus a limited right (similar to its formulation in the postal statute at issue in *Rowan*), that is, a right to decline further mail from the same source.[93]

The right to exclude unwanted communications is also indirectly protected by those provisions of the Act that require spammers to conform to a set of prohibitions and requirements, including prohibitions on false or misleading transmission information and deceptive subject headings,[94] and the requirement that each message provide "clear and conspicuous identification that the message is an advertisement or solicitation."[95] Further, specific labels are required for sexually-oriented materials.[96] The latter requirement is scaled back from some of the state statutes (and other proposed US federal legislation), which required that all unsolicited commercial emails bear the label "ADV,"[97] indicating an advertisement. These prohibitions and requirements are designed to assist the recipient in discarding messages that he or she does not want to open, and to more effectively implement spam filtering software to prevent unwanted messages from reaching the user's inbox at all. The decision to not require consistent labels on all commercial messages consciously eliminates the

---

91. CAN-SPAM Act, *supra* note 39, s. 5(3)(a).

92. Gary Miller, "How to Can Spam: Legislating Unsolicited Commercial E-Mail" (2000) 2 Vanderbilt Journal of Entertainment Law & Practice 127; Jacquelyn Trussell, "Is the CAN-SPAM Act the Answer to the Growing Problem of Spam?" (2004) 16 Loyola Consumer Law Review 175; Amit Asaravala, "With This Law, You *Can* Spam" *Wired News* (23 January 2004), <http://www.wired.com/news/business/0,1367,62020,00.html>; "United States set to Legalize Spamming on January 1, 2004" *The Spamhaus Project* (22 November 2003), <http://www.spamhaus.org/news.lasso?article=150>; Tom Spring, "Why Spammers Love the CAN-SPAM Law: Antispam laws make some spamming legal and do little to quell the onslaught" *PC World* (19 January 2004), <http://www.pcworld.com/resource/printable/article/0,aid,114363,00.asp>. For a discussion of these criticisms, see Mossoff, *supra* note 62 at pp. 636-637 and Kelman, *supra* note 62 at pp. 375-377.

93. CAN-SPAM Act, *supra* note 39, s. 2(b)(3). These provisions have been criticized, due to the widespread popular wisdom that it is unwise to ever respond to spam, since doing so tips off the spammer that he or she has reached a live target. Thus, while the opt-out regime conforms to the limited right to exclude *further* communications as discussed above, in practice it might make recipients vulnerable to abuse by unscrupulous spam marketers.

94. *Ibid.*, s. 5(a)(1) and (2).

95. *Ibid.*, s. 5(a)(5)(A)(i).

96. *Ibid.*, s.5(d)(1)(A). The Federal Trade Commission adopted a rule on 19 May 2004 that the warning "SEXUALLY-EXPLICIT-CONTENT" must be included in the subject line or the body of spam messages that contain such content (16 C.F.R. Part 316). If the label only appears in the body of the message, then the recipient must not be confronted with explicit images upon opening the message but must instead engage in further affirmative steps to view such material (CAN-SPAM Act, *supra* note 39, s. 5(d)(1)(B)).

97. State statutes that prescribed an "ADV" label included Alaska, Arizona, Colorado, Illinois, Indiana, Kansas, Maine, Michigan, Minnesota, Missouri, Nevada, New Mexico, North Dakota, Oklahoma, Pennsylvania, South Dakota, Tennessee, Texas, and Utah. For a complete list of state spam statutes see <http://www.spamlaws.com/state/summary.html>. The proposed federal *Restrict and Eliminate the Delivery of Unsolicited Commercial Electronic Mail or Spam Act of 2003* (REDUCE Spam Act) (H.R. 1933), <http://www.govtrack.us/congress/bill.xpd?bill=h108-1933>, would have included the ADV labelling requirement (s. 4(a)(1)(B)). The CAN-SPAM Act did require the Federal Trade Commission to deliver a report on subject line identifiers like "ADV" within eighteen months to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Energy and Commission (CAN-SPAM Act, *supra* note 39, s. 11(2)).

individual's capacity to categorically refuse to receive these messages—a decision in favour of marketers who complained that consumers should not be able to so easily insulate themselves from commercial messages as a whole.[98]

Nonetheless, the CAN-SPAM Act does provide individuals with some concrete tools with which to exercise their somewhat limited right to exclude unwanted communications from the perceived personal space of their inboxes. So while the Act comes nowhere close to preserving the idealized world of perfectly private email communications depicted in *You've Got Mail*,[99] the statute acknowledges that individuals should be given some means to manage the "assault" of marketing messages which the Act's full title names, and which is portrayed in the AOL commercial described at the beginning of this article.

Whether the Act actually achieves the promise of its long title has been hotly contested, although effectiveness is surely not the only function that legislation serves. Nonetheless, providing a means of redress for complaints of personal affront should be one of its aims, and so the next section of the article will examine anti-spam legislation's enforcement mechanisms, in order to assess how well they enable individuals to legally address complaints about the personal affront of spam.

*

3. SPAM'S PERSONAL AFFRONT AND THE CALL FOR AN INDIVIDUAL MEANS OF REDRESS

ADVERTISING OFTEN RIDES THE EDGE of personal space—addressing people in public about their intimate problems and suggesting products to solve them. Historically, controversies over advertising have often focussed on the impropriety of public discussions of such matters as personal hygiene, constipation, menstruation, incontinence and all manner of sexuality.[100] Spam, because it mimics personal, intimate modes of address, marks a new chapter in these sorts of controversies: while public advertising like billboards and subway car placards bring private matters into public spaces, spam confounds the boundaries between public and private spaces by pretending to be private conversation, thereby belying its mass marketing design.

Through an orchestrated collection of lawsuits, all filed the same day (9 March 2004) in various district courts in the US, the ISP industry launched an aggressive campaign against spamming practices.[101] One of the striking features

---

98. For a discussion of the feared impact of such a requirement on legitimate commercial email, see Joseph P. Kendrick, "'Subject: ADV:' Anti-Spam Laws Force Emerging Internet Business Advertisers to Wear the Scarlet 'S'" (2003) 7 Journal of Small & Emerging Business Law 563 at pp. 573-575.

99. *You've Got Mail*, *supra* note 1.

100. See for instance Juliann Sivulka**,** *Stronger than dirt: a cultural history of advertising personal hygiene in America, 1875 to 1940* (Amherst, NY: Humanity Books, 2001); Jackson Lears, *Fables of abundance: a cultural history of advertising in America* (NY: BasicBooks, 1994); McAllister, *supra* note 80.

101. While the suits vary to some extent, they each mobilize a long list of common law and statutory complaints, including violation of the CAN-SPAM Act. Among the other causes of action cited are violations of the *Computer Fraud and Abuse Act*, various state statutes, civil conspiracy or conspiracy to engage in unlawful conduct, trademark infringement, trespass to chattels, and unjust enrichment.

of some of these lawsuits is the way that they are able to bring the invasion of the personal spaces of ISPs' customers before the courts, although the cause of action itself is not able to address this type of affront directly. In *AOL v. Hawke el al. and John Does 1-50,* for instance, the exhibits attached to the complaint appear to be chosen to amply illustrate the highly personal nature of both the products and the mode of address employed by the spammers.[102]

The emails promoting penis enlargement treatments, of which five examples are included in the exhibits, pitch their products in decidedly personal ways, using a format which is clearly designed to create a false intimacy with the recipient and manipulate his insecurities. The examples consist of two variations, both written as if from a friend, containing testimonial accounts. One recounts that after taking the product and growing three inches in two weeks, the writer exacted revenge on his ex-wife who, he says, left him because his penis was too small. The revenge consists of seducing her, giving her pleasure with his newly resized member, and then kicking her unceremoniously out of bed and out of his life. The other version is less mean-spirited, and basically narrates how the new size improves relations with his girlfriend. Other spam emails included in the exhibits also employ this personal style, those promoting weight loss products, for instance, confessing to having tried many diets but finally finding that this product works.[103]

What AOL deemed the most representative examples acutely demonstrate the paradox of spam: that the mode of delivery is completely impersonal and indiscriminate (the spammer sending out huge quantities of messages to often randomly-generated addresses), while the contents of the messages are extremely personal. Indeed, the types of products most often promoted via spam attempt to capitalize on the personal character of email. The products either address personal insecurities (sexual dysfunction and body image enhancement via sexual parts enlargement or weight loss), debt relief, self-image (bogus university degrees), interpersonal distrust and insecurity (spying devices, ways to steal passwords or investigate people) or sexuality (pornography). These products address people's insecurities or hidden desires—the kind of stuff you either wouldn't want to share with strangers (or anyone but

---

102. *America Online, Inc v. Hawke and John Does 1-50* (US Dist Ct ED Va) Civil Action No. 04-259-A. In another AOL lawsuit, the exhibits included with the statement of claim consist of three spam email examples sent to AOL account holders, each of which represents a particular kind of personal affront: one is pornographic (the subject line reading "Drunk College Girls Get Done Hard"), another one deceives recipients into thinking the sender is a personal associate (the subject line reading "Hey there my friend…" while the text of the message reads "Need a loan?"), and one falsely purporting to be from AOL itself ("Important message from AOL") (*America Online, Inc. v. John Does 1-40* (US Dist Ct ED Va) Civil Action No. 04-260-A).

103. False sender information and subject headings also often pretend to established friendships, with subject lines like "Hi" or "Hello" or "Have you seen this?" and purporting to be from "Mike" or "Sue."

the closest of friends) or indeed with anyone but strangers (*i.e.* due to internet communications' perceived anonymity, the transaction occurs in secret, so nobody who matters knows).[104]

Spam marketing is all about temptation—to indulge in either morally questionable activities (spying, obtaining false credentials, and viewing some types of porn) or to secretly remedy a felt inadequacy (whether physical or financial). Aimed at a generic Western consumer culture prone to overspending, overeating, a sense of personal inadequacy and paranoia, these products are bound to strike a chord with some recipients—either inspiring them to purchase these products or escalating the sense of affront.

Aside from the small percentage of recipients who succumb to these pitches, a much larger group finds at least some of these materials offensive or, as in Charles Booher's case described at the beginning of this article, even emotionally hurtful.[105] Booher's story is motivated by this affront, but it is also propelled by his frustration over his own powerlessness, his inability to find an effective means to redress his complaint. Booher's case reveals the tension between mass mailing and the personal nature of the inbox: Booher took the spam emails he received personally (in particular, the ones selling penis enlargement potions), found an individual and a company to blame, and retaliated in kind. He read the increase in spam volume in his inbox to be a sign of engagement by his adversary. His adversary called the police.

Booher's actions represent an effort to make his complaint conform to a more conventional modern narrative, where a foe is identifiable and direct conflict is possible. The messages therefore symptomatically repeat the full name of Doug Mackay, the president of the Victoria email marketing company he targeted, the repetition making up for the otherwise mostly unidentifiable origins of spam messages. One email, for instance, threatened the following:

> I am going to slam a 10cm ice pick into your left ear…as the ice pick pushes through into your brain Doug Mackay it will cause damage that might kill you, or will more likely maim you causing brain damage such as loss of control over the right side of your body, seizures, and with luck a neuro-surgeon from the fine Canadian health care service will be able to get the bleeding stopped. If

---

104. For an early example of concern over the manipulations that motor marketing, see the classic study by Vance Packard, *The Hidden Persuaders* (NY: David McKay Co., 1957), which includes an account of how manufacturers create markets for products that address human insecurities (regarding body odor, bad breath, household cleanliness) or that play on other anxieties (pain medications for hypochondriacs or people who don't like to go to doctors, for instance). Packard concludes his famous study with the following comment: "The most serious offense many of the depth manipulators commit, it seems to me, is that they try to invade the privacy of our minds. It is this right to privacy of our minds—privacy to be either rational or irrational—that I believe we must strive to protect" (at p. 266).

105. "Consumer Attitudes Towards Spam in Six Countries: Survey of 6,000 Internet Users by Forrester Data" *Business Software Alliance* (9 December 2004) <http://www.bsa.org/usa/events/loader.cfm?url=/commonspot/security/getfile.cfm&pageid=20654>; Diana Pereira "Who opens e-mail spam?" *Globe and Mail* (22 December 2004); "Spam e-mails tempt net shoppers" *BBC News* (10 December 2005), <http://news.bbc.co.uk/2/hi/technology/4084871.stm>. Other examples of more-than-offensive spam might include situations where sexual abuse survivors are constantly confronted with invitations to view "incest" pornography.

> I roll around the ice pick enough I think I can either kill you or take out your language area such that you are rendered aphasic. It should be an interesting trial you fucking pig piece of shit Doug Mackay. Be afraid Doug MacKay, be very afraid.[106]

As Booher intuitively knew, without an adversary there can be no story, since there is no ability to retaliate, no ability to seek redress of wrongs, and hence no way to re-establish the equilibrium that classical narrative seeks. If indeed Booher's rage is misdirected, as the victim of his threats claims, then Booher's online fame celebrates him as a tragic hero, battling against forces bigger than he is, unable to sit back like the rest of us and accept his fate.

The desire to name an adversary is also legible in newspaper articles profiling known spammers. These stories satisfy because they put a name and a face to an otherwise amorphous enemy. Wallace "Spamford" Sanford, for instance, proprietor of Cyber Promotions Inc. discussed above, improved this problem with narration by being such a media hound.[107] He and other spammers, willingly or unwillingly identified in the media, give the public someone to direct their anger towards, someone to engage in conflict, and so appear at least to move towards resolution.[108]

Anti-spam legislation, including the CAN-SPAM Act and the proposed Canadian bills, tries to legislate a solution to the narrative impasse by restructuring the nature of the relationship between spammer and recipient, by requiring the spammer to both announce the non-personal nature of the message and to be accountable to it. Features of the CAN-SPAM Act that work towards this goal include requiring spam messages to have a valid return email address and to state a valid postal address.[109] These requirements are designed to provide recipients with a means to contact the sender and, when things go wrong, to provide them with an identifiable adversary.[110]

Knowing the adversary is, of course, also necessary in order to bring a spammer to court, though virtually all of the ISP lawsuits noted above brought under the CAN-SPAM Act address John Doe defendants in the hopes that later evidence will be gatherable through court processes. Some now pre-empted US state anti-spam statutes granted individual causes of action upon receiving even

---

106. *Supra* note 11. The email is quoted at para. 11 of the criminal complaint, and serves as count three of the indictment, where the name of the victim is removed.

107. Janet Kornblum "Spamford speaks" *CNET News.com* (31 March 1997), <http://news.com.com/Spamford+speaks/2009-1082_3-233712.html>.

108. See for instance Myles White "The perfect program for 'spam haters'" *Toronto Star* (16 October 1997) J03, where he writes "Wallace is crying the blues. Apparently, he'd lined up a few other ISPs to host his account as a backup, but they too cancelled. Aw, shucks. Too bad."; Bill Husted & Ann Hardie "Spam wars play out across Internet" *Atlanta Journal-Constitution* (14 December 2003), which includes a profile of Flo Fox, who "feeds the hungry by day but spams by night"; see also references to spammer Jeff Slaton in Peter Krivel "You've got spam" *Toronto Star* (28 June 2001) J1, J2; and Mike Wendland "Spam king lives large off others' e-mail troubles" *Detroit Free Press* (22 November 2002), <http://www.freep.com/money/tech/mwend22_20021122.htm> which is a profile of Alan Ralsky, who lives in a brand new 8,000 square foot luxury home which the writer calls "the house that spam built."

109. CAN-SPAM Act, *supra* note 39, s. 5(a)(3) [return email requirement], s. 5(a)(5)(A)(iii) [postal address requirement]. *Spam Control Act*, *supra* note 26, s. 11(1)(d) requires that messages "show address of the sender" but does not specify whether this should be electronic or postal or both.

110. The provisions of the CAN-SPAM Act that require the opt-out mechanisms discussed above and the provisions that create offences for spammers who do not honour these requests also try to re-infuse spam practices with personal accountability.

a single contravening spam email, entitling the recipient to statutory damages low enough to be pursued in relatively accessible small claims courts, and specifying easily provable legal standards.[111] The Canadian bills, as mentioned above, would also create an individual cause of action in nuisance, though no statutory damages are specified, leaving the determination of damages or other relief to the courts.[112]

Private causes of action by individuals may be symbolically important, as some consumer advocates have argued,[113] insofar as they provide a public option for addressing grievances against spammers. Other avenues for individual redress that statutory causes of action might enable include facilitating the certification of classes of spam email recipients for class action suits against spammers. A flaw with this approach of course remains the difficulty that private individuals face in deciphering the identity of spammers, the resources it takes to initiate a court action, and the fact that initiating lawsuits as a named party might invite retaliation by unscrupulous spammers. Alternative means of mobilizing collective action are called for.

One alternative route might be to enable a consumer protection entity, such as the Competition Bureau, federal or provincial Privacy Commissioner, or some other specially-designated not-for-profit organization, to compile complaints from individuals who could either choose to be named or choose to remain anonymous. This organization would then be empowered to either initiate proceedings against particular spammers or to forward the complaints to the sender's ISP once the complaints had reached a certain numerical threshold. This latter strategy is similar to the method currently employed by the not-for-profit organization SpamCop, which collects, compiles, deciphers and submits complaints sent in by spam recipients to the ISP of the spam sender.[114] ISPs are free to do what they will with this information, and many use the forwarded

---

111. California, Delaware and Washington had particularly strong anti-spam statutes, for instance. Washington's statute contained an individual cause of action where "Damages to recipient of a commercial electronic mail message sent in violation of this chapter are five hundred dollars, or actual damages, whichever is greater" (Ch. 19.190.040). For a complete list of state anti-spam statutes, see <www.spamlaws.com/state/summary.html>. The Utah Court of Appeals recently overturned a lower court ruling which dismissed a case for lack of personal jurisdiction, finding instead that sending one email in contravention of the Utah's *Unsolicited Commercial and Sexually Explicit Email Act* (Utah Code Ann. ss. 13-36-101 to 105) indicated sufficient contact for Utah to assert personal jurisdiction over the defendant, an Arizona company. The state statute was in effect at the time the email was received, and had not yet been pre-empted by the federal CAN-SPAM Act. *Fenn v. MLeads Enterprises, Inc. and John Does I through X*, 3004 UT App 412. Some US federal bills that died on the vine also included private rights of action with statutory damages, like the *Unsolicited Commercial Electronic Mail Act of 2000*.

112. *Spam Control Act*, *supra* note 26, s. 17; *Anti-Spam Act 2004*, *supra* note 39, s. 12.

113. "CAUCE Statement on CAN SPAM Act" *Coalition Against Unsolicited Commercial Email* (16 December 2003), <http://www.cauce.org/news/2003.shtml>; Jessica Levine "Spam and the Law" *PC Magazine* (25 February 2003), <http://www.pcmag.com/print_article/0,3048,a=36204,00.asp>. For a discussion, see Kelman, *supra* note 62 at p. 375.

114. SpamCop.net, <http://www.spamcop.net>.

complaints as a reason to either initiate an investigation into the impugned subscriber or else terminate his or her service on the basis of the complaints alone.[115]

The CAN-SPAM Act provides two other avenues of redress indirectly available to individuals. First, the Act provides that state Attorneys General can bring lawsuits for contravention of the Act on behalf of their states' residents.[116] Second, the Act provides that ISPs can bring a suit against a spammer engaging in a pattern or practice that violates the consumer protection prohibitions in section 5 of the Act. The latter cause of action further carries statutory damages for each unlawful message transmitted or attempted to be transmitted over their facilities.[117] The state suits have the benefit of providing a public context to frame the complaints, where individuals are represented collectively as citizens, since the act specifies statutory damages for each unlawful message received by residents.[118] Attorneys General can receive complaints from individuals through consumer complaint hotlines, through specifying a mechanism for forwarding spam emails to the Attorney General's office, or through other established complaint filing mechanisms.[119]

ISP suits have the benefit of mobilizing private companies' resources, and ISPs clearly have a vested interest in finding ways to redress the complaints of unhappy customers. Further, because of the determination that email servers and computer networks are the private property of ISPs, it makes sense that ISPs would have a central role to play in the redress of these wrongs, since they also have a property interest to defend. Judging by the language used in the ISP suits brought under the CAN-SPAM Act so far, the ISPs have embraced their position as the conduit through which customer grievances are heard. Cases launched by Yahoo! and Microsoft both quote the US Congress' rationale for enacting the CAN-SPAM Act, saying that spam has "quickly become one of the most pervasive intrusions in the lives of Americans."[120] The inclusion of this quote positions the suits as speaking for "Americans"—enacting the substitution of customers for citizens that the CAN-SPAM Act itself encourages by limiting

---

115. In a lawsuit initiated by legitimate email marketer OptInRealBig.com, the US District Court for the Northern District of California rejected the plaintiff marketer's argument that SpamCop was compelled to identify the source of the complaints so that the plaintiff could comply with the CAN-SPAM Act and remove the complainants from its mailing list (*OptInRealBig.com, LLC v. Ironport Systems, Inc and its wholly owned subsidiary, SpamCop.net, Inc.* (US Dist Ct ND Cal) No. C 04-1687 SBA). The court also found SpamCop to be immune from liability for any damages resulting from complaints forwarded under the *Communications Decency Act*, which provides that "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider" (*Communications Decency Act*, s. 230). Canada would need to have similar safeguards from liability for false accusations in place if such a regime were to be officially adopted.

116. CAN-SPAM Act, *supra* note 39, s. 7(f).

117. *Ibid.*, s. 7(g).

118. *Ibid.*, s. 7(g)(3)(A).

119. See for instance "AG Reilly Sues Deceptive Spammer For Violating Massachusetts Law, Federal Can Spam Act" *Office of Massachusetts Attorney General Tom Reilly* (1 July 2004) <http://www.ago.state.ma.us/sp.cfm?pageid=986&id=1257>. Missouri has a spam forwarding mechanism whereby forwarded spam messages are identified via a specified subject heading (Missouri Attorney General's Office, <http://www.ago.mo.gov/nospam/nospam.htm#complaint>. The FTC and the FBI also have mechanisms for consumers to file complaints about spam.

120. *Yahoo! Inc. v. Eric Head et al. and John Does 1-5* (US Dist Ct, ND Calif, C04 00965) at para. 28; *Microsoft Corporation v. John Does 1-5 d/b/a Super Viagra Group* (US Dist Ct WD Wash) No. CV04-0516 at para. 13; *Microsoft Corporation v. JDO Media, Inc. and John Does 1-50* (US Dist Ct WD Wash), No. CV04-0517 at para. 14 [*Microsoft Corporation v. JDO Media, Inc.*]. These suits are among those filed on 9 March 2004.

causes of action to ISPs and state Attorneys General.[121]

Nonetheless, because individuals in ISP suits are able to be represented only as customers and not the more public designation of consumers or citizens, these suits should not be the only means of finding legal voice, lest the public interest in supporting the autonomy-based right to maintain personal boundaries be lost to a purely business interest-oriented dispute-resolution strategy.

*

4. PUTTING SOME ACTION INTO CANADA'S ANTI-SPAM ACTION PLAN

INDUSTRY CANADA'S RECENTLY-RELEASED "Anti-Spam Action Plan for Canada" is devoid of any acknowledgement of personal affronts.[122] The plan is in fact very light on law generally, and does not suggest any enforcement strategies, opting instead to reiterate the need for collaboration between industry and government and the importance of consumer education (*i.e.* to get people to stop responding to spam).[123]

The plan finds that most of the products and services promoted in spam might be "unwanted and often offensive to many Internet users, [but that] they do not, for the most part, involve the offering of illegal products or services, or the making of what might be considered, in law, misleading claims"[124]—a finding which appears to diminish the role of law and instead elevate the interests of ISPs in keeping their customers happy. This is of course a very different approach than that put forward in anti-spam legislation, like Oliver's *Spam Control Act*, which despite its fatal flaws at least gives law a central role in orchestrating a solution to spam and in giving recipients a means of redress.[125]

Nevertheless, the government of Canada continues to be reluctant to introduce its own legislation. Michael Geist has argued that existing legislation

---

Incidentally, the Yahoo! case includes named defendants associated with a company located in Kitchener, Ontario, so while there have not been similar cases in Canada, Canadian companies have been involved in American suits.

121. Both Microsoft and AOL launched suits which included complaints about the use of misleading subject lines in contravention of the CAN-SPAM Act, again underscoring the ISP's role as spokesperson for individuals not able to bring their own suits. *Microsoft Corporation v. JDO Media, Inc.*, *supra* note 120; *America Online, Inc v. Hawke and John Does 1-50, supra* note 102.

122. Industry Canada, *An Anti-Spam Action Plan for Canada*, *supra* note 19.

123. There has been surprisingly little change between the 2004 action plan and Industry Canada's SPAM Discussion Paper *Internet and Bulk Unsolicited Electronic Mail*, which announced that

> The government believes that an appropriate mix of policies and laws, consumer awareness, responsible Internet industry stakeholders and technological solutions is the best and most appropriate way to deal with behaviour in the new and evolving on-line environment. The government believes that Canada has this right mix today but will continue to monitor developments and consider changes if they are required.

Industry Canada, *SPAM Discussion Paper—July 1997: Internet and Bulk Unsolicited Electronic Mail* (Ottawa: July 1997), <http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/gv00188e.html> at p. 4.

124. Industry Canada, *An Anti-Spam Action Plan for Canada*, *supra* note 19 at p. 2.

125. Most notable among these flaws is the legislation's misguided efforts to impose penalties on ISPs for not implementing adequate spam protection measures. By raising the ire of the ISP industry, instead of trying to harness the interests of the ISPs by offering them a cause of action against spammers (as in the CAN-SPAM Act), the legislation has hopelessly doomed itself. This flaw has meant that the more positive features of the bill discussed above will have to be incorporated into another bill with better hopes of being enacted.

adequately addresses all of the troubling aspects of spam, and so no new legislation is necessary[126]—a position which the Anti-Spam Action Plan appears to so far support. But this position does not consider the lack of redress available for addressing affronts to the autonomy interests at stake in individuals' efforts to exclude spam from their inboxes, which anti-spam legislation can bring to the foreground through the requirements and prohibitions discussed above. Further, anti-spam legislation has the benefit of addressing the spam problem in a centralized fashion, marking a specific legislative response which addresses the autonomy-based interests that inform public complaints about spam.

While the *Personal Information Protection and Electronic Documents Act* (PIPEDA)[127] already does provide a means of redress via its prohibition against the misuse of email addresses, as the report suggests, without further efforts to coordinate methods for identifying spammers, individuals will not be able to access this remedy. Further, it is decidedly inefficient to expect each individual to bring a separate complaint to the Privacy Commissioner. Canadian anti-spam legislation could implement a means of submitting complaints collectively, as described above, which could improve the effectiveness of this avenue of redress. Relying on PIPEDA without further action implements a weakly enforceable opt-in regime, where more directly stated anti-spam legislation could make clear the consequences for not obtaining prior consent before using email addresses in unauthorized ways.

Also, existing legislation does not address the question of whether consumers have a right to know that they are about to view advertising materials. While the action plan claims that the *Competition Act* already addresses the problem of misleading claims about products and services, it is not at all clear that a false subject heading pretending to be from a friend, for instance, is really a *materially* misleading claim about the product being sold, as required by the Act.[128] Also, the *Competition Act* certainly does not place any affirmative requirements on spammers, such as requirements to include labels such as "ADV" in subject lines (which could greatly facilitate the use of filtering software by individuals), or even the less specific requirement to identify a message as an advertisement as required by the CAN-SPAM Act.

Current legislation also does not expressly require that advertisers be identifiable to the recipients of advertising messages, making it difficult for individuals to know who to hold accountable when they want to complain. Like the other affirmative requirements in US anti-spam legislation, violation of these requirements at least provides grounds for legal complaint, and so empowers

---

126. Michael Geist, "Untouchable?: A Canadian Perspective on the Anti-Spam Battle" (May 2004), <http://www.michaelgeist.ca/geistspam.pdf>.

127. *Personal Information Protection and Electronic Documents Act*, R.S.C. 2000, c. 5 <http://laws.justice.gc.ca/en/P-8.6/92607.html> [PIPEDA].

128. Geist also asserts that the Competition Bureau's Fair Business Practices Branch is empowered to review the conduct of businesses that send messages with false header information under s. 74.01 of the *Competition Act*, which names as reviewable conduct the making of "a representation that is false or misleading in a material respect" in the course of promoting a product (Geist, *supra* note 126 at p. 26). The issue here will be whether misrepresentations of header information (and false subject lines) that dupe a recipient into opening an email are misleading in a material respect.

individuals to protect their autonomy interests to the degree they choose to, even where there continues to be other hurdles to bringing spammers in line with the regime.

Enforcement mechanisms also form a crucial part of the strategy, as Geist has rightly pointed out. But without specific causes of action, as set out in anti-spam legislation, individuals are left few avenues of recourse, whether director indirect.[129] The legislation does not stand alone, but rather interacts with all the other possible grounds of legal action, as is illustrated by the multiple causes claimed in the ISP suits against spammers cited above. Anti-spam legislation therefore presents an opportunity to articulate straightforward violations of consumer privacy and autonomy rights, and to delineate the legal means for addressing violation of those rights, including by means of collective actions.

Industry Canada's January 2003 discussion paper on spam recognizes that the options discussed above are available and vows to consider them. Yet, the May 2004 action plan appears to be no closer to identifying the value of each measure, much less to coming to a conclusion on whether to implement any of them. Indeed, the Action Plan's restatement of its task is not promising, in that the Task Force will

> review existing laws to determine whether stronger enforcement or new legislation *could make a significant impact on the reduction and control of spam,* and whether the government should consider taking any further legislative or enforcement measures.[130]

By phrasing the problem merely in terms of making a "significant impact on the reduction and control of spam," the Task Force has severely limited the function that law can play, placing an inordinate emphasis on the effectiveness of legislation, and completely ignoring the symbolic functions that law plays in making clear the values that the legal system supports.

Moreover, Canada's current inaction disempowers consumers and citizens by making classical legal narrative, where a person can meet his or her adversary and seek redress of legally defined wrongs, basically unobtainable. While encouraging cooperation with the ISP industry, development of technical solutions, and consumer education are all important components of an effective anti-spam strategy, the absence of more targeted legal responses to individuals' complaints about spam practices distances Canadians from public agency. It further privatizes wrongs that stem from an ostensibly public value in personal autonomy by channelling complaints about these wrongs exclusively through the relationship between ISPs and their customers.

---

129. The CAN-SPAM Act also empowers the Federal Trade Commission and some other government agencies to launch enforcement campaigns against senders of fraudulent emails (CAN-SPAM Act, *supra* note 39, s. 7(a) and (b)). Industry Canada's January 2003 discussion paper on spam points out that Canada does not have a similar overarching national organization. Instead, enforcement measures against purveyors of fraudulent schemes falls to more traditional policing agencies, like the RCMP (Industry Canada, *E-mail Marketing*, *supra* note 19 at p. 50).

130. Industry Canada, *Anti-Spam Action Plan*, *supra* note 19 at p. 5 [emphasis added].

When Parliament decided to implement section 13(2) of the *Canadian Human Rights Act,* it was clear that purveyors of hate speech over the internet could easily evade Canadian jurisdiction and so escape the reach of the legislation. Nonetheless, as the Canadian Human Rights Tribunal has held, the message that Canada does not tolerate hate speech is a value that is central enough that effectiveness alone did not and should not determine the content of the legislation. The Tribunal stated:

> Any remedy awarded by this, or any Tribunal, will inevitably serve a number of purposes: prevention and elimination of discriminatory practises is only one of the outcomes flowing from an Order issued as a consequence of these proceedings. There is also a significant symbolic value in the public denunciation of the actions that are the subject of this complaint. Similarly, there is the potential educative and ultimately larger preventative benefit that can be achieved by open discussion of the principles enunciated in this or any Tribunal decision.[131]

The same principle should guide the decision of whether or not to implement anti-spam legislation, primarily as a statement about the value of individual autonomy interests in Canada, with some practical, even if currently not easily enforceable, parameters to restructure the relationship between spammers and email users.

This article has argued that, in the search for legal solutions to spam, autonomy interests should be in the foreground. Images of the residential internet user should not be read as locating the conflict between spammers and recipients, but rather as calling upon the law to respond to spam's personal affront. In other words, the significance of persistent images of the home in anti-spam imagery and discussion is not to be found in property interests, but rather in the social importance of the individual autonomy interests symbolically housed there.

---

131. *Citron v. Zündel,* Canadian Human Rights Tribunal (18 January 2002), <http://www.chrt-tcdp.gc.ca/search/view_html.asp?doid=252&lg=_e&isruling=0> at para. 300. See also Jane Bailey, "Of Mediums and Metaphors: How a Layered Methodology Might Contribute to Constitutional Analysis of Internet Content Regulation" (2004) 30:2 Manitoba Law Journal 197.

*

5. EPILOGUE

THE TASK FORCE ON SPAM, formed under the auspices of the Government of Canada's *An Anti-Spam Action Plan for Canada*, issued its final report "Stopping Spam: Creating a Stronger, Safer Internet" in May 2005 shortly after this article was finalized.[132] The report states that after its year-long studies and discussions with the full panoply of stakeholders, the Task Force recommends, *inter alia*, the enactment of specific anti-spam legislation containing many of the same features endorsed in this article, such as the creation of spam offences and a private right of action with meaningful statutory penalties, and the creation of an opt-in regime for receipt of commercial email. This position is a welcome departure from the general trend in Canadian approaches to internet issues, which tends to shy away from addressing such problems directly, preferring instead to find a home for them within larger, technology-neutral legal concepts.

While the Task Force Report does not explore the underlying reasons for supporting such measures, suggesting instead that they are needed in order to implement an effective policy to combat spam and its even more malicious descendants, it is encouraging that this article and the Task Force Report arrive at some common recommendations. This common ground illustrates that an effective *and* principled approach to the evolving intrusions of the most bothersome commercial internet practices is possible.

132. Canada, Spam Task Force, *Stopping Spam: Creating a Stronger, Safer Internet* (Ottawa: Industry Canada, 17 May 2005), <http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00248e.html>.