

## ESTABLISHING A LEGITIMATE EXPECTATION OF PRIVACY IN CLICKSTREAM DATA

*Gavin Skok\**

Cite as: Gavin Skok, *Establishing a Legitimate Expectation of Privacy in Clickstream Data*, 6 MICH. TELECOMM. TECH. L. REV. 61 (2000)  
available at <<http://www.mttl.org/volsix/skok.html>>

I.	THE INTERNET AND CLICKSTREAM DATA COLLECTION .....	62
II.	THE FOURTH AMENDMENT AND THE INTERNET.....	70
	A. <i>A Brief Overview of the Fourth Amendment’s Expectation of Privacy and Reasonableness Requirements</i> .....	70
	B. <i>Application of the Fourth Amendment to the Internet has Thus far Been Marked by Reliance on Principles Ill-Suited to Cyberspace, Leading Courts to Conclude that Net Users Lack an Expectation of Privacy in Online Activity</i> .....	72
	C. <i>Courts Employing Traditional Fourth Amendment Jurisprudence will Probably Conclude that Net Users Lack a Legitimate Expectation of Privacy in Clickstream Data</i> .....	75
III.	ESTABLISHING A LEGITIMATE EXPECTATION OF PRIVACY IN CLICKSTREAM DATA .....	81

The development of the Internet presents unprecedented opportunities for global communications and commerce. However, it also poses dramatic risks to personal privacy.<sup>1</sup> The series of electronic footprints created when a Web user moves about in cyberspace, commonly called a “clickstream,” can be monitored and recorded by prying eyes. This data

---

\* Law Clerk to the Honorable Robert H. Whaley, United States District Court for the Eastern District of Washington. Gavin Skok received his Juris Doctor With Honors from the University of Washington School of Law in 1999, and his Bachelor of Arts-Honors from Gonzaga University in 1996. The views expressed in this article are those of the author, and should not be attributed to either the United States District Court for the Eastern District of Washington or the Honorable Robert H. Whaley.

1. See Paul Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1610–11 (1999) (“[I]nformation technology in cyberspace also affects privacy in ways that are dramatically different from anything previously possible. By generating comprehensive records of online behavior, information technology can broadcast an individual’s secrets in ways that he or she can neither anticipate nor control. Once linked to the Internet, the computer on our desk becomes a potential recorder and betrayer of our confidences.”).

can then be “mined” for information and used to profile a Web user or to recreate her online experience.

A significant Fourth Amendment question is raised when the prying eyes monitoring a clickstream belong to law enforcement officers: does a Net user retain a legitimate expectation of privacy in his or her clickstream data? Unfortunately, traditional Fourth Amendment jurisprudence is ill-suited to answer this question.<sup>2</sup>

This Article argues that Web users should enjoy a legitimate expectation of privacy in clickstream data. Fourth Amendment jurisprudence as developed over the last half-century does not support an expectation of privacy. However, reference to the history of the Fourth Amendment and the intent of its drafters reveals that government investigation and monitoring of clickstream data is precisely the type of activity the Framers sought to limit. Courts must update outdated methods of expectation of privacy analysis to address the unique challenges posed by the Internet in order to fulfill the Amendment’s purpose.

Part I provides an overview of the Internet and clickstream data collection, and explains the value of this data to law enforcement. Part II discusses general Fourth Amendment principles, then explores how these principles have been, and are likely to be, applied to the Internet. Part III explores the intent of the Fourth Amendment’s drafters, analogizes clickstream searches to the general searches the Framers sought to prohibit, and argues that the values underlying the Fourth Amendment require courts to eschew the traditional two-prong expectation of privacy test in favor of a normative inquiry which recognizes a legitimate expectation of privacy in clickstream data.<sup>3</sup>

## I. THE INTERNET AND CLICKSTREAM DATA COLLECTION

The Internet is a global electronic communications medium comprised of innumerable computer networks which communicate by using a common language and set of data transfer protocols.<sup>4</sup> The Internet is

---

2. *See, e.g.*, *United States v. Hambrick*, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999) (“Cyberspace is a nonphysical ‘place’ and its very structure, a computer and telephone network that connects millions of users, defies traditional Fourth Amendment analysis.”).

3. While clickstream monitoring and data mining technology are still in their infancy, courts must frequently lay the groundwork for future laws without the benefit of foresight into future technological advancement. Accordingly, this Article assumes that data storage and processing technology will in the near future allow mass processing and sorting of clickstream information.

4. The Federal Networking Council defines “Internet” as “the global information system that—(i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons; (ii) is able to support commu-

not a location; rather, it is the aggregate of the electronic communications routers and devices which transmit and receive electronic information through the global network. Originally conceived during the Cold War as a means by which to insure continuity in military communications during wartime, the modern Internet has brought hundreds of millions of people together online. While the exact number of Internet users is impossible to determine, it is estimated that nearly 300 million people worldwide are currently online.<sup>5</sup> These users can travel among the five million active Web sites on the Net.<sup>6</sup> The growth of this medium over the past five years has been explosive,<sup>7</sup> and promises to continue at

---

nications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and (iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein.” *FNC Resolution: Definition of “Internet,”* (last modified October 30, 1995) <[http://www.fnc.gov/Internet\\_res.html](http://www.fnc.gov/Internet_res.html)>. See also Stephan K. Bayens, *The Search and Seizure of Computers: Are We Sacrificing Personal Privacy for the Advancement of Technology?*, 48 *DRAKE L. REV.* 239, 248–49 (2000) (“‘The Internet is not a physical or tangible entity, but rather a giant network which interconnects innumerable smaller groups of linked computer networks.’ The Internet is an overwhelming mass of information that has no centralized administrator, storage location, or control point. ‘It exists and functions as a result of the fact that hundreds of thousands of separate operators of computers and computer networks independently decided to use common data transfer protocols to exchange communications and information with other computers (which in turn exchange communications and information with still other computers).’”) (footnotes omitted). For a good overview of the way the Internet works, see Schwartz, *supra* note 1, at 1618–21. See also *Overview of the World Wide Web* (visited March 2, 2000) <[http://www.cio.com/WebMaster/sem2\\_home.html](http://www.cio.com/WebMaster/sem2_home.html)>; *The World Wide Web for the Clueless* <[http://www.cio.com/WebMaster/sem2\\_simple\\_pieces.html](http://www.cio.com/WebMaster/sem2_simple_pieces.html)>.

5. *Nua Internet Surveys: How Many Online?* (visited April 21, 2000) <[http://www.nua.ie/surveys/how\\_many\\_online/index.html](http://www.nua.ie/surveys/how_many_online/index.html)> (estimating 304.36 million Internet users as of March 2000); *Global Reach: Global Internet Statistics* (last modified March 31, 2000) <<http://www.glreach.com/globstats/index.php3>> (estimating 288 million Internet users worldwide).

6. *Nua Internet Surveys: Netcraft: 5 Million Web Sites on the WWW* (last modified April 20, 1999) <[http://www.nua.ie/surveys/index.cgi?f=VS&art\\_id=905354851&rel=true](http://www.nua.ie/surveys/index.cgi?f=VS&art_id=905354851&rel=true)> (“Just two years ago the Netcraft survey counted 1 million web sites on the Web, the latest survey finds that there are now over 5 million web sites.”). See also *Domainstats.com* (last modified April 6, 2000) <<http://www.domainstats.com>> (recognizing 15,719,462 registered domain names worldwide).

7. See *Computer Industry Almanac Inc.: Over 150 Million Internet Users Worldwide at Year-end 1998* (last modified April 30, 1999) <<http://www.c-i-a.com/199904iu.htm>> (“April 30, 1999—According to the Computer Industry Almanac Inc. there were over 150 million Internet users at year-end 1998—up from 61 million Internet users at year-end 1996.”); *Nua Internet Surveys: Netcraft, supra* note 6 (“Just two years ago the Netcraft survey counted 1 million web sites on the Web, the latest survey finds that there are now over 5 million web sites.”); *Headcount.com: Who’s online by country: The World* (visited March 19, 2000) <<http://www.headcount.com/count/datafind.htm?choice=country&choicev%5B%5D=The+World&submit=Submit>> (“In June 1998, Matrix Information and Directory Services (MIDS) reported that there are 102 million accessing the Internet in the world. This number is esti-

a rapid pace well into the twenty-first century. Recent estimates show the number of people going online during the next two years approaching one billion, and show the value of Internet commerce swelling to over \$1 trillion by 2003.<sup>8</sup>

Unfortunately, Web surfing generates a massive amount of personal information about a user each time he or she goes online.<sup>9</sup> Net users often operate under an illusion of anonymity in cyberspace. However, the reality of the Internet is much different: prying eyes can identify individual users and track online activity by monitoring and examining "clickstreams." A "clickstream" is the aggregation of the electronic information generated as a Web user communicates with other computers and networks over the Internet.<sup>10</sup> The name "clickstream" refers to the series of mouse clicks users make as they travel the Web. Each click translates into an electronic signal which is then sent by the surfer's computer to other computers on the Net telling them what information to return to the user. Since online movement requires the user to send or request certain information from other computers on the Web, every step in cyberspace inevitably becomes part of the clickstream record.<sup>11</sup> This

---

mated as of January 1998 and has increased from the estimate of 57 million in January 1997.").

8. See *Headcount.com*, *supra* note 7 ("MIDS [Matrix Information and Directory Services] estimates that the total number of worldwide Internet users will grow to 707 million by 2001."); *Internet Commerce Will Rocket to More Than \$1 Trillion by 2003, According to IDC* (last modified June 28, 1999) <<http://www.idc.com/Data/Internet/content/NET062899PR.htm>> ("In recent market research, International Data Corporation (IDC) reports the amount of commerce conducted over the World Wide Web will top a staggering \$1 trillion by 2003.").

9. *Federal Trade Commission Staff Report: Online Privacy: General Practices and Concerns* (last modified September 15, 1997) <<http://www.ftc.gov/reports/privacy/privacy3.htm>> ("The Internet is a highly decentralized, global network of electronic networks. It is unique among communications media in the variety and depth of personal information generated by its use.").

10. Eric Johnson, *An Examination of the Role of Clickstream Data in Marketing through the Internet* (last modified May 12, 1997) <<http://www.ftc.gov/bcp/privacy/wkshp97/comments2/johnson0.htm>> n.1 ("A formal definition of 'clickstream' data, according to CASIE, the Consortium for Advertising Supported Information and Entertainment: 'The database created by the date-stamped and time-stamped, coded/interpreted, button-pushing events enacted by users of interactive media, controlling their systems via remote control channel changers, alphanumeric PC keyboards and mice, numeric keyboards of PDAs and similar devices, and voice command of screen media.'"). See also JULIAN S. MILLSTEIN, ET AL., *DOING BUSINESS ON THE INTERNET: FORMS AND ANALYSIS* § 10.02(1)(a) (1999) ("As an individual user browses the Internet, a trail of electronic information is left at Web sites he or she visits. [This i]nformation about the path a user takes through the Internet, called 'clickstream' data, can be collected and sorted.").

11. Schwartz, *supra* note 1, at 1620 ("The Internet's technical qualities also have a negative consequence: they make possible an intense surveillance of activities in cyberspace. Digital reality is constructed through agreement about technical norms. This 'code,' to use Lawrence Lessig's term, creates cyberspace. As a result of cyberspace code, surfing and other

data can be shockingly revealing, providing a record of the entirety of one's online experience, including movements among Web sites, geographical location, the type of computer and Internet browser in use, and any transactions or comments made at individual Web sites.<sup>12</sup>

Clickstream data poses a dramatic risk to the personal privacy of Net users since it can be collected, stored, and reused indefinitely.<sup>13</sup> An increasing number of private companies are monitoring, recording, and analyzing clickstreams in an effort to make Internet advertising more effective. This data is typically collected by online advertisers and retailers, and by Internet service providers ("ISPs").<sup>14</sup> Most online advertisers

---

cyberspace behavior generate finely granulated data about an individual's activities—often without her permission or even knowledge.") (footnotes omitted).

12. See *Center for Democracy & Technology: CDT's guide to online privacy* (visited February 23, 2000) <<http://www.cdt.org/privacy/guide/start>> ("Use of the network, however, generates detailed information about the individual—revealing where they "go" on the Net (via URLs), who they associate with (via list—serves, chat rooms and news groups), and how they engage in political activities and social behavior."); Jerry Berman & Deirdre Mulligan, *Privacy in the Digital Age: Work in Progress*, 23 NOVA. L. REV. 551, 554 (1999) ("The data trail, known as transactional data, left behind as individuals use the Internet is a rich source of information about their habits of association, speech, and commerce. Transactional data, click stream data, or 'mouse droppings,' as it is alternatively called, can include the Internet protocol address ('IP address') of the individual's computer, the browser in use, the computer type, and what the individual did on previous visits to the Web site, or perhaps even other Web sites."); Damien Cave, *Salon.com: Do They Know Where You Live?* (last modified February 28, 2000) <<http://www.salon.com/tech/feature/2000/02/28/geographic/index.html>> ("Ad-serving companies like Double Click offer services that they say can target ads to users by location. And Digital Island introduced technology last year called TraceWare, which can identify the location of Web site visitors with 96 percent accuracy. TraceWare works by scanning worldwide traffic as it passes through ISPs, then matching users' IP addresses with a database of IP address locations that Digital Island has built.").

13. See *Federal Trade Commission Staff Report: Online Privacy*, *supra* note 9 ("When users browse on the World Wide Web ('the Web'), for example, they leave an electronic marker at each site (or on each page within a site) they visit. The series of electronic markers, or 'clickstream' generated by each user's browsing activities can be aggregated, stored, and re-used."); *Center for Democracy & Technology: CDT's guide to online privacy*, *supra* note 12 ("Some of the newest tracking tools can so efficiently mine and manipulate the data trail (or 'clickstream') people leave behind when they use the Internet that they build a detailed database of personal [sic] information without any human intervention."); Jerry Berman & Deirdre Mulligan, *Privacy in the Digital Age: Work in Progress*, 23 NOVA. L. REV. 551, 554 (1999) (explaining that clickstream data "is captured at various points on the network and available for reuse and disclosure."); JULIAN S. MILLSTEIN, ET AL., *DOING BUSINESS ON THE INTERNET: FORMS AND ANALYSIS* § 10.02(1)(a) (1999) ("[C]lickstream data [] can be collected and stored.").

14. An Internet service provider, or ISP, is the portal which provides access to the Internet for individuals, educational institutions, companies, and organizations. A Net user dials into the ISP using his or her PC and a modem; the ISP then connects the user to the Internet. See Stephen Jenkins, *Glossary of PC and Internet Terminology* (last modified January 9, 2000) <<http://homepages.enterprise.net/jenko/Glossary/G.htm>> ("Internet Service Provider or sometimes referred to as Internet Access Provider (IAP) is a company which provides access

and merchants can monitor clickstreams only while a user is at the particular Web site operated by the advertiser or retailer; however, even this data can be incredibly revealing.<sup>15</sup> Some online advertisers have developed “networks” of hundreds of unrelated Web sites which use individual identifying codes to identify and track Web users’ clickstreams as they travel among the sites on the network.<sup>16</sup> The data compiled by these businesses is then “mined” for hints about consumer

---

to the Internet for people like you & me. The company handles the link from your PC to the rest of the Internet. The ISP’s central computer is linked to the rest of the internet so the person using this service only pays the telephone charges to connect from their home computer to the ISP’s central computer.”); *UGeek Technical Glossary* (last modified April 26, 1999) <[http://www.geek.com/glossary/glossary\\_search.cgi?i](http://www.geek.com/glossary/glossary_search.cgi?i)> (“Internet Service Provider (ISP)—An ISP provides Internet access to people or corporations. ISPs generally have pools of modems awaiting dial-up connections.”)

15. See *Federal Trade Commission Staff Report: Online Privacy*, *supra* note 9 (“Each Web site, in turn, captures certain information about users as they enter the site. A Web site can ‘know’ users’ email addresses, the names of their browsers, the type of computer they are using, and the universal resource locator (URL), or Internet address of the site from which they linked to the current site. . . . Clickstream data also permits Internet site owners to understand activity levels at various areas within sites, in a manner analogous to a retail store’s practice of checking inventory.”); Millstein, *supra* note 11 (“Web sites, for instance, often have the capability to automatically log information about users. A Web site may be able to determine a user’s e-mail address, the type of computer and browsing software being used, and the address of the Web site from which the user linked. The Web pages or files a user accessed while browsing a Web site—and how long the user remained on a particular Web page—can also be recorded.”); Peter McGrath, *Newsweek: Knowing You All Too Well* (last modified March 29, 1999) <[http://www.newsweek.com/nw-srv/printed/us/st/ty0113\\_2.htm](http://www.newsweek.com/nw-srv/printed/us/st/ty0113_2.htm)> (“Your clickstream reveals your interests and tastes with unnerving precision. (Did you go from slate.com to a Volvo dealer’s Web site? Did you then buy some brie from peapod.com, the online grocery? You may be one of those limousine liberals we’ve been hearing about.) And when Web merchants combine clickstream analysis with another new software technique known as ‘collaborative filtering,’ which makes educated inferences about your likes and dislikes based on comparing your user profile with others in the database, they have a marketing tool of high potential not only for customer satisfaction but also for abuse.”); Eric Wieffering, *Protecting your digital footprints*, MINNEAPOLIS STAR TRIB., November 7, 1999, at 1D (“[O]nline, every mouse-click within a particular site can be tracked and analyzed. Even on sites where you’re not required to volunteer personal information, a Web site operator can log your computer’s address and know approximately where you’ve come from. It can then follow you around the site, recording which features and links you clicked on and how long you lingered there, and create a complete profile that it can use to determine what kind of advertising and products you will see.”). See also Beth Givens, *Privacy Rights Clearinghouse: The Emperor’s New Clothes: Privacy on the Internet in 1999* (last modified June 21, 1999) <<http://www.privacyrights.org/ar/emperor.htm>> (reporting results of Georgetown University’s McDonough School of Business May 1999 Internet Privacy Policy Survey, and noting that “the collection of personally identifiable information has become standard practice on a vast majority of commercial web sites.”).

16. Hiawatha Bray, *Boston Globe: Matching Ads to Eyeballs* (last modified February 22, 2000) <[http://www.boston.com/dailyglobe2/053/business/Matching\\_ads\\_to\\_eyeballsP.shtml](http://www.boston.com/dailyglobe2/053/business/Matching_ads_to_eyeballsP.shtml)> (describing Engage online user tracking network which coordinates numerous Web sites in tracking user clickstreams, thereby allowing Engage to compile detailed user profile, and explaining that Engage network has already tracked over 35 million online users.).

preferences, and may be used to generate personal profiles of surfers in order to target Internet advertising.<sup>17</sup>

In contrast, ISPs can precisely monitor and record an entire clickstream since all of the user's online commands are sent through the ISP.<sup>18</sup> This data can be combined with information the user voluntarily provides to the ISP to create a massive database detailing the online use habits of individually-identifiable surfers.<sup>19</sup> Such monitoring is becoming

---

17. Jesse Berst, *ZDNet AnchorDesk: The Good, Bad, and Ugly of Personalization* (last modified November 2, 1999) <[http://www.zdnet.com/anchordesk/story/story\\_4050.html](http://www.zdnet.com/anchordesk/story/story_4050.html)> (“Personalization is a huge trend on the Web. Sites create user profiles by identifying you each time you come to a site, recording your preferences, and then delivering ads and content targeted to your profile. . . . [T]he typical profile can contain: Explicit information. This is what you voluntarily reveal when registering at a site or signing up for a service. Your name, email address, etc. Implicit information. This is data the site gathers by monitoring your click stream—what you do, where you go. From that it infers what your interests are.”); John M. Broder, *Making America Safe for Electronic Commerce*, N.Y. TIMES, June 22, 1997, at 4D (“Those [clickstream] records provide invaluable information for marketers who can use them to pinpoint customers for their products. By following your Internet ‘clickstream,’ they can learn about your medical condition, your reading habits, your political predilections.”).

18. In this way, the ISP's role can be analogized to that of an interpreter in court proceedings. Since everything passes through the interpreter en route to its intended destination, the interpreter has access to all of the party's statements.

19. Roger Taylor, *FTC clicks on to fears over data on web users*, FIN. TIMES (London), April 5, 1999, at 5 (“At present there is no privacy on the Internet. Internet service providers know an individual user's name and address and can track every single move the user makes on the web. And the information is held on record. . . .”); Jeffrey Pollock, *A Tangled Web—Thoughts for a Law Firm Using the Web*, 198 AUG-N.J. LAW. 18–19 (1999) (“Virtually all netizens (Internet users for the uninitiate) access the Net through an ISP. As you are searching your way merrily along the strands of the WWW, however, your friendly ISP is collecting information regarding where you've been. The information captured is called a ‘click stream’ and records every website you've visited.”); James F. Brelsford & Nicole A. Wong, *Online Liability Issues: Defamation, Privacy and Negligent Publishing*, 564 PLI/PAT. 231, 244 (1999) (“Clickstream Data. While a user ‘surfs’ the Internet, each web site visited and each page viewed are typically logged by the user's Internet Service Provider. The ISP may maintain a record of a user's email communications and other online activities, including Web sites visited, purchases made, and more.”); Schwartz, *supra* note 1, at 1627 (“ISPs are in an advantageous position to tie together the information that exists about anyone who surfs the Web . . . [T]he ISP has detailed information about the Internet behavior of each of its customers. Through its role as an entrance ramp to the Internet, the ISP gains access to clickstream data and other kinds of detailed information about personal online habits. It can easily take these scattered bits of cyberspace data, pieces of which at times enjoy different degrees of practical obscurity, and make them into ‘personal information’ by linking them to the identity of its customers.”); David Whalen, *The Unofficial Cookie FAQ v. 2.53*, (last modified May 10, 1999) <<http://www.cookiecentral.com/faq/index.shtml>> (“The very nature of Web servers allows for the tracking of your surfing habits . . . .”); *Center for Democracy & Technology: CDT's guide to online privacy*, *supra* note 12 (“Over the past two decades the Internet has grown into a semi-autonomous network where anonymity has been honored. Use of the network, however, generates detailed information about the individual—revealing where they “go” on the Net (via URLs), who they associate with (via list—serves, chat rooms and news groups), and how they engage in political activities and social behavior. Some of the newest tracking tools can so efficiently mine and manipulate the data trail (or ‘clickstream’) people

increasingly common.<sup>20</sup> Unfortunately, the massive data collection regarding a user's online behavior and habits is performed largely *sub rosa*, occurring without the user's knowledge or consent.<sup>21</sup>

Clickstream data gathered by ISPs and online companies could be a fertile source of information for law enforcement. Law enforcement agents could analyze clickstream data<sup>22</sup> for evidence of crime or digital contraband.<sup>23</sup> Such

---

leave behind when they use the Internet that they build a detailed database of personal [sic] information without any human intervention.”).

20. Charles Babcock, *ZDNet Interactive Week: Problems Surface With Data Mining* (last modified February 2, 1999) <<http://www.zdnet.com/intweek/stories/news/0,4164,388207,00.html>> (“Businesses’ desire to generate online customer relationships is a mighty engine in the new electronic economy. It is prompting pioneering businesses, such as Internet service providers, to engage in extensive data mining to individualize the otherwise faceless customer base. . . . A young and aggressive ISP will mine other forms of customer data that falls into its hands in order to buttress the customer relationship and retain customers, according to Larry Goldman, a customer relationship management expert at Braun Technology Group.”).

21. *Federal Trade Commission Staff Report: Online Privacy*, *supra* note 9 (“The fact that online information-gathering is automated means that it is invisible to the user and often takes place without the user’s knowledge and consent.”); *Center for Democracy & Technology: CDT’s guide to online privacy: Terms* (visited February 23, 2000) <<http://www.cdt.org/privacy/guide/terms>> (“The collection of personal information online occurs in two ways. First, information is collected through your active provision of information, such as when you purchase a product online or when you join as a member of a web site. Second, while you are engaged in ‘passive’ online activity—for example when you are lurking in chat rooms, reading bulletin boards, or browsing through online resources—your personal information is also being collected and possibly stored, all under your illusion of anonymity.”); Erika S. Koster, *Zero Privacy: Personal Data on the Internet*, 16 No. 5 *COMPUTER LAW* 7, 7 (1999) (“New technology and more powerful computers now make it possible, without the visitor’s knowledge, for companies to record and track information about visitors to their Web sites . . . .”); Schwartz, *supra* note 1, at 1621–22 (“Visitors to cyberspace sometimes believe that they will be fully able to choose among anonymity, semi-anonymity, and complete disclosure of identity and preferences. Yet, in each of the three areas, finely granulated personal data are created—often in unexpected ways. Moreover, most people are unable to control, and are often in ignorance of, the complex processes by which their personal data are created, combined, and sold.”).

22. The fact that the data may be stored in computers owned by the ISP or another business does not prevent a Web user from retaining a legitimate expectation in the information since the “capacity to claim the protection of the [Fourth] Amendment depends not upon a property right in the invaded place but upon whether the area was one in which there was a reasonable expectation of freedom from governmental intrusion.” *Mancusi v. DeForte*, 392 U.S. 364, 368 (1968). Accordingly, the question is whether the user has a legitimate expectation of privacy in not being tracked online, not whether he or she retains an expectation of privacy in his ISP’s computers.

23. The range of crimes committed on or facilitated by the Internet is virtually limitless. *See, e.g., Note, Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication*, 110 *HARV. L. REV.* 1591, 1591 (1997) (hereinafter “Keeping Secrets”) (“Some crimes actual occur in cyberspace: people can illegally download copyrighted software, gamble, or view obscene photographs. The Internet has facilitated other criminal acts, such as kidnapping, hate crimes, and illegal drug sales. Dangerous information,

searches<sup>24</sup> could be generalized, scanning all clickstreams for evidence of illegal activity,<sup>25</sup> or limited to a specific suspect at a specific time and cyber-location.<sup>26</sup> Law enforcement officers who obtain this data from an ISP or online business would have a powerful investigative tool at their disposal: a record of the entirety of a suspect's online experience. This data would dramatically promote the efficacy and efficiency of police investigation into crimes consummated in or facilitated by cyberspace. Officers could track every step a Net surfer takes from the moment she logs on until she logs off, and could note each site visited, how long she stayed there, whom she "chatted" with, and what she downloaded.<sup>27</sup> Surfers who download child pornography or recipes for methamphetamine or explosives could be easily identified, allowing officers to improve the accuracy of "real world" investigations.

---

such as how to build bomb, infiltrate computer security systems, forge credit cards and phone cards, pick locks, or kill people with one's bare hands is readily available."); Brian Simon, Note, *The Tangled Web We Weave: The Internet and Standing Under the Fourth Amendment*, 21 NOVA L. REV. 941, 959 (1997) ("Aside from hacking, various forms of computer crime now exist. Criminals upload viruses in an attempt to destroy computer systems, steal copyrighted material, and engage in the exchange of child pornography amongst other thing. Private files exist which contain evidence of crime occurring outside cyberspace (the dreaded physical world).").

24. Fourth Amendment jurisprudence is somewhat inconsistent in its use of the term "search." The most widespread school of thought is that a search occurs "when an expectation of privacy that society is prepared to consider reasonable is infringed." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). I do not mean to put the cart before the horse by using the phrase "clickstream search" in my analysis. Instead, I use the term "search" in its plain meaning sense to describe the act of monitoring, examining, or analyzing clickstream data, regardless of whether the Web user ultimately retains a legitimate expectation of privacy.

25. Such a broad search might prove difficult in practice due to the massive amounts of clickstream data generated by Net surfers; even a short online session can generate millions of bytes of information. However, while technological barriers may currently prevent police from conducting a dragnet clickstream, the danger of such searches is becoming increasingly real as data collection and processing technology rapidly advances. Furthermore, law enforcement agencies have empirically shown themselves willing to sort through large amounts of innocuous information in order to unearth evidence of a crime. *See, e.g., Eversole v. Steele*, 59 F.3d 710, 713 (7th Cir. 1995) (describing efforts of regional drug task force to enforce state anti-narcotics laws by monitoring and logging all drug store sales and pharmacy records in a four-county area to determine whether any customers purchased more than four ounces of cough syrup containing codeine within any given forty-eight hour period). Importantly, the difficulty of such a search will undoubtedly be lessened as technology advances, thereby heightening the risk to Net users.

26. The scope of any actual search is irrelevant for purposes of this article. The question is whether a Web user enjoys an expectation of privacy in his or her clickstream. If he or she does not, then a generalized "dragnet" search and a specific targeted search are equally permissible. If he or she retains an expectation of privacy, then the scope of the search is relevant in determining whether the intrusion occasioned by the search is reasonable. However, that inquiry is beyond the scope of the present discussion.

27. *See supra* notes 12, 15, and 19, and accompanying text.

In addition, law enforcement agents could mine clickstream data to create psychological profiles for use at trial to establish intent or motive. Online businesses already use clickstream data to profile users in an effort to determine what types of products a particular user is likely to purchase.<sup>28</sup> Law enforcement using the same data could compile a dossier of a defendant's online behavior replete with potentially incriminating "evidence."<sup>29</sup> For example, the clickstream of a defendant on trial for possession of child pornography could be potentially damning if it showed significant amounts of time spent in cyberspace searching for or viewing pornography. Similarly, a defendant accused of murdering his wife to inherit her assets might be condemned by a clickstream that recorded recent research into "manslaughter" inheritance statutes or intestacy schemes. A third example: the clickstream of a defendant on trial for conspiracy to blow up a government building which logged an excessive amount of time spent on anti-government militia Web sites could provide strong evidence of association or intent.

Although the goals of promoting the accuracy and efficiency of criminal investigations and prosecutions are certainly laudable, courts must take caution in pursuing them in cyberspace. Police discovery of "real world" contraband would certainly be more expeditious if general suspicionless searches of residences were allowed; however, the text of the Fourth Amendment specifically prohibits such searches.<sup>30</sup> General searches of clickstream data should likewise be forbidden. The danger in Internet criminal law is that courts will rigidly adhere to outdated Fourth Amendment concepts which are ill-suited to cyberspace, leading to the conclusion that Web users lack legitimate expectations of privacy in clickstream data.

## II. THE FOURTH AMENDMENT AND THE INTERNET

### A. *A Brief Overview of the Fourth Amendment's Expectation of Privacy and Reasonableness Requirements*

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable

---

28. See *supra* notes 15, 17, and 19, and accompanying text.

29. See, e.g., Koster, *supra* note 21, at 7 ("Psychographic profiles can be made by analyzing a Web surfer's 'click stream,' or listing of sites visited."); Berman & Mulligan, *supra* note 12, at 554 ("The data trail, known as transactional data, left behind as individuals use the Internet is a rich source of information about their habits of association, speech, and commerce. . . . Along with information intentionally revealed through purchasing or registration activities, this transactional data can provide a 'profile' of an individual's activities.");

30. See *infra* notes 83–100, and accompanying text.

searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”<sup>31</sup>

As an initial matter, a defendant raising a Fourth Amendment challenge to a government search or seizure must show that he or she is entitled to the Amendment’s protections by establishing a legitimate expectation of privacy that was infringed upon by the government’s actions.<sup>32</sup> The legitimate expectation of privacy test traditionally entails a two-part inquiry: (1) whether the defendant had an actual (subjective) expectation of privacy; and (2) whether society is prepared to recognize that expectation as reasonable.<sup>33</sup> In analyzing the second question, “[t]he test of legitimacy is not whether the individual chooses to conceal assertedly “private” activity,’ but instead ‘whether the government’s intrusion infringes upon the personal and societal values protected by the Fourth Amendment.’”<sup>34</sup>

The existence of a legitimate expectation of privacy is subject to an important limitation: “[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.”<sup>35</sup> The Supreme Court subsequently expanded upon this principle, first announced in *Katz v. United States*, by holding that a person lacks a legitimate expectation of privacy in information which he or she voluntarily provides to a third party, even if that information is provided in confidence or for business purposes.<sup>36</sup>

If a defendant establishes a legitimate expectation of privacy, the inquiry then becomes whether the government’s intrusion upon that expectation was “reasonable.” The first step in this analysis is to determine whether the intrusion was regarded as an unlawful search and

---

31. U.S. CONST. amend. IV.

32. See *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring); *Rakas v. Illinois*, 439 U.S. 128, 139–40 (1978).

33. See *Smith v. Maryland*, 442 U.S. 735, 740 (1979); *California v. Ciraolo*, 476 U.S. 207, 211 (1986); *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

34. *Ciraolo*, 476 U.S. at 212 (quoting *Oliver v. United States*, 466 U.S. 170, 182–83 (1984)).

35. *Katz*, 389 U.S. at 351–52 (citations omitted).

36. See, e.g., *United States v. Miller*, 425 U.S. 435 (1976) (defendant lacked legitimate expectation of privacy in bank records since he exposed information in records to bank employees); *Smith v. Maryland*, 442 U.S. 735 (1979) (defendant lacked legitimate expectation of privacy in phone numbers dialed from phone since he voluntarily provided the numbers to the telephone company).

seizure when the Amendment was framed.<sup>37</sup> Where this inquiry yields no result, courts must evaluate the search or seizure under traditional standards of reasonableness by weighing the degree to which it intrudes upon an individual's privacy against the degree to which the search or seizure is necessary for the promotion of legitimate governmental interests.<sup>38</sup>

*B. Application of the Fourth Amendment to the Internet has Thus far Been Marked by Reliance on Principles Ill-Suited to Cyberspace, Leading Courts to Conclude that Net Users Lack an Expectation of Privacy in Online Activity*

Very few courts have addressed the applicability of the Fourth Amendment to the Internet. Decisions addressing this topic have focused on an expectation of privacy in two categories: (1) information knowingly passed online to other Web users, and (2) information voluntarily passed offline to ISPs when signing up for Internet service. Both lines of authority conclude that Net users lack legitimate expectations of privacy in the data at issue, either because the information was knowingly exposed to public view or because the Net user assumed the risk that the recipient would share the information with others.

Courts employing assumption of risk analysis focus on the Supreme Court's decisions in *United States v. Miller*<sup>39</sup> and *Smith v. Maryland*.<sup>40</sup> In *Miller*, the Court held that a bank depositor had no legitimate expectation of privacy in transactional records compiled and kept by his bank because he voluntarily conveyed the financial information to his bank, and because this information was exposed to bank employees in the ordinary course of business.<sup>41</sup> According to the Court, "[t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to another . . . even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."<sup>42</sup> The

---

37. See *Florida v. White*, 526 U.S. 559, 562–63 (1999); *Wilson v. Arkansas*, 514 U.S. 927, 931 (1995); *California v. Hodari D.*, 499 U.S. 621, 624 (1991); *Tennessee v. Garner*, 471 U.S. 1, 8 (1985); *Carroll v. United States*, 267 U.S. 132, 149 (1925).

38. See *Wyoming v. Houghton*, 526 U.S. 295, 299–300 (1999); *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 652–53 (1995). See also *Carroll*, 267 U.S. at 149 ("The Fourth Amendment is to be construed in light of what was deemed an unreasonable search and seizure when it was adopted, and in a manner which will conserve public interests as well as the interests and rights of individual citizens.").

39. *United States v. Miller*, 425 U.S. 435 (1976).

40. *Smith v. Maryland*, 442 U.S. 735 (1979).

41. *Miller*, 425 U.S. at 442.

42. *Id.* at 443. See also *Hoffa v. United States*, 385 U.S. 293, 302 (1966). *Miller* has been broadly read as standing for the proposition that a customer has no legitimate expectation of

Supreme Court similarly employed assumption of risk analysis in *Smith* in concluding that a defendant lacked a legitimate expectation of privacy in the numbers dialed on his telephone. Shortly after being robbed, the victim of a robbery started receiving harassing phone calls from a man identifying himself as the robber.<sup>43</sup> Police installed a pen register on Smith's phone after he became the subject of suspicion, and were thereby able to log him making a threatening call to the robbery victim.<sup>44</sup> Smith moved to suppress the evidence, arguing that use of the pen register violated his Fourth Amendment rights.<sup>45</sup> The Court rejected Smith's argument, explaining:

This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties. . . . In *Miller*, for example, the Court held that a bank depositor has no "legitimate 'expectation of privacy'" in financial information "voluntarily conveyed to . . . banks and exposed to their employees in the ordinary course of business." This analysis dictates that petitioner can claim no legitimate expectation of privacy here. When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.<sup>46</sup>

Courts have employed the knowing exposure and the assumption of risk rationales to deny an expectation of privacy in electronic information voluntarily exposed online, such as electronic mail or Internet postings.<sup>47</sup> The few courts to have considered the issue have held that a user retains a legitimate expectation of privacy in e-mail while it is in transmission; however, this expectation evaporates once the e-mail is

---

privacy in records of his business transactions held or created by a third party. *See, e.g.*, *United States v. Phibbs*, 999 F.2d 1053 (6th Cir. 1993) (reading *Miller* to include credit card statements and telephone records regarding defendant kept by various businesses). *Miller* has been harshly criticized by commentators. *See, e.g.*, WAYNE R. LAFAYE, 1 SEARCH AND SEIZURE § 2.7(c) at 631 (3d ed. 1996) ("The result reached in *Miller* is dead wrong, and the Court's woefully inadequate reasoning does great violence to the theory of Fourth Amendment protection which the Court had developed in *Katz*.").

43. *See Smith*, 442 U.S. at 737.

44. *See id.*

45. *See id.*

46. *Id.* at 743–44 (citations omitted).

47. *Katz*, 389 U.S. 347, 351–52 (1967) (citations omitted).

received and read.<sup>48</sup> These courts analogize e-mail to postal mail, and hold that the sender assumes the risk that the recipient will disclose the contents of the e-mail to law enforcement.<sup>49</sup> As the court in *United States v. Charbonneau*<sup>50</sup> explained:

E-mail transmissions are not unlike other forms of modern communication. We can draw parallels from these other mediums. For example, if a sender of first-class mail seals an envelope and addresses it to another person, the sender can reasonably expect the contents to remain private and free from the eyes of police absent a search warrant founded upon probable cause. However, once the letter is received and opened, the destiny of the letter then lies in the control of the recipient of the letter, not the sender, absent some legal privilege. . . . Thus an e-mail message, like a letter, cannot be afforded a reasonable expectation of privacy once that message is received. Moreover, a sender of e-mail runs the risk that he is sending the message to an undercover agent.<sup>51</sup>

Courts have also declined to extend Fourth Amendment protection to electronic postings in Internet chat rooms,<sup>52</sup> since the contents of these communications are knowingly exposed to public view.<sup>53</sup>

---

48. See *United States v. Charbonneau*, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997); *Smyth v. Pillsbury*, 914 F. Supp. 97, 101 (E.D. Pa. 1996); *United States v. Maxwell*, 45 M.J. 406, 417–18 (C.A.A.F. 1996).

49. See *Charbonneau*, 979 F. Supp. at 1184; *Smyth*, 914 F. Supp. at 101; *Maxwell*, 45 M.J. at 417–18. Commentators have made the same analogy. See, e.g., *Keeping Secrets in Cyberspace*, *supra* note 23, at 1597 (“For example, commentators discussing privacy in cyberspace often have compared e-mail to traditional postal mail. Individuals retain a reasonable expectation of privacy in sealed first-class mail sent through the postal system, but because anyone can read the contents of a postcard, an expectation of privacy in its contents would be unreasonable and a law enforcement officer’s reading it is thus not a search. E-mail, which ‘can be accessed or viewed on intermediate computers between the sender and recipient,’ may more closely resemble a postcard than a letter in this regard.”) (footnotes omitted).

50. *Charbonneau*, 979 F. Supp. at 1177.

51. *Id.* at 1184 (quoting *Maxwell*, 45 M.J. at 417).

52. A “chat room” is an Internet site set up to allow Web users to “talk” to each other over the Internet by typing messages on their keyboard. See *Jenkins*, *supra* note 14.

53. See *Charbonneau*, 979 F. Supp. at 1184. See also Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 116 (1994) (“Posting a message in the publicly accessible areas of a BBS can be viewed as either putting the message into ‘plain view,’ or as voluntarily disclosing the information to all other parties. One loses any expectation of privacy in an otherwise private item by placing the item into plain view. As a result, outsiders such as law enforcement officials may monitor BBS communications if those communications are stored or transmitted in a manner that is accessible to the public. Similarly, voluntary disclosure of information to another permits the other party to relay that information to law enforcement personnel without offending the Fourth Amendment.”); Terri Cutrera, *The Constitution in Cyberspace: The Fundamental Rights of Computer Users*, 60

At least two other courts have concluded that Net users surrender any expectation of privacy in personal information voluntarily passed to an ISP when contracting for Internet service.<sup>54</sup> These courts analyzed the issue using the assumption of risk analysis developed in *Miller and Smith*, and concluded that an Internet user assumes the risk that an ISP will disclose sign-up information (including name, address, social security number, and credit card number) to authorities.<sup>55</sup> Significantly, the district court in *United States v. Hambrick* noted that the traditional *Katz* expectation of privacy framework was ill-suited for application to cyberspace; nonetheless, the court applied it to the defendant's motion to suppress sign-up information obtained by law enforcement from the defendant's ISP, and denied the motion because "employees [of the ISP] had ready access to these records in the normal course of [the ISP's] business, for example, in the keeping of its records for billing purposes, and nothing prevent[ed] [the ISP] from revealing this information to nongovernmental actors."<sup>56</sup>

*C. Courts Employing Traditional Fourth Amendment Jurisprudence will Probably Conclude that Net Users Lack a Legitimate Expectation of Privacy in Clickstream Data*

The two-prong *Katz* expectation of privacy test is ill-suited to cyberspace since it fails to take into account the unique nature of the Internet.<sup>57</sup>

---

UMKC L. REV. 139, 151–52 (1991) (concluding that Net users lack legitimate expectation of privacy in "computer service's bulletin board files").

54. ISPs routinely collect personal information when a customer signs up for Internet access. See Schwartz, *supra* note 1, at 1627 ("ISPs are in an advantageous position to tie together the information that exists about anyone who surfs the Web. First, the ISP has highly accurate data about the identity of anyone who uses its services. This information is within its grasp because the ISP generally collects the client's name, address, phone number, and credit card number at the time it assigns an account.").

55. *United States v. Kennedy*, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000); *United States v. Hambrick*, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999).

56. *Hambrick*, 55 F. Supp. 2d at 508 ("Cyberspace is a nonphysical 'place' and its very structure, a computer and telephone network that connects millions of users, defies traditional Fourth Amendment analysis. So long as the risk-analysis approach of *Katz* remains valid, however, this court is compelled to apply traditional legal principles to this new and continually evolving technology.").

57. *Id.* Judicial notions of the parameters of Fourth Amendment protection have traditionally evolved with changing technology. Application of traditional Fourth Amendment principles to the telephone initially yielded results contrary to a modern understanding of the Amendment's protection. In *Olmstead v. United States*, 277 U.S. 438 (1928), the Supreme Court held that the Fourth Amendment was not violated when government agents tapped a telephone line without a warrant since the phone line was not within one of the protected zones specified in the text of the Fourth Amendment: persons, houses, papers, and effects. Forty years later, in *Katz v. United States*, 389 U.S. 347 (1967), the Court held that warrant-

Application of this test to clickstreams will almost certainly lead courts to conclude that Web users lack a legitimate expectation of privacy based upon two rationales: (1) users lack a subjective expectation of privacy in their clickstreams due to private monitoring, and (2) any actual expectation of privacy is objectively unreasonable since Net users assume the risk that their clickstream data will be disclosed to law enforcement.<sup>58</sup> The growing body of authority applying the Fourth Amendment to email, chat room postings, and ISP sign-up information shows courts moving in this direction. Only one court has considered the existence of an expectation of privacy in clickstream data; in a brief opinion, the Fourth Circuit concluded that an employee could not claim Fourth Amendment protection for clickstream data generated while at work because an employment policy put him on notice that his government employer was monitoring his Internet use.<sup>59</sup> Rigid adherence to the two-prong *Katz* expectation of privacy test requires a Net user to establish a subjective expectation of privacy in her clickstream data as a prerequisite for Fourth Amendment protection. However, it will ultimately be impossible for Net users to hold such an expectation due to the lack of privacy protection on the Net.<sup>60</sup> As the fact of clickstream

---

less electronic monitoring of a telephone conversation in a public phone booth constituted an unreasonable search in violation of the Fourth Amendment. The shift in the Court's analysis, from the focus on protecting a "place" in *Olmstead* to the protection of the "person" in *Katz*, was, in part, an acknowledgment that changing technology necessitated new means of constitutional analysis. The unique nature of the Internet again calls for a change in the manner in which courts evaluate the reasonableness of a search or seizure. See, e.g., *Federal Trade Commission Staff Report: Online Privacy: General Practices and Concerns* (September 15, 1997) (visited March 1, 2000) <<http://www.ftc.gov/reports/privacy/privacy3.htm>> ("It is unique among communications media in the variety and depth of personal information generated by its use.").

58. At least one commentator has applied traditional *Katz* analysis and reached this conclusion. See Simon, *supra* note 23, at 967 ("Hypothetically, if the police used a device to track where one travels in cyberspace, there is no reason to think that the use of such technology would constitute a search under the Fourth Amendment. When one travels along the digital highway, such movements are knowingly exposed to the public and merit no Fourth Amendment protection. The digital web where a user journeys would be considered the functional equivalent of the public streets. . . . As long as a user travels along a *public* area in cyberspace, where one can legally view their movements, cyber-tracking devices would not constitute a search.").

59. *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000).

60. Similarly, the court in *Smith* recognized that because the use of telephones was so commonplace, telephone users know or should know that they are disclosing information (numbers dialed) to the telephone company every time they dial, thereby preventing them from harboring any subjective expectation of privacy. See *Smith v. Maryland*, 442 U.S. 735, 742-43 (1979) ("First, we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their

monitoring becomes widely known, Net users will be forced to acknowledge that their transmissions may be monitored by online businesses or ISPs.<sup>61</sup> Instead of leading courts to conclude that clickstream data should be unprotected, courts should instead conclude that the Internet presents the type of situation envisioned by the Supreme Court in *Smith* in which “*Katz*’ two-pronged inquiry would provide an inadequate index of Fourth Amendment protection.”<sup>62</sup>

---

long-distance (toll) calls on their monthly bills. . . . Although subjective expectations cannot be scientifically gauged it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.”).

61. In such a case, clickstream searches might be analogized to searches conducted at open and obvious fixed checkpoints, such as airport metal detectors. These searches are constitutionally permissible since their open and obvious nature eliminates any subjective expectation of privacy by giving the subject notice that a search is certain to occur when he or she enters a controlled area, and because they allow the subject to avoid the search by changing his or her behavior. *See Michigan Department of State Police v. Sitz*, 496 U.S. 444, 463, 473–74 & n.18 (1990) (Stevens, J., concurring) (noting “critical difference” between open and obvious checkpoint searches and other less obvious measures, and discussing permissibility of metal detector searches). *See also McMorris v. Alioto*, 567 F.2d 897, 901 (9th Cir. 1978) (requirement that the public pass through metal detectors before entering courthouses does not unreasonably violate privacy expectations because search is obvious and public has choice not to enter); *United States v. Doran*, 482 F.2d 929, 932 (9th Cir. 1973) (no expectation of privacy infringed upon by airport metal detectors). While facially appealing, this analogy fails to recognize that a clickstream search is significantly more invasive than a metal detector or magnetic strip scan. Unlike traditional fixed searches, which look only for particular contraband or criminal activity, clickstream monitoring tracks the entirety of an individual’s online activity. This distinction is significant: while an individual can still choose to avoid the search by “opting out” of Internet use, the extensiveness of the potential search is much more likely to change an individual’s lawful behavior than a metal detector. For example, an outwardly heterosexual man may be deterred by the prospect of a clickstream search from legally entertaining homosexual fantasies online in adult chat rooms for fear of being “outed.” Fringe political groups may become wary of using the Internet to advocate lawful political change over the Internet, or use the Web to engage in legal fund-raising activity. While these concerns are better addressed under the First Amendment than the Fourth, the potential chilling effect on all types of online behavior illustrates the inadequacy of an analogy to metal detectors or fixed checkpoints since those types of searches are limited to curtailing a particular illegal activity. *See also Keeping Secrets*, *supra* note 23, at 1607–08 (“A free society demands free discourse, and free discourse requires the ability to communicate privately. If our polity is to engage in vibrant political debate, if our marketplace of ideas is to remain open to radical and innovative suggestions, we must ensure that citizens can speak both freely and privately. Some of our most cherished communications—whispers between lovers, vows between friends—would be stifled if government officials had unbounded discretion to eavesdrop. This necessarily private communication has already moved into cyberspace, and by all accounts will continue to do so in the future. Communication in cyberspace must be protected to the same extent as is more traditional communication if our advancing communication technology is to achieve its full potential without the sacrifice of any of the free speech or privacy that we enjoy today.”) (footnotes omitted).

62. *Smith*, 442 U.S. at 740 n.5. *See also*, Bayens, *supra* note 4, at 278 (“Even relatively novice computer users understand that employers, Internet service providers, and hackers can easily monitor electronic transmissions. However, this recognition should not operate as a bar to Fourth Amendment protections. Electronic communication in its various forms is a practi-

Application of the assumption of risk principle to online expectation of privacy issues is similarly flawed because the principle fails to take into account the extent of intrusion made possible by clickstream data. There is a significant qualitative difference between clickstream data and other types of transactional data routinely provided to third parties in the course of business. A police officer who learns that a suspect has called a particular phone number, as in *Smith*, knows only that a call was made; the number is content neutral, and does not give the officer a means to reconstruct the suspect's conversation.<sup>63</sup> Similarly, an officer who searches bank records, as in *Miller*, learns only that transactions were made, and by whom; he or she does not learn the underlying circumstances of the transactions. In contrast, an Internet address, while itself content neutral, allows an officer to view the same information that the suspect viewed. The clickstream, a record of a person's cyberspace activity, allows officers to entirely recreate an online experience.<sup>64</sup>

Instead, clickstream data is better analogized to library records which reveal the titles of books read by library patrons.<sup>65</sup> Using such records, officers could view the same content viewed by the suspect. Officers could potentially reconstruct the suspect's interactions in the library by interviewing other patrons or reviewing security camera tapes. However, even this analogy significantly underestimates the intrusiveness of a clickstream search. An Internet user's clickstream reveals not only what sites were visited, but also for how long each site was visited, how often each site was re-visited, and which links were followed from each site. A comparable level of knowledge in the concrete world would

---

cal necessity despite its inherent dangers. Thus, the judiciary or legislature must acknowledge this dilemma and formulate appropriate responses.”).

63. As the Court noted in *Smith*, “a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications.” 442 U.S. at 741.

64. The revealing nature of clickstream data has been recognized by leading online privacy advocates. See *Center for Democracy & Technology: CDT's guide to online privacy: Terms*, *supra* note 21 (“Personally identifiable transactional data is the information describing your online activities, including web sites you have visited, whom you have sent email, what files you have downloaded, and other information revealed in the normal course of using the Internet. Transactional data differs from the content of a communication in that it is not the actual substance of your communication, but the information about your communication. Traditionally, the content of your communications has received greater protections in the law that [sic] transactional data. Recent developments in the law have given greater protections to transactional data in that *it is just as revealing as the content of your communications.*”) (emphasis added).

65. See LaFave, *supra* note 42, at 633 n.61 (questioning whether officers can access library records after *Miller*, and suggesting that disclosure of library use information might properly take place under “judicial supervision” which regulated the State's activities to eliminate content bias and required showing that suspect's reading practices were relevant to criminal act under investigation) (citation omitted).

require that the officers know not only which books the suspect borrowed, but also when she read the books, how long she spent reading each book and each page, and the sequence in which she read each book and each page. Furthermore, clickstream data, unlike the hypothetical library search, is not subject to poor witness memory.

The assumption of risk doctrine is further ill-suited to clickstream data since a Net user seldom knows the type or extent of data being collected by Web sites or ISPs.<sup>66</sup> In addition, clickstream data is often unwillingly exposed. Recent studies indicate that the majority of Net users dislike clickstream data collection by online companies.<sup>67</sup> It is logically infirm to hold that a person surrenders his or her expectation of privacy in clickstream data when he or she neither knows nor intends to expose such information to public view. As Justice Marshall explained in his dissent in *Smith*, “[i]mplicit in the concept of assumption of risk is some notion of choice.”<sup>68</sup> Application of the assumption of risk principle to involuntary data collection is contrary to the values the Fourth Amendment was intended to protect.<sup>69</sup>

---

66. See *supra* note 21 and accompanying text, explaining that clickstream data collection often occurs without the user’s knowledge.

67. A recent study by AT&T found that an overwhelming majority of Web users particularly disliked automated data collection services which provided them with no notice that data was being collected as they surfed the Net. *AT&T online press release: Survey: ‘One-Size-Fits-All’ Privacy Won’t Work on ‘Net* (last modified April 14, 1999) <<http://www.research.att.com/projects/privacystudy/press.htm>> (“Users dislike automatic data transfer and unsolicited communications. When asked about possible browser features that would make it easier to provide information to a Web site, 86 percent reported no interest in doing so without their taking some action.”). See also Bob Tedeschi, *Targeted Marketing Confronts Privacy Concerns*, N.Y. TIMES (last modified May 10, 1999) <<http://www.nytimes.com/library/tech/99/05/cyber/commerce/10commerce.html>> (“[R]ecent surveys indicat[e] that Internet users are increasingly uncomfortable with the amount of personal data gathered by online companies, and as online companies become more aggressive about collecting that information.”); *Federal Trade Commission Staff Report: Online Privacy: General Practices and Concerns*, *supra* note 9 (“Survey results suggest that although many individuals are willing to strike a balance between maintaining personal privacy and obtaining the information and services that new interactive technologies provide, they are concerned about potential misuse of their personal information and want meaningful and effective protection of that information. In the 1994 Harris Survey, fifty-one percent of respondents stated they would be concerned if an interactive service to which they subscribed engaged in ‘subscriber profiling,’ i.e., the creation of individual profiles based upon subscribers’ usage and purchase patterns, in order to advertise to subscribers.”).

68. *Smith*, 442 U.S. at 749–50 (Marshall, J., dissenting).

69. As one commentator warns, “The *Katz* decision . . . included limiting language which specified that a person could not have a reasonable expectation of privacy in things that were ‘knowingly expose[d] to the public.’ . . . The Supreme Court has used the ‘knowing exposure’ rationale to transform the reasonable expectation of privacy standard into a simple assumption of risk test. . . . In its evolved form, the *Katz* privacy test has become a roadblock to fourth amendment protection instead of a roadmap for ensuring it. It strips the individual of a great measure of fourth amendment protection—the single most important characteristic

Nonetheless, there are indications that courts will apply the subjective expectation of privacy and assumption of risk principles to clickstream data. As discussed above, these principles have already been applied to email, chat room postings, and sign-up information provided to ISPs. The only court to thus far address expectations of privacy in clickstream data held that a Web user lacked an expectation of privacy in clickstream data generated while at work since he had notice that his Internet usage was being monitored. In *United States v. Simons*,<sup>70</sup> the Fourth Circuit considered whether an employee retained a legitimate expectation of privacy in records of his Internet use from work in light of a policy implemented by his employer, the Foreign Bureau of Information Services,<sup>71</sup> which warned employees that all Internet activity in the workplace would be monitored and recorded.<sup>72</sup> Applying the traditional two-prong *Katz* test, the court concluded that the policy stripped the defendant of any expectation of privacy by putting him on notice that his online activity was not private:

Simons did not have a legitimate expectation of privacy with regard to the record or fruits of his Internet use *in light of the FBIS Internet policy*. . . . The policy placed employees on notice that they could not reasonably expect that their Internet activity would be private. Therefore, regardless of whether Simons subjectively believed that the files he transferred from the Internet were private, such a belief was not objectively reasonable after FBIS notified him that it would be overseeing his Internet use.<sup>73</sup>

*Simons* is frightening because it could potentially be read as eliminating an expectation of privacy in clickstream data whenever the user knows or should know that his or her clickstream is being monitored. As discussed above, the rapid development of data tracking technology and data mining practices make it virtually inevitable that the capacity will soon exist to monitor and record all online activity. As this technology becomes commonplace, so too will public knowledge of its use. In such

---

which distinguishes a free society from a police state—simply as a result of living in a high-tech society. Its result is to strip the fourth amendment of its normative values which were intended to regulate and limit the powers of government.” Lewis R. Katz, *In Search of A Fourth Amendment for the Twenty-First Century*, 65 *IND. L.J.* 549, 564 (1990).

70. *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000).

71. The FBIS is a division of the Central Intelligence Agency. *Id.* at 395.

72. *Id.* at 395–96.

73. *Id.* at 398 (emphasis added). See also *United States v. Monroe*, 52 M.J. 326 (C.A.A.F. 2000) (acknowledging that military serviceman retained legitimate expectation of privacy in email while it was in transmission, but holding that he lacked expectation of privacy in email stored in electronic mailbox on government Internet server when government computer use policy warned him that his account was subject to monitoring).

a world, *Simons* could be read for the proposition that a Net user enjoys no expectation of privacy in clickstream data.

Such a broad reading of *Simons* is improper. Importantly, a government agency was defendant *Simons*'s employer; in light of the Internet use policy, *Simons* was knowingly and voluntarily exposing his clickstream data directly to the government.<sup>74</sup> Furthermore, *Simons* does not stand for the proposition that the government can place the clickstream data of non-government employees beyond the reach of the Fourth Amendment merely by announcing that it is subject to monitoring. As the Supreme Court explained in *Smith*, a nationwide announcement by the government proclaiming that all homes are henceforth subject to warrantless entry would not defeat a homeowner's legitimate expectation of privacy.<sup>75</sup> In addition, even if *Simons* establishes that Web users who know that their clickstreams are monitored lack a subjective expectation of privacy, this is not necessarily fatal to a legitimate expectation of privacy.<sup>76</sup>

### III. ESTABLISHING A LEGITIMATE EXPECTATION OF PRIVACY IN CLICKSTREAM DATA

Unfortunately, the doctrinal basis for finding an expectation of privacy in clickstream data is far from clear. As discussed above, application to the Internet of contemporary expectation of privacy jurisprudence might well lead courts to conclude that Net users lack an

---

74. The fact that ISPs and online businesses are collecting clickstream data instead of the government may ultimately require a defendant to establish that these actors are government agents in order to obtain suppression. That issue is beyond the scope of this article.

75. See *Smith v. Maryland*, 442 U.S. 735, 740 n.5 (1979) ("Situations can be imagined, of course, in which *Katz*'s two-pronged inquiry would provide an inadequate index of Fourth Amendment protection. For example, if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects. Similarly, if a refugee from a totalitarian country, unaware of this Nation's traditions, erroneously assumed that police were continuously monitoring his telephone conversations, a subjective expectation of privacy regarding the contents of his calls might be lacking as well. In such circumstances, where an individual's subjective expectations had been 'conditioned' by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was. In determining whether a 'legitimate expectation of privacy' existed in such cases, a normative inquiry would be proper.")

76. Web users can retain a legitimate expectation of privacy in some instances even in the absence of a subjective expectation of privacy. See *Smith*, 442 U.S. at 740 n.5. See also *Hudson v. Palmer*, 468 U.S. 517, 525 n. 7 (1984) (noting that Supreme Court has always emphasized objective over subjective prong of *Katz* test).

expectation of privacy in clickstream data. Such a result is clearly incorrect.

Courts foraying into cyberspace must shift their focus away from the two-prong *Katz* expectation of privacy test in order to preserve the values underlying the Fourth Amendment. In developing a new framework for expectation of privacy analysis in cyberspace, courts should focus on the historic context of the Fourth Amendment and the intent of its Framers. Government monitoring and analysis of clickstream data is closely analogous to the general searches which the Framers sought to curtail in enacting the Fourth Amendment. Both types of searches are indiscriminate, exposing lawful activity along with contraband or unlawful action. Both are also incredibly intrusive, exposing intimate details about the lives of citizens to government scrutiny. A new rule needs to be established which recognizes that clickstream data may be protected by the Fourth Amendment, not because that protection fits well with expectation of privacy analysis as developed by the Court in recent years, but rather because government clickstream analysis is precisely the type of search the Framers intended to be subject to the Amendment's limitations.

Courts addressing this question should apply the normative analysis set forth by the Supreme Court in *Smith v. Maryland* instead of the rigid two-prong *Katz* test. The Court in *Smith* recognized that the two-prong *Katz* expectation of privacy test will sometimes provide "an inadequate index of Fourth Amendment protection."<sup>77</sup> In such situations, the Court explained, courts must undertake a normative inquiry to determine whether Fourth Amendment protection was appropriate.<sup>78</sup> This normative inquiry asks a very simple question: should an individual in a free and open society be forced to assume the risk that the government will monitor her as she engages in the activity at issue?<sup>79</sup> Courts employing the normative inquiry "must evaluate the 'intrinsic character' of investigative practices with reference to the basic values underlying the Fourth Amendment."<sup>80</sup> Unlike the two-prong test, which assumes that society has already reached an objective conclusion about the proper amount of

---

77. *Smith*, 442 U.S. at 741 n.5.

78. *Id.*

79. *See Smith*, 442 U.S. at 750–51 (Marshall, J., dissenting). *See also California v. Ciraolo*, 476 U.S. 207, 220 n.5 (1986) (Powell, J., dissenting) (stating that legitimate expectation of privacy determination "necessarily focuses on personal interests in privacy and liberty recognized by a free society"); *Vega-Rodriguez v. Puerto-Rico Telephone Co.*, 110 F.3d 174, 180 n.4 (1st Cir. 1997) ("In cases in which notice would contradict expectations that comport with traditional Fourth Amendment freedoms, a normative inquiry is proper to determine whether the privacy expectation is nonetheless legitimate.").

80. 442 U.S. at 750–51 (Marshall, J., dissenting).

protection a particular activity deserves, the normative test acknowledges that society has not reached a consensus about the proper level of protection a certain activity warrants. In that case, the activity can be evaluated against constitutional norms.<sup>81</sup>

Application of *Smith's* normative inquiry to clickstreams reveals that Net users should retain an expectation of privacy in clickstreams because this data is precisely the type of information the Framers sought to protect against arbitrary government intrusion.<sup>82</sup> The Fourth Amendment was intended to limit government searches which held the potential to intrude into the intimate details of the private lives of citizens; courts must recognize a legitimate expectation of privacy in the intimate records of our online activity in order to satisfy these constitutional norms.

The passage of the Fourth Amendment was the Framers' reaction to overly intrusive searches and seizures conducted by British and colonial authorities. Prior to the Amendment's passage, the colonists were plagued by the use of general warrants and writs of assistance which authorized law and customs enforcement officers to enter and search any building suspected of housing contraband.<sup>83</sup> The searches conducted

---

81. See also *Keeping Secrets*, *supra* note 23, at 1607 ("The truth is that the application of *Katz* to new technology is simultaneously normative and descriptive. Deciding which expectations of privacy are reasonable is not simply an empirical determination, but rather requires a judgment about the kind of society in which we want to live; in determining 'reasonable expectations,' we cannot divorce the level of privacy that the Constitution does protect from a judgment about how much privacy our society ought to protect. The Fourth Amendment balances the individual's claim to privacy against the societal demand for effective law enforcement.") (citations omitted).

82. Although discussion of the types of searches and seizures the Fourth Amendment is intended to cover is typically undertaken as part of the "reasonableness" inquiry, see, e.g., *Wilson v. Arkansas*, 514 U.S. 927, 931 (1995), it would clearly be improper to deny a defendant the opportunity to raise a Fourth Amendment defense to a search of the type the Framers intended to prohibit merely because courts have developed a Fourth Amendment jurisprudence which is ill-suited to a new communications technology.

83. General warrants allowed authorities to conduct searches and seizures without particularized suspicion as to place or contraband. See NELSON LASSON, *THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION* 26 (1976) (describing content and service of general warrants: "Persons and places were not necessarily specified, seizure of papers and effects was indiscriminate, everything was left to the discretion of the bearer of the warrant."). Writs of assistance, designed to help enforce customs laws, were even more intrusive than general warrants since they typically granted officers unlimited discretion in conducting searches and seizures. LEONARD W. LEVY, *ORIGINAL INTENT AND THE FRAMERS' CONSTITUTION* 227 (1988) (detailing 'writs of assistance' which gave customs agents and law enforcement officials broad power to search for and seize any untaxed goods, and explaining that these warrants lasted for the life of the sovereign and could be used without any showing of particularized suspicion); Barbara C. Salken, *The General Warrant of the Twentieth Century? A Fourth Amendment Solution to Unchecked Discretion to Arrest for Traffic Offenses*, 17 PACE L. REV. 97, 144 (1997) ("Writs of assistance were used extensively in the colonies in the 1760s and were a principal irritant to the colonists. The writs were even more offensive than the general warrants, which had at least

using these devices were broad and abusive, occurred without particularized suspicion and were led by executive officials with unlimited discretion.<sup>84</sup> For example, the New Hampshire Council once allowed search warrants for “all houses, warehouses, and elsewhere in this Province”; the Pennsylvania Council once required a weapons search of “every house in Philadelphia.”<sup>85</sup> Far from being isolated instances, such searches were widespread.<sup>86</sup>

In response to these abuses, the Framers sought to limit the power of government actors to search or seize persons, houses, papers, and effects.<sup>87</sup> The invasion the Framers sought to prohibit was not merely the

---

been directed at the perpetrators of a particular offense; writs of assistance permitted unlimited discretion and . . . were designed to prevent the American colonies from trading outside the Empire.”). One scholar has suggested that the widespread use of writs of assistance was the prime cause of the American Revolution. *See* Salken, *supra* at 144–45 (“The relationship of the revolution to the writs is clear. John Adams, who had been a young courtroom spectator during the argument in the writs-of-assistance case, later, wrote: ‘Mr. Otis’ oration against the Writs of Assistance breathed into this nation the breath of life. [H]e was a flame of fire. Every man of a crowded audience appeared to me to go away, as I did, ready to take arms against writs of assistance. Then and there was the first scene of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born. In 15 years, namely in 1776, he grew to manhood, and declared himself free.’”) (citations omitted).

84. William J. Cuddihy & B. Carmon Hardy, *A Man’s House Was Not His Castle: Origins of the Fourth Amendment to the United States Constitution*, 37 WM. & MARY Q. 371, 372 (1980) (explaining that colonists were subject to forcible intrusion by British officials acting under authority of general warrants and writs of assistance); Phoebe Weaver Williams, *Governmental Drug Testing: Critique and Analysis of Fourth Amendment Jurisprudence*, 8 HOFSTRA LAB. L.J. 1, 39 (1990) (“During the period when the English were struggling to free themselves from indiscriminate searches, the American colonists were being subjected to broad and abusive searches.”).

85. Tracey Maclin, *Informants and The Fourth Amendment: A Reconsideration*, 74 WASH. U. L.Q. 573, 583 (1996) (citation omitted).

86. *Id.* at 581 (“The general warrant, or something resembling it, was the usual protocol of search and arrest everywhere in colonial America, excepting Massachusetts after 1756.”); Levy, *supra* note 83, at 224 (noting that 106 of the 108 warrants issued in period of 1700–1763 were general warrants).

87. *Stanley v. Georgia*, 394 U.S. 557, 569 (1969) (Stewart, J., concurring) (“The purpose of these clear and precise words [in the Fourth Amendment] was to guarantee to the people of this Nation that they should forever be secure from the general searches and unrestrained seizures that had been a hated hallmark of colonial rule under the notorious writs of assistance of the British Crown.”); *Stanford v. Texas*, 379 U.S. 476, 481 (1965) (“These words [of the Fourth Amendment] are precise and clear. They reflect the determination of those who wrote the Bill of Rights that the people of this new Nation should forever ‘be secure in their persons, houses, papers, and effects’ from intrusion and seizure by officers acting under the unbridled authority of a general warrant. Vivid in the memory of the newly independent Americans were those general warrants known as writs of assistance under which officers of the Crown had so bedeviled the colonists.”). *See also*, Cuddihy & Hardy, *supra* note 84, at 372 (stating that the Fourth Amendment’s protections “arose from the harsh experience of householders having their doors hammered open by magistrates and writ-bearing agents of the crown. Indeed, the Fourth Amendment is explainable only by the history and memory of such abuse”); Williams, *supra* note 84, at 39 (“The fourth amendment was the Framers’ response to broad

physical intrusion upon a “person” or “house.” Instead, “the amendment’s opposition to unreasonable intrusion . . . sprang from a popular opposition to the surveillance and divulgement that intrusion made possible.”<sup>88</sup> As one scholar explained, “[t]he objectionable feature of general warrants was their indiscriminate character.”<sup>89</sup> In addition to any contraband or unstamped goods that the generalized searches uncovered, the entirety of a person’s private life was exposed to prying government eyes. This sort of indiscriminate search stripped the colonists of privacy without adequate justification, exposing them to the arbitrary and potentially despotic acts of government officials.<sup>90</sup>

Monitoring and analysis of clickstreams by government officials is closely analogous to colonial general searches because it exposes the intimate lives of Web users, fails to discriminate between lawful and unlawful activity, and grants enormous discretion to front-line executive officials. As with general searches of colonial homes, clickstream searches will unnecessarily reveal private information to government view, even when this information pertains to lawful activity. For example, law enforcement agents monitoring clickstreams could learn that an outwardly heterosexual man spends time entertaining homosexual fantasies online in an adult chat room, or that a high-profile political leader used the Internet to reserve a spot in an addiction recovery center.<sup>91</sup> While such conduct is certainly legal, it is also intensely private. Allowing government agents to expose the conduct of the innocent in order to pursue the guilty contradicts the purpose and intent of the Fourth Amendment.<sup>92</sup>

---

and abusive searches conducted by the British government.”); Tracey Maclin, *When the Cure for the Fourth Amendment Is Worse than the Disease*, 68 S. CAL. L. REV. 1, 11–13 (1994) (arguing that the Fourth Amendment was the framers’ reaction to a historical period where government actors demonstrated little respect for individual privacy).

88. William J. Cuddihy, *The Fourth Amendment: Origins and Original Meaning* 602, 1546 (1990) (unpublished Ph.D. dissertation, Claremont Graduate School).

89. Salken, *supra* note 83, at 145. *See also* *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971) (acknowledging that colonist’s chief objection to general warrants was “not that of the intrusion *per se*, but of a general, exploratory rummaging in a person’s belongings”).

90. *See* Anthony Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 411 (1974).

91. The litany of potential abuses is limitless since the proliferation of Web sites and services now allows Web users to engage in virtually any activity online. The development of online voting for political office highlights the danger of an indiscriminate clickstream search: law enforcement officers analyzing a suspect’s clickstream might well learn the way he or she voted in a cyber-election. *See Arizona Democrats* (visited May 15, 2000) <<http://www.azdem.org/breakdown.html>> (describing first binding Internet election in Arizona’s Democratic presidential primary in which 35,765 people cast official votes online).

92. *See* *United States v. Rabinowitz*, 339 U.S. 56, 82 (1950) (Frankfurter, J., dissenting) (“By the Bill of Rights the founders of this country subordinated police action to legal restraints, not in order to convenience the guilty but to protect the innocent.”).

On a more general level, the broad and arbitrary intrusion occasioned by a clickstream search is contrary to “the most basic values underlying the Fourth Amendment.” Although the use of general warrants and writs of assistance undoubtedly motivated the Framers in drafting the Amendment, they did not intend its protection to be limited to the narrow purpose of outlawing general searches.<sup>93</sup> Instead, the Amendment was intended to protect citizens against the type of arbitrary invasions by government into the lives of citizens which general searches typified.<sup>94</sup> As one commentator explained:

While the history of the Fourth Amendment reveals many facets, one central aspect of that history is pervasive: controlling the discretion of government officials to invade the privacy and security of citizens, whether that discretion be directed toward the homes and offices of political dissentients, illegal smugglers, or ordinary criminals.<sup>95</sup>

Similarly, the Supreme Court has repeatedly recognized that the harm the Fourth Amendment seeks to prevent is not the tangible inva-

---

93. *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 669 (1995) (O’Connor, J., dissenting) (“[W]hat the Framers of the Fourth Amendment most strongly opposed . . . were general searches. . . . [T]hese various forms of authority led in practice to ‘virtually unrestrained,’ and hence ‘general,’ searches. To be sure, the Fourth Amendment, in the Warrant Clause, prohibits by name only searches by general warrants. But that was only because the abuses of the general warrant were particularly vivid in the minds of the Framers’ generation, and not because the Framers viewed other kinds of general searches as any less unreasonable.”) (citations omitted); *Stanford v. Texas*, 379 U.S. 476, 482 (1965) (“But while the Fourth Amendment was most immediately the product of contemporary revulsion against a regime of assistance, its roots go far deeper. Its adoption in the Constitution of this new Nation reflected the culmination in England a few years earlier of a struggle against oppression which had endured for centuries.”). *See also* Maclin, *supra* note 85, at 582 (“The newly emerging ‘Americanization’ of the right against unreasonable search and seizure was not confined to rejection of the general warrant. Other types of intrusion were also deemed unreasonable. For example, nocturnal searches were universally condemned. . . . Unannounced entries were also denounced.”).

94. Numerous scholars have recognized that the Fourth Amendment was prefaced on the broad purpose of protecting citizens against arbitrary governmental intrusion on personal privacy. *See, e.g.*, Maclin, *supra* note 85, at 584–85 (“Although it did not explicitly outlaw all discretionary searches and seizures, the [Fourth] Amendment initiated and symbolized an ideal that was uniquely American – discretionary invasions of privacy and personal security, whether by warrant or without, violated constitutional liberty. . . . [W]e should remember that the Fourth Amendment was designed to check the discretionary power of government to invade individual privacy and security”); Thomas K. Clancy, *The Role of Individualized Suspicion in Assessing the Reasonableness of Searches and Seizures*, 25 U. MEM. L. REV. 483, 528 (1995) (“The core complaint of the colonists was not that searches and seizures were warranted, warrantless, or unauthorized actions; it was the general, suspicionless nature of the searches and seizures. . . . As they sought to regulate searches and seizures, the framers held certain principles to be fundamental, of which particularized suspicion was in the first rank.”).

95. Maclin, *supra* note 85, at 585 n.53.

sion of one's person, papers, effects, or home, but rather the intangible invasion upon the sanctity and privacy of those objects occasioned by an unreasonable search or seizure.<sup>96</sup>

The indiscriminate nature of clickstream searches illustrates their incompatibility with the values upon which the Fourth Amendment was based. As one scholar argued:

The first [problem with indiscriminate searches] is that they expose people and their possessions to interferences by government when there is no good reason to do so. The concern here is against unjustified searches and seizures: it rests upon the principle that every citizen is entitled to security of his person and property unless and until an adequate justification for disturbing that security is shown. The second [problem] is that indiscriminate searches and seizures are conducted at the discretion of executive officials, who may act despotically and capriciously in the exercise of the power to search and seize. This latter concern runs against arbitrary searches and seizures; it condemns the petty tyranny of unregulated rummagers.<sup>97</sup>

---

96. An arbitrary or excessive intrusion upon personal sanctity and privacy by government officials was widely considered the hallmark of an unreasonable search and seizure at the time the Fourth Amendment was adopted. In *Boyd v. United States*, 116 U.S. 616, 630 (1885), the Court explained that the values underlying the Fourth Amendment were shaped by English common law, particularly Lord Camden's opinion in *Entick v. Carrington*, 19 How. St. Tr. 1029 (1765), stating:

The principles laid down in this opinion affect the very essence of constitutional liberty and security. . . . [T]hey apply to all invasions on the part of the government and its employees of the sanctity of a man's home and the privacies of life. It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty and private property, where that right has never been forfeited by his conviction of some public offense,—it is the invasion of this sacred right which underlies and constitutes the essence of Lord Camden's judgment.

116 U.S. at 630. The Court emphasized that these principles were in the forefront of the minds of the Framers when the Fourth Amendment was drafted.

As every American statesman during our revolutionary and formative period as a nation was undoubtedly familiar with this monument of English freedom, and considered it as the true and ultimate expression of constitutional law, it may be confidently asserted that its propositions were in the minds of those who framed the Fourth Amendment to the Constitution, and were considered as sufficiently explanatory of what was meant by unreasonable searches and seizures.

*Id.* at 626. See also *Camara v. Municipal Court*, 387 U.S. 523, 528 (1967) (“The basic purpose of [the Fourth] Amendment . . . is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials”); *Davis v. Mississippi*, 394 U.S. 721, 726 (1969) (“Nothing is more clear than that the Fourth Amendment was meant to prevent wholesale intrusions upon the personal security of our citizenry.”).

97. Amsterdam, *supra* note 90, at 411.

Absent an expectation of privacy in clickstream data, law enforcement agents will be free to rummage through our online lives, revealing intensely private conduct. The Framers found the ability to conduct such arbitrary and suspicionless searches to be one of the most offensive aspects of general warrants and writs of assistance,<sup>98</sup> and clearly intended such searches to be illegal.<sup>99</sup> Allowing such intrusions into private cyberspace activity merely because an outdated expectation of privacy test would find assumption of risk or the absence of a subjective expectation of privacy in clickstream data does intense violence to the values underlying both the Fourth Amendment and a free society.<sup>100</sup> Yet this is exactly the result that will be reached if courts continue to cling to *Katz*'s two part test.

Once an expectation of privacy is established in clickstream data, traditional Fourth Amendment principles regulating the reasonableness of searches and seizures can easily be applied. The traditional test of reasonableness, which balances the nature and quality of the intrusion upon an individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion,<sup>101</sup> is perfectly suited for cyberspace. This test allows courts to protect against overly extensive and indiscriminate intrusion into our online lives while also acknowledging that a sufficiently compelling governmental interest may justify such searches. This is the question that should be getting asked in every clickstream search; however, it will never be asked until courts loosen their vise grip on the two-prong *Katz* test and decide that Internet users should retain a legitimate expectation of privacy in clickstream data.

---

98. Lasson, *supra* note 84, at 26 (explaining that with general warrants, "everything was left to the discretion of the bearer of the warrant"); Salken, *supra* note 83, at 144 (explaining that writs of assistance granted their bearers "unlimited discretion" in conducting searches and seizures).

99. Maclin, *supra* note 85, at 579 (arguing that the framers intended "general searches and seizures [to be] illegal on their face").

100. *Wolf v. Colorado*, 338 U.S. 25, 27 (1949) ("[T]he security of one's privacy against arbitrary intrusion by the police—which is at the core of the Fourth Amendment—is basic to a free society.").

101. *See, e.g., Tennessee v. Garner*, 471 U.S. 1, 7–8 (1985); *United States v. Place*, 462 U.S. 696, 703 (1983).