EMORY | LAW

Emory Law Journal

Volume 61 | Issue 3

2012

# Big Brother Gets A Makeover: Behavioral Targeting and the Third-Party Doctrine

Elspeth A. Brotherton

# BIG BROTHER GETS A MAKEOVER: BEHAVIORAL TARGETING AND THE THIRD-PARTY DOCTRINE


## ABSTRACT

*A staggering 239 million Americans have access to the Internet and spend, on average, sixty hours each month online, visiting some 2646 websites. What few Internet users realize is that, during the time they surf the Web, they are subjected to constant surveillance by potentially hundreds of different private companies. These companies, called advertising networks, track Internet users across the Web, collecting all sorts of personal information about them—their gender, age, income, location, medical concerns, sexual orientation, political affiliations, and music preferences, among many other things. Advertising networks then use this information to deliver highly personalized online advertisements to Internet users, a process known as behavioral targeting.*

*But advertising networks can use the information they collect for purposes beyond behavioral targeting. In addition to exploiting Internet users' information to deliver targeted advertisements, ad networks sell the information to third parties, which could include, perhaps surprisingly, the government. Armed with detailed records about Internet users and their online activities, the government has unprecedented access to the most intimate details of peoples' lives. What seems such a gross invasion of privacy can occur despite the Fourth Amendment's prohibition against unreasonable searches and seizures by the government. The Fourth Amendment likely does not apply to information gathered for behavioral targeting because of what is known as the "third-party doctrine." Under the third-party doctrine, the Fourth Amendment does not protect any information a person volunteers to a third party, because that person presumptively has assumed the risk that the third party will reveal the information to the government.*

*This Comment explores why the third-party doctrine would apply in the context of behavioral targeting, resulting in an unprecedented threat to Americans' privacy. Arguing that the Supreme Court's justification for the doctrine is inherently flawed, this Comment sets forth a new way of conceptualizing the third-party doctrine and a corresponding analytical framework called the "competing-interests test." The competing-interests test ultimately seeks to reconcile the conceptual difficulties that arise when*

*applying the doctrine not only within the context of behavioral targeting but in all situations in which a third party holds information about another person.*

## INTRODUCTION

Justice Brandeis once predicted that, in the future, "[w]ays may . . . be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose . . . the most intimate occurrences of the home. Advances in . . . sciences may bring means of exploring unexpressed beliefs, thoughts and emotions."[1] Justice Brandeis's warning, from his famous dissenting opinion in *Olmstead v. United States*,[2] perhaps seemed far-fetched in 1928 when it was published. Eighty-four years later, however, the Justice's prediction has proven startlingly insightful, if not frighteningly accurate. Indeed, true to Justice Brandeis's vision, in the last decade the government has developed a powerful tool for not only exploring but also exploiting peoples' "unexpressed beliefs, thoughts and emotions." That tool is the Internet—or,

[1] Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

[2] 277 U.S. 438.

more precisely, the capacity to indirectly track individuals on the Internet through private companies that conduct "behavioral targeting."

Behavioral targeting is an online advertising technique designed to deliver specific, targeted advertisements to Internet users based on their perceived interests. Companies that conduct behavioral targeting, known as advertising networks, are able to predict Internet users' interests by using sophisticated technology that tracks and gathers information about users' online activity.[3] The resulting targeted ads are approximately twice as effective as—and, therefore, much more valuable than—other forms of online advertisements.[4] As a result, online content providers can fund their entire operations with revenues from selling online advertising space, making it possible for websites to offer online content for an unbeatable price—for free.

Over the last decade, behavioral targeting has proven increasingly important, if not essential, as a means of supporting free content on the Internet. According to industry experts, targeted ads "significantly enhanc[e] the advertising revenue engine driving the growth of the Internet"[5] and are a critical component of "the economic model supporting free online content and services for consumers."[6] But describing behavioral-targeting-supported online content as "free" is somewhat misleading. Online content is "free" only in monetary terms; with respect to privacy, however, behavioral targeting exacts a hefty price. Behavioral targeting requires that ad networks collect and retain immense amounts of data about Internet users. Moreover, under current law, ad networks essentially enjoy unmitigated leeway to use the information they collect for whatever other purposes they wish. In addition to using Internet users' information for targeted ads, ad networks trade and sell information to third parties,[7] which could include the government. Thus, unbeknownst to the millions of people who regularly surf the Internet, their personal information

---

[3] *See* TRUEFFECT, ONLINE BEHAVIORAL ADVERTISING: POSSIBLE SELF-REGULATORY PRINCIPLES 2 (2008), *available at* http://www.ftc.gov/os/comments/behavioraladprinciples/080411trueffect.pdf (describing the Internet as one big "ad delivery mechanism").

[4] Howard Beales, *The Value of Behavioral Advertising*, NETWORK ADVERTISING INITIATIVE 3, http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf (last visited Mar. 27, 2012).

[5] Press Release, Network Adver. Initiative, Study Finds Behaviorally-Targeted Ads More than Twice as Valuable, Twice as Effective as Non-Targeted Online Ads (Mar. 24, 2010) (quoting Howard Beales, former Director, FTC Bureau of Consumer Protection), *available at* http://www.networkadvertising.org/pdfs/NAI_Beales_Release.pdf.

[6] *Id.* (quoting Charles Curran, Executive Director, Network Advertising Initiative).

[7] *See* Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J., July 31, 2010, at W1.

has been put on sale for the government to buy up and then use to monitor their online activity.

Perhaps surprisingly, the Fourth Amendment—the bulwark of constitutional privacy—likely offers little to no protection because of what is known as the "third-party doctrine." Under the third-party doctrine, the Fourth Amendment does not protect a person's privacy in information she has volunteered to a third party.[8] Likely falling within this definition is information collected by advertising networks for behavioral targeting.

This Comment explores the privacy implications of the Fourth Amendment third-party doctrine within the context of behavioral targeting. Part I provides a brief explanation of how behavioral targeting works and why it plays such an important role on the Internet. Part II offers an overview of the Supreme Court's Fourth Amendment jurisprudence pertaining to government searches, including the development of the third-party doctrine, and explores the primary criticisms of the doctrine. It then goes on to explain how the third-party doctrine might apply to ad-network databases, noting that a paradoxical problem would arise if ad networks were forced to obtain Internet users' consent to conduct behavioral targeting: while Internet users would gain some degree of privacy if they were given notice and an opportunity to opt out of tracking, those users who chose to remain opted in to access free online content would relinquish their privacy to the government because the third-party doctrine, at least under its current formulation, would inevitably apply. Part III presents a critical analysis of the Court's third-party doctrine, arguing that the problem stems both from a common misconception of Fourth Amendment privacy (as strictly "informational") and from a limited perception of the justification for the third-party doctrine. The Comment then offers a new analytical framework for the third-party doctrine, called the "competing-interests test," that incorporates these two considerations. Under this newly conceptualized third-party doctrine, Internet users would retain Fourth Amendment protections even if they consented to behavioral targeting.

[8] United States v. Miller, 425 U.S. 435, 442–43 (1976).

## I. BEHAVIORAL TARGETING AND THE INTERNET

### *A. How Behavioral Targeting Works*

Online behavioral targeting involves four key players: (1) the Internet user; (2) the content provider, the website that provides online content and displays an advertisement to the Internet user; (3) the advertiser, the company seeking to advertise its product;[9] and, finally, (4) the ad network, the company that acts as a middleman to the advertisers and content providers. The ad network is responsible for tracking and profiling the Internet user, and then placing the advertiser's ad on the content provider's website when the website is visited by an interested user.[10]

The ad network gauges an Internet user's interest in any given product by collecting and analyzing data about the user from three different sources. First, the ad network collects information from individual content providers about an Internet user's particular activity on any given website.[11] Second, the ad network gathers information provided by multiple content providers, called "clickstream" data, which reflects an Internet user's activity across the Web.[12] Finally, the ad network supplements the information it gathers with data about any given individual it obtains from third-party commercial databases.[13]

First, an ad network can gather information from a content provider that reveals a user's specific activity on the content provider's website.[14] Technically speaking, this occurs in one of two ways. When a website connects to a user's computer, it can attach the user's information to a command.[15] The user's browser then sends the command to an ad network requesting an appropriate advertisement based on the attached information.[16] Alternatively, the content provider might simply send the information to the ad

---

[9] Targeted ads are also used to promote political candidates. *See* David Herbert, *Candidates Walk Thin Line with Targeted Web Ads*, NAT'L J. (Jan. 10, 2011, 1:05 PM), http://www.nationaljournal.com/njonline/candidates-walk-thin-line-with-targeted-web-ads-20081001?mrefid=site_search (discussing how the Obama and McCain 2008 presidential campaigns exploited behavioral targeting).

[10] *See Behavioral Advertising Across Multiple Sites*, CENTER FOR DEMOCRACY & TECH. (Oct. 27, 2009), http://www.cdt.org/content/behavioral-advertising-across-multiple-sites [hereinafter *Behavioral Advertising*].

[11] *Testimony of Edward W. Felten*, COMMITTEE ON ENERGY & COM. DEMOCRATS 2–3 (June 18, 2009), http://democrats.energycommerce.house.gov/Press_111/20090618/testimony_felten.pdf.

[12] *See id.* at 3–4.

[13] *Id.* at 4.

[14] *Id.* at 2.

[15] *Id.* at 3.

[16] *Id.*

network directly.[17] The information sent to the ad network can represent the Internet user's activity on the website at any given moment or over a period of time, and can include any personally identifiable information the user discloses to the website when, for instance, she signs up for a service or completes a survey.[18]

Depending on the user's activity and the nature of the website, an ad network may be able to paint a fairly detailed portrait of a user based on this information alone. For example, if an Internet user is browsing through an online women's magazine, the ad network might learn that she is female, somewhere between ages twenty and thirty-five, and interested in fashion. But the information could be much more specific. For example, if the user accesses articles about depression and dieting, the ad network might note that she is depressed and wants to lose weight. If the Internet user signs up for the magazine's online sweepstakes, the ad network might then know her real name, phone number, and e-mail and home addresses. Thus, if the user is reading an article about weight loss on the website, the ad network might display any number of targeted ads based on her activity on that website alone: an ad for workout clothes based on a page she is currently viewing, an ad for a depression medication based on her past activity on the website,[19] or an ad for a nearby business based on location information she provided.[20]

Second, an ad network can gather data about an Internet user by tracking her online activity across multiple websites.[21] This information is known as clickstream data.[22] To collect clickstream data, the ad network sends a "cookie"[23] to the user's browser when she visits a website, which the user's

---

[17] *Id.*

[18] *See id.* at 2–3.

[19] Or, if the ad network is particularly cruel, it might display an ad for cheesecake, believing that dieters are more susceptible to focusing on their cravings. Stephen Henderson is concerned that an evil ad network might send depressed users advertisements for books about how to commit suicide. Stephen E. Henderson, Response, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39, 47 (2011), http://www.uiowa.edu/~ilr/bulletin/ILRB_96_Henderson.pdf. Assuming such books exist, Henderson's fear seems questionable at best.

[20] An ad network could determine the user's geographic location from her Internet Protocol (IP) address as well.

[21] *See Behavioral Advertising*, *supra* note 10; *Testimony of Edward W. Felten*, *supra* note 11, at 3.

[22] For an excellent explanation of the evolution of cookie technology in online advertising, see Andrew Hotaling, Comment, *Protecting Personally Identifiable Information on the Internet: Notice and Consent in the Age of Behavioral Targeting*, 16 COMMLAW CONSPECTUS 529 (2008).

[23] The Network Advertising Initiative defines cookies as "information (a small text file) that a site saves to your computer using your web browser" that "may allow sites to record [a user's] browsing activities" and that "may be placed in [a user's] browser by a third-party advertising network or company that helps deliver

computer then stores on its hard drive.[24] The cookie contains a unique number that allows the ad network to identify the user when she connects to another website within its network.[25] Thus, by recognizing the user's cookie, the ad network can track the user across the Internet, gathering information about her "web page visits, searches, online purchases, videos watched, [and] posts on social network[s]," among other things.[26]

An ad network's cookie categorizes the user's online activity into distinct "segments" that supposedly reflect her interests and that are used to determine which ads to display.[27] For example, according to an investigation on online tracking conducted by the Wall Street Journal, one of the largest ad networks, a company called RapLeaf, used segments such as "household income range, age range, political leaning, and gender and age of children in the household, as well as interests in topics including religion, the Bible, gambling, tobacco, adult entertainment and 'get rich quick' offers."[28] In total, RapLeaf's cookies segmented Internet users into over four hundred categories.[29] Armed with the user's browsing history represented in segments, the ad network can then display advertisements that reflect the user's interests when she is viewing a website that is entirely unrelated to that interest. For example, if, after reading the article about depression on the online women's magazine, the Internet user then visits another website to check the weather forecast, the ad network might at that point display an ad for an antidepressant.

An ad network can then take the information it gathers through both individual content providers and tracking cookies and compile everything it knows about a particular user into a personal "profile."[30] These profiles are often quite comprehensive—so much so that they can personally identify individual Internet users.[31] This can occur even if the ad network technically

---

the ads [a user] sees online." *Managing Your Privacy: FAQs*, NETWORK ADVERTISING INITIATIVE, http://www.networkadvertising.org/managing/faqs.asp (last visited Mar. 27, 2012).

[24] *Testimony of Edward W. Felten*, *supra* note 11, at 4.

[25] *Id.*

[26] Michael W. Macleod-Ball & Christopher Calabrese, *Written Statement of the American Civil Liberties Union*, AM. CIV. LIBERTIES UNION 3 (Nov. 19, 2009), http://www.aclu.org/files/assets/Statement_for_11-19-09_hearing_before_Subcommittees_on_Commun_Tech_and_the_Internet__Commerce_Trade_Consumer_Protection.pdf.

[27] *See Cracking the Code*, WALL ST. J. (Oct. 25, 2010), http://s.wsj.net/public/resources/documents/st_RAPLEAF_20101018.html.

[28] Emily Steel, *A Web Pioneer Profiles Users by Name*, WALL ST. J., Oct. 25, 2010, at A1.

[29] *Id.*

[30] *Testimony of Edward W. Felten*, *supra* note 11, at 4.

[31] *See id.*

does not collect any "personally identifiable information"—information such as a "name, address, telephone number, email address, financial account number, [and] government-issued identifier" that can be used "to identify, contact or precisely locate a person."[32] Notably, ad networks are not bound (legally or otherwise) to refrain from collecting personally identifiable information, and as a result, ad networks that do so face few consequences in the unlikely event they are detected.[33]

Finally, an ad network can supplement its user profiles with information purchased from commercial third-party databases.[34] For example, "supermassive databases"—like those made available by companies such as LexisNexis—offer *billions* of records about individuals aggregated from public and private records.[35] Thus, a user's profile could reflect vast quantities of highly sensitive personal information, including the user's "demographics, family information, and credit history."[36]

Given the invasiveness of online tracking, wary Internet users may hope to avoid behavioral targeting entirely. These users face no easy task. In fact, ad networks have developed technological capabilities to actually *prevent* users from effectively removing tracking cookies.[37] For example, a mechanism called a "Flash cookie" effectively bars a user from deleting tracking cookies

---

[32] *Managing Your Privacy: FAQs*, *supra* note 23. The Wall Street Journal's investigation of behavioral targeting revealed that one ad network used enough specific segments in its cookies that it came "extremely close" to "de-anonymizing" the user—at least "[close] enough to narrow him down to one of just 64 or so people *world-wide*." Emily Steel & Julia Angwin, *On the Web's Cutting Edge, Anonymity in Name Only*, WALL ST. J., Aug. 4, 2010, at A1 (emphasis added) (quoting Peter Eckersley, Technology Projects Director, Electronic Frontier Foundation) (internal quotation marks omitted); *accord* Susan E. Gindin, *Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears*, 8 NW. J. TECH. & INTELL. PROP. 1, 8 n.31 (2009) ("[R]esearch has shown that there is really no such thing as non-personally identifiable information because nearly all so-called anonymized data can be linked to a particular person.").

[33] *See* Hotaling, *supra* note 22, at 541 ("Amounting to little more than a non-binding policy statement, the [self-regulatory] principles have no legal effect on the use of [behavioral targeting] technology by the online advertising industry."). *See generally infra* Part II.A (discussing the ad-network industry's self-regulatory principles and the lack of effective legal regulation regarding the collection of personal information).

[34] *Testimony of Edward W. Felten*, *supra* note 11, at 4.

[35] Joseph T. Thai, *Is Data Mining Ever a Search Under Justice Stevens's Fourth Amendment?*, 74 FORDHAM L. REV. 1731, 1738 (2006).

[36] *Testimony of Edward W. Felten*, *supra* note 11, at 4.

[37] And as Edward Felten points out, "There are no *technical* barriers to the ad [network] selling this information to third parties." *Id.*

by instantly and automatically regenerating deleted cookies.[38] Flash cookies are often embedded in online videos[39] and are configured such that a user's browser saves them in a different location than it does tracking cookies.[40] Thus, when the user deletes her tracking cookies, the Flash cookies remain on her computer and can restore whatever tracking cookies she tried to remove.[41] But even if a user successfully deletes all of her cookies—Flash and tracking—it simply means that the ad network will install a new tracking cookie on her browser.

When deleting cookies proves futile, an Internet user might then turn to other security measures, which include opting out of individual ad networks or installing privacy "plug-ins."[42] First, a user can opt out of an ad network to limit or block targeted advertisements.[43] Perhaps ironically, this process requires the Internet user to install the ad network's unique opt-out cookie on her browser.[44] But opting out of the various ad networks is not necessarily easy or effective. For example, while two industry groups offer centralized locations where a user can opt out of some ad networks,[45] if an ad network does not belong to one of those groups, a user must opt out of each individual ad network separately. If, after opting out, a user erases the cookies on her browser, she then must opt out from each ad network all over again.[46] This means that the unwary user who purposely erases her cookies as a privacy precaution will become vulnerable to tracking cookies, as will the user who inadvertently erases her cookies by selecting the "anonymous browsing" setting on her Web browser, for example.[47] But opting out has a more basic flaw, which is that it offers no guarantee that the ad network will stop tracking

---

[38] Ashkan Soltani et al., Flash Cookies and Privacy 3 (Aug. 10, 2009) (unpublished manuscript) (explaining Flash-cookie technology and noting that Flash cookies selectively respawned ad-network tracking cookies, but not opt-out cookies), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862; *see also* Tanzina Vega, *Code that Tracks Users' Browsing Prompts Lawsuits*, N.Y. TIMES, Sept. 21, 2010, at B3 (reporting at least five class action lawsuits regarding companies' use of Flash cookies).

[39] Fifty-four of the top one hundred websites use Flash cookies. Soltani et al., *supra* note 38, at 3.

[40] *Id.* at 4.

[41] Vega, *supra* note 38.

[42] Jennifer Valentino-DeVries, *How to Avoid the Prying Eyes*, WALL ST. J., July 31, 2010, at W3.

[43] *Testimony of Edward W. Felten*, *supra* note 11, at 6.

[44] *See id.*

[45] *See Frequently Asked Questions*, PRIVACYCHOICE, http://www.privacychoice.org/faq (last visited Mar. 27, 2012); *Opt Out of Behavioral Advertising*, NETWORK ADVERTISING INITIATIVE, http://www.networkadvertising.org/managing/opt_out.asp (last visited Mar. 27, 2012).

[46] Valentino-DeVries, *supra* note 42.

[47] *Testimony of Edward W. Felten*, *supra* note 11, at 6.

the user.[48] Instead, opting out of an ad network only has the effect of blocking targeted ads,[49] thereby imparting only a false—if not misleading—sense of privacy. The Internet user who is seriously concerned about her privacy might be better off installing privacy plug-ins. These tools can be used to regularly delete cookies or to monitor invisible ad networks that track users without serving targeted ads.[50] But plug-ins are hardly an ideal or complete solution: certain plug-ins might only work with certain browsers, and for unsophisticated Internet users, these tools may be difficult to set up.

Ultimately, regardless of whether people realize it—and despite some people's efforts to avoid it—behavioral targeting has become an integral part of the Internet, if not of everyday life. While the Internet has made large-scale behavioral targeting technologically feasible, behavioral targeting has, in turn, made the Internet sustainable as a limitless source of free content.

### *B. Behavioral Targeting and Free Public Access to Online Content*

Online content providers depend heavily on selling ad space on their websites to provide free online content. This dependence is made possible, in part, by behavioral targeting.[51] Because targeted ads are so effective compared to other forms of online advertisements, content providers take in relatively

---

[48] JOSEPH TUROW ET AL., AMERICANS REJECT TAILORED ADVERTISING AND THREE ACTIVITIES THAT ENABLE IT 8 (2009), *available at* http://repository.upenn.edu/cgi/viewcontent.cgi?article=1138&context=asc_papers.

[49] *Testimony of Edward W. Felten*, *supra* note 11, at 6. The user is still subjected to invisible tracking through use of a "[W]eb beacon." *Id.* at 4. Web beacons are pervasive even when Internet users do not opt out of behavioral targeting. For example, one study revealed that Google's ad services used Web beacons on eighty-eight percent of the sampled websites and on ninety-two of the top one hundred most popular sites. Aleecia M. McDonald & Lorrie Faith Cranor, Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising 2 (Aug. 16, 2010) (unpublished manuscript), *available at* http://www.tprcweb.com/index.php?option=com_jdownloads&Itemid=0&view=finish&cid=123&catid=48.

[50] Valentino-DeVries, *supra* note 42.

[51] Content providers' dependence upon ad revenue stems from a number of factors, including the removal of meaningful barriers to making perfect copies of digital content on the Internet, rampant copyright infringement, and the resulting inability of content providers to profit from direct sales. *See* Ben Depoorter et al., *Copyright Backlash*, 84 S. CAL. L. REV. 1251, 1253 (2011) ("Digital downloading and file sharing present unprecedented challenges to the enforcement of copyright law. These new technologies greatly facilitate unauthorized reproduction and distribution of copyrighted material." (footnote omitted)). While the death of copyright on the Internet is beyond the scope of this Comment, for an enlightening discussion of recent technological advances, including the Web, that have created complications in the application of copyright protections, see Glynn S. Lunney, Jr., *The Death of Copyright: Digital Technology, Private Copying, and the Digital Millennium Copyright Act*, 87 VA. L. REV. 813 (2001).

greater profits from selling online ad space.[52] With increased profits, websites can provide online content without needing to charge the Internet user a fee.[53] As free online content has become the norm, behavioral targeting has become a practical necessity for sustaining the Internet. In the words of the Network Advertising Initiative, a cooperative of advertising networks, "[T]he increased revenues associated with [targeted ads] are *vital* to supporting the continued growth in ad-supported Web content."[54]

When viewed in isolation, behavioral targeting is purely beneficial, allowing for the continued growth of the Internet and the increasing availability of free online content.[55] And consider the alternative: If people were required to pay even a small amount of money to access a website, it is unlikely that the average Internet user would visit 2646 different websites each month as they do currently.[56] But the benefits of behavioral targeting are far less compelling when viewed from a privacy perspective given the ease with which online tracking invokes images of Orwell's Big Brother[57] or Jeremy Bentham's Panopticon.[58] The current question, then, is whether the benefits of behavioral targeting outweigh the potential privacy harms that result from the near-constant tracking of Internet users.

---

[52] *See* Beales, *supra* note 4, at 3 (noting that behavioral targeting is about twice as profitable as standard online advertising techniques). One study found that revenue from behavioral targeting could be matched only by "highly obtrusive ads." Avi Goldfarb & Catherine Tucker, *Online Display Advertising: Targeting and Obtrusiveness*, 30 MARKETING SCI. 389, 400 (2011).

[53] Beales, *supra* note 4, at 1.

[54] Memorandum from the Network Adver. Initiative to the Internet Policy Task Force 5–6 (June 14, 2010) (emphasis added), *available at* http://naiblog.org/wp-content/uploads/2010/06/Commerce-Comments1.pdf; *accord* Thomas M. Lenard & Paul H. Rubin, *In Defense of Data: Information and the Costs of Privacy*, 2 POL'Y & INTERNET 149, 157, 160 (2010) (explaining how privacy advocates often ignore the trade-off between privacy and free information).

[55] These benefits may seem even more attractive during difficult economic times, when consumers are less likely to pay for online content. *Testimony of Anne Toth, Vice President of Policy and Head of Privacy, Yahoo! Inc.*, COMMITTEE ON ENERGY & COM. DEMOCRATS 3 (June 18, 2009), http://democrats.energycommerce.house.gov/Press_111/20090618/testimony_toth.pdf.

[56] Catharine Smith, *Internet Usage Statistics: How We Spend Our Time Online*, HUFFINGTON POST (May 25, 2011), http://www.huffingtonpost.com/2010/06/22/internet-usage-statistics_n_620946.html.

[57] GEORGE ORWELL, 1984 (1949).

[58] Bentham's Panopticon is a prison in which none of the prisoners can see whether anyone is watching them, but each knows that anyone could be watching at any time. Bentham described the Panopticon as a new mode of obtaining "power of mind over mind," "in [a] hitherto unexampled quantity." MICHEL FOUCAULT, DISCIPLINE & PUNISH: THE BIRTH OF THE PRISON 201, 202, 206 (Alan Sheridan trans., Vintage Books 2d ed. 1995) (1975) (quoting 4 JEREMY BENTHAM, *Panopticon*, *in* THE WORKS OF JEREMY BENTHAM 37, 39 (John Bowring ed., Edinburgh, William Tait 1843) (1787)) (internal quotation marks omitted).

## II. PRIVACY

> *The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. . . . They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.*
>
> *—Olmstead v. United States*[59]

### *A. Introduction: Overview of Current Privacy Protections*

The law offers little meaningful protection for Internet users seeking to shield their online activity from the prying eyes of both private third parties and the government. As a result, behavioral targeting poses a very real threat to Internet users' privacy.[60]

Internet users seeking to protect their information from private third parties might turn to a variety of legal remedies: online privacy policies under a contract theory, common law privacy torts, federal privacy laws, or the ad-network industry's self-imposed standards.[61] These protections are fairly limited. For example, with only a few exceptions,[62] websites are not legally required to adopt privacy policies. Privacy policies that websites do adopt are often impossibly confusing and unreasonably lengthy for the average Internet user, serving little purpose but to shield the website from liability.[63] Therefore,

---

[59] 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

[60] *See Testimony to the House Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection, and the Subcommittee on Communications, Technology, and the Internet*, COMMITTEE ON ENERGY & COM. DEMOCRATS 2–5 (June 18, 2009), http://democrats.energycommerce.house.gov/Press_111/20090618/testimony_chester.pdf.

[61] *See* Luke J. Albrecht, Note, *Online Marketing: The Use of Cookies and Remedies for Internet Users*, 36 SUFFOLK U. L. REV. 421, 424–37 (2003).

[62] *See* Children's Online Privacy Protection Act of 1998 § 1303, 15 U.S.C. § 6502(b)(1)(A) (2006) (requiring a privacy policy for websites that collect information about children under age thirteen); Gramm–Leach–Bliley Act § 502, *id.* § 6802(b)(1)(A) (requiring clear and conspicuous statements of information-gathering practices by an institution that is significantly engaged in financial activity if that institution discloses nonpublic personal information to third parties).

[63] *See* JOSHUA GOMEZ ET AL., KNOWPRIVACY 11 (2009), *available at* http://knowprivacy.org/report/KnowPrivacy_Final_Report.pdf (reporting that privacy policies are ineffective because they are difficult and time-consuming to read, and lead consumers to believe they are protected); Jon Leibowitz, Comm'r, Fed.

an Internet user seeking to enforce a website's privacy policy against the website under a contract theory is likely doomed from the outset.[64] Similarly, common law privacy torts—including intrusion into seclusion, misappropriation of likeness, and public disclosure of private facts[65]—offer weak remedies in the context of behavioral targeting because they require a plaintiff to show some discrete harm committed by a distinct tortfeasor.[66] This is often a difficult task given the indirect and invisible nature of ad-network activity.[67]

In addition, federal statutory privacy laws are complex and ill-equipped for protecting Internet users from behavioral targeting.[68] For example, while the Electronic Communications Privacy Act of 1986 (ECPA) offers Internet users some protection from private parties intentionally accessing or intercepting stored electronic communications,[69] courts have held that the ECPA does not apply to clickstream data.[70] Similarly, the Computer Fraud and Abuse Act, which protects against third parties obtaining unauthorized information by accessing a computer,[71] fails to provide any meaningful remedy because the statute's minimum-damages requirement is difficult to meet in the case of behavioral targeting.[72]

---

Trade Comm'n, So Private, So Public: Individuals, the Internet & the Paradox of Behavioral Marketing, Remarks at the FTC Town Hall Meeting on Ehavioral Advertising: Tracking, Targeting, & Technology 4 (Nov. 1, 2007), *available at* http://www.ftc.gov/speeches/leibowitz/071031ehavior.pdf ("In many cases, consumers don't notice, read, or understand . . . privacy policies. They are often posted inconspicuously . . . and filled with fine-print legalese and technotalk. A recent study . . . found that they were essentially incomprehensible for the majority of Internet users.").

64 *See, e.g.*, *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 510 (S.D.N.Y. 2001) (inferring that plaintiffs, a class of Internet users, gave implied consent for content providers to share personally identifiable information with their contractual affiliates). *But see In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 20–21 (1st Cir. 2003) (declining to follow *DoubleClick*, explaining that "consent 'should not casually be inferred'" (quoting Griggs-Ryan v. Smith, 904 F.2d 112, 117 (1st Cir. 1990)).

65 RESTATEMENT (SECOND) OF TORTS § 652A(2)(a)–(c) (1977).

66 Hotaling, *supra* note 22, at 550.

67 *See id.*; *see also* Albrecht, *supra* note 61, at 433–36.

68 Gindin, *supra* note 32, at 34.

69 Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.). The two relevant sections of the ECPA are the Stored Communications Act, 18 U.S.C. §§ 2701–2711 (2006), and the Wiretap Act, *id.* §§ 2510–2522. *See generally* Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375 (2004) (explaining the ECPA).

70 *See, e.g.*, *In re* Toys R Us, Inc., Privacy Litig., No. C 00-2746 MMC, 2001 U.S. Dist. LEXIS 16947, at *4, 14 (N.D. Cal. Oct. 9, 2001) (noting that cookies placed on a hard drive are not in "electronic storage" for the purpose of the Stored Communications Act); Chance v. Ave. A, Inc., 165 F. Supp. 2d 1153, 1163 (W.D. Wash. 2001); *In re DoubleClick*, 154 F. Supp. 2d at 526.

71 18 U.S.C. § 1030.

72 *See, e.g.*, *Chance*, 165 F. Supp. 2d at 1158–60; *In re DoubleClick*, 154 F. Supp. 2d at 519–26.

Finally, consumer-protection regulations offer little in the way of protection against private third parties. For example, the Federal Trade Commission (FTC) has taken a hands-off approach to regulating behavioral targeting, only periodically pressuring the ad-network industry to self-regulate.[73] The ad-network industry, in an unapologetic attempt to "[f]end off . . . legislation and regulation,"[74] has developed a set of guiding principles that focuses on transparency, consumer control, data security, and accountability, among other things.[75] Regardless of the industry's efforts, however, because ad networks are not legally bound by their own rules, they are not forced to abide by them.[76] For example, according to a 2010 *Wall Street Journal* investigation, RapLeaf, a major ad network, was discovered to have been transmitting personally identifiable information linked to sensitive data to other companies in violation of the industry principles.[77]

Recently, the FTC has renewed its efforts to crack down on what many perceive to be an out-of-control industry. The FTC's proposed guidelines would allow Internet users to opt out of online tracking once and for all through the creation of a national "Do Not Track" list, similar to the National Do Not Call Registry for telemarketing.[78] Though the proposals are by no means perfect, they represent an important improvement.

Internet users seeking to restrict government access to information gathered by private third parties face similarly steep legal obstacles. For example, one of

---

[73] The FTC first expressed concern about targeted ads in 1999 and, in 2007, issued guidelines containing general principles for behavioral targeting, *see* FTC, ONLINE BEHAVIORAL ADVERTISING: MOVING THE DISCUSSION FORWARD TO POSSIBLE SELF-REGULATORY PRINCIPLES (2007), *available at* http://www.ftc.gov/os/2007/12/P859900stmt.pdf, which it revised in 2009, *see* FTC, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

[74] *About the IAB*, INTERACTIVE ADVERTISING BUREAU, http://www.iab.net/about_the_iab (last visited Mar. 27, 2012).

[75] AM. ASS'N OF ADVER. AGENCIES ET AL., SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 2–4 (2009), *available at* http://www.iab.net/media/file/ven-principles-07-01-09.pdf. These principles are based more or less on the FTC's suggestions and include education, transparency, consumer control, data security, material changes to existing online, behavioral-advertising policies and practices, sensitive data, and accountability. *Id.* at 1.

[76] *See* Gindin, *supra* note 32, at 34 ("A potential problem with self regulation is that unless there are formal sanctions available for violations of established guidelines, some companies may be inclined to ignore industry guidelines or to minimize their significance.").

[77] *See* Steel, *supra* note 28.

[78] *See* FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS 63–69 (2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf; *Testimony of Daniel J. Weitzner*, COMMITTEE ON ENERGY & COM. DEMOCRATS 10 (Dec. 2, 2010), http://democrats.energycommerce.house.gov/documents/20101202/Weitzner.Testimony.12.02.2010.pdf.

the most sweeping federal privacy laws regulating the government's collection and use of personal information, the Privacy Act of 1974, does not prevent the government from accessing information gathered for behavioral targeting.[79] This is because the Act likely does not apply when the government accesses information from third-party databases without actually establishing its own database or without "retriev[ing]" the information through use of a "name or other personal identifier."[80] As a result, the Act would not apply in the case of behavioral targeting where the government accesses information collected in databases created and controlled by advertising networks. This conclusion is particularly troubling because federal statutory laws are likely the only tools for providing uniform privacy protection in the context of behavioral targeting.[81] Indeed, information gathered for behavioral targeting does not seem to fall within the protective scope of the Constitution.

The Fourth Amendment is implicated when the government violates "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[82] There is a clear case that the Fourth Amendment would protect people from direct online tracking performed by the government, as opposed to an ad network.[83] On the other hand, because ad networks are not state actors, ad networks cannot violate users' Fourth Amendment rights by collecting information about them through online tracking.

---

[79] 5 U.S.C. § 552a (2006).

[80] *See Privacy: The Use of Commercial Information Resellers by Federal Agencies: Hearing Before the Subcomm. on Info. Policy, Census & Nat'l Archives of the H. Comm. on Oversight & Gov't Reform*, 110th Cong. 97 (2008) (testimony of Paula J. Bruening, Deputy Executive Director, Center for Information Policy Leadership, Hunton & Williams LLP) [hereinafter *Bruening Testimony*] (quoting Bartel v. FAA, 725 F.2d 1403, 1408 n.10 (D.C. Cir. 1984)). *See generally* 5 U.S.C. § 552a (stating that the Privacy Act only applies to information maintained in a "system of records," meaning a "group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual"). Further, under the ECPA, the government can access or intercept routing information (e.g., websites visited by an Internet user) from an Internet Service Provider as long as the government certifies to a court that the information it seeks is "relevant to an ongoing criminal investigation" and is "likely to be obtained." 18 U.S.C. § 3123(a)(1).

[81] Though this Comment focuses on more broadly applicable privacy laws, it should be noted that some states offer protection in this area. *See, e.g.*, CAL. GOV'T CODE § 11015.5(a) (West 2012) (requiring that government agencies provide certain notices to individuals when collecting personal information electronically).

[82] U.S. CONST. amend. IV.

[83] *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1018 (2010) (proposing a framework for applying the Fourth Amendment to the Internet and arguing that the approach should apply to "content surveillance," or surveillance of "private thoughts and speech").

The relevant question, then, is whether the Fourth Amendment applies if the government, though not doing the tracking itself, accesses information gathered by ad networks. The answer to that question is probably in the negative. Under the Supreme Court's third-party doctrine, the Fourth Amendment does not protect information a person "volunteers" to a third party.[84] The third-party doctrine would apply in the case of behavioral targeting if, when a person goes online, she "volunteers" information about her online activity to an ad network. This means that the government could obtain all of the information compiled in an ad network's profile database and use it for whatever purpose it likes—for example, in a criminal investigation—even though the database is comprised of information that the government could not lawfully collect itself.[85] In other words, the government could circumvent the Fourth Amendment with the cooperation of an ad network and legally conduct searches of every Internet user's online activity, amounting to millions of general fishing expeditions.

In fact, the government has been accessing and mining databases—its own and those offered up by third parties—for years.[86] In the wake of the 9/11 terrorist attacks, the government began accumulating and analyzing "vast amounts of data about the everyday transactions of American citizens" through its Total Information Awareness (TIA) program.[87] In 2002 Congress passed the Homeland Security Act, which authorized the Department of Homeland Security to use data mining in its investigations.[88] A related government

---

84 *See* United States v. Miller, 425 U.S. 435, 442–43 (1976).

85 *Bruening Testimony*, *supra* note 80, at 97.

86 *See* Joshua L. Simmons, Note, *Buying You: The Government's Use of Fourth-Parties to Launder Data About 'The People,'* 2009 COLUM. BUS. L. REV. 950.

87 Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 317 (2008). Although Congress defunded TIA in 2003 in response to increasing privacy concerns, *see* Consolidated Appropriations Resolution, 2003, Pub. L. No. 108-7, § 111(a), 117 Stat. 11, 534–36, many of TIA's programs have continued in other forms, *see Total/Terrorism Information Awareness (TIA): Is It Truly Dead?*, ELECTRONIC FRONTIER FOUND., http://w2.eff.org/Privacy/TIA/20031003_comments.php (last visited Mar. 27, 2012).

88 Homeland Security Act of 2002, Pub. L. No. 107-296, § 201(d)(14), 115 Stat. 2135, 2147 (codified at 6 U.S.C. § 121(d)(14) (2006)). Congress later passed the Federal Agency Data Mining Reporting Act of 2007, Pub. L. No. 110-53, tit. VIII, § 804, 121 Stat. 362 (codified at 42 U.S.C. § 2000ee-3 (Supp. I 2007)), to require some transparency in federal data-mining programs. The Act defines data mining as

> a program involving pattern-based queries, searches, or other analyses of 1 or more electronic databases, where a department or agency of the Federal Government, or a non-Federal entity acting on behalf of the Federal Government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals,

program called ADVISE (Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement) was created "to troll a vast sea of information . . . and extract suspicious people, places and other elements based on their links and behavioral patterns."[89] As of 2007, the federal government was operating an estimated two hundred data-mining programs.[90] And while oversight of government data-mining programs is fairly limited,[91] a 2008 Government Accountability Office report revealed that, in 2005, federal government agencies—including the Department of Justice and the Department of Homeland Security—reported plans "to spend a combined total of approximately $30 million to purchase personal information from resellers."[92] According to the report, "The vast majority—approximately 91 percent—of the planned spending was for purposes of law enforcement (69 percent) or counterterrorism (22 percent)."[93] Thus, it seems that commercial-database companies and the government are already allies in the pursuit of personal information.[94]

The remainder of this section offers an overview of the Supreme Court's Fourth Amendment third-party doctrine and important criticisms surrounding it. It then discusses in greater detail why the doctrine likely would apply in the case of behavioral targeting under the current legal landscape, as well as in the event that the FTC's proposed privacy protections succeed.

---

*id.* § 2000ee-3(b)(1)(A), where the search is not done by name or with another personal identifier, *id.* § 2000ee-3(b)(1)(B), and if the purpose of the search "is not solely the detection of fraud, waste, or abuse . . . or the security of a Government computer system," *id.* § 2000ee-3(b)(1)(C).

89 Slobogin, *supra* note 87, at 318 (quoting Ellen Nakashima & Alec Klein, *Profiling Program Raises Privacy Concerns*, WASH. POST, Feb. 28, 2007, at B1) (internal quotation marks omitted).

90 CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 192 (2007).

91 For example, the E-Government Act of 2002, Pub. L. No. 107-347, § 208(b)(1)(B), 116 Stat. 2899, 2922, which requires that federal agencies publish Privacy Impact Assessments (PIAs) on data collected through information technology, does not apply to searches of data collected by third parties. THE CONSTITUTION PROJECT, PRINCIPLES FOR GOVERNMENT DATA MINING: PRESERVING CIVIL LIBERTIES IN THE INFORMATION AGE 17 (2010). Further, though the Federal Agency Data Mining Reporting Act of 2007 requires federal agencies to compile annual reports on all data-mining activities, it allows agencies to keep confidential material private and adopts a very narrow definition of what constitutes "data mining." 42 U.S.C. § 2000ee-3(c).

92 LINDA D. KOONTZ, U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-08-543T, PRIVACY: GOVERNMENT USE OF DATA FROM INFORMATION RESELLERS COULD INCLUDE BETTER PROTECTIONS 3 (2008) (footnote omitted).

93 *Id.* at 3–4.

94 Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1101 (2002).

### *B. The Fourth Amendment and the Third-Party Doctrine*

> *You have no privacy. Get over it.*
>
> —Scott McNealy
> CEO, Sun Microsystems, Inc.[95]

The Supreme Court's modern formulation for determining when a search is "unreasonable" within the meaning of the Fourth Amendment comes from its landmark decision, *Katz v. United States*.[96] In *Katz*, the Court held that law enforcement had conducted an unreasonable search when it eavesdropped on the defendant's telephone-booth conversation using an electronic surveillance device.[97] According to Justice Stewart, "the Fourth Amendment protects people, not places,"[98] and a search is unreasonable if it "violate[s] the privacy upon which [a person] justifiably relie[s]."[99] The Court noted, however, that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[100]

Justice Harlan, in his concurring opinion, formulated his famous "reasonable expectation of privacy" test,[101] which has come to control when determining whether a government search violates the Fourth Amendment. A search is unreasonable when it violates a person's reasonable expectation of privacy, and a person's expectation of privacy is reasonable only if (1) that person herself "exhibit[s] an actual (subjective) expectation of privacy," and (2) "the expectation [is] one that society is prepared to recognize as 'reasonable.'"[102]

One might expect that, given Justice Harlan's test, the Fourth Amendment would preclude the government from accessing and analyzing information gathered by ad networks for behavioral targeting. After all, many people subjectively expect privacy from the government when they use the Internet, and their expectation would seem to be one that society would accept as

---

95 *On the Record: Scott McNealy*, S.F. CHRON., Sept. 14, 2003, at I1.

96 389 U.S. 347 (1967).

97 *Id.* at 349–50, 359.

98 *Id.* at 351.

99 *Id.* at 353. The defendant in *Katz* "justifiably relied" on his conversation remaining private because "[o]ne who occupies [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world." *Id.* at 352.

100 *Id.* at 351.

101 *Id.* at 361 (Harlan, J., concurring).

102 *Id.*

reasonable. Nevertheless, the Fourth Amendment likely does not protect information about Internet users' online activities because of the so-called third-party doctrine.

The third-party doctrine holds that, under the Fourth Amendment, an individual has no reasonable expectation of privacy in information that she volunteers to a third party. The Court's classic statement of the doctrine comes from *United States v. Miller*, a case in which law enforcement officials obtained the defendant's financial records from his bank without a warrant.[103] The Supreme Court held that the government's activity did not amount to an unreasonable search because the defendant had no reasonable expectation of privacy in records kept by a third party, his bank.[104] According to the Court:

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, 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.[105]

The Court justified its holding on the basis that the defendant had assumed the risk that the bank would share his information with the government, regardless of the defendant's actual expectations of confidentiality. According to the Court, "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[106]

The Court's assumption-of-risk rationale was actually drawn from another line of cases involving undercover agents and confidential informants.[107] Beginning in the 1952 case of *On Lee v. United States*, the Court held that the Fourth Amendment does not protect information revealed by one party to another in the course of a conversation.[108] The Court subsequently offered some justification for its position in *Hoffa v. United States*, explaining that the

---

[103] 425 U.S. 435, 438–39 (1976).

[104] *Id.* at 442. The Court further explained that it made no difference, for purposes of the Fourth Amendment, that the banks were required to maintain the defendant's financial records pursuant to the Bank Secrecy Act. *Id.* at 443. In addition, the Court rejected any Fourth Amendment challenges based on arguments that the banks were acting as agents of the government or that the defendant received no notice of the subpoenas. *Id.* at 443 & n.5.

[105] *Id.* at 443.

[106] *Id.*

[107] *Id.* (citing United States v. White, 401 U.S. 745, 751–52 (1971) (plurality opinion); Hoffa v. United States, 385 U.S. 293, 302 (1966); and Lopez v. United States, 373 U.S. 427 (1963)).

[108] 343 U.S. 747, 754 (1952). A decade later, but still pre-*Katz*, the Court reaffirmed *On Lee* in *Lopez v. United States*, 373 U.S. 427.

Fourth Amendment does not protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."[109] Post-*Katz*, the Court approved the line of cases in *United States v. White*, reframing its reasoning to comport with the reasonable-expectation-of-privacy test: a person has no reasonable expectation of privacy in information she has shared with another person because she has assumed the risk that her confidant might share that information with the government.[110] In essence, the Court extracted the assumption-of-risk justification from *White* and applied it in *Miller*, which differed to the extent that the third party was an entity, instead of another person.

After *Miller*, the Court developed its third-party doctrine in two more key cases. In *Smith v. Maryland*, the Court held that the defendant had no reasonable expectation of privacy in numbers he dialed from his home telephone.[111] The case involved a phone company, which, per the government's request, had installed a pen register[112] on the defendant's home telephone to track his outgoing calls.[113] The Court applied the third-party doctrine after reasoning that a person "volunteers" information as long as most people realize or should be aware of the possibility that third parties are capable of collecting that information.[114] According to the Court, "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."[115] In other words, as long as most people realize a third party is capable of collecting information, then any given individual assumes the risk that the third party will not only collect that information but also share it with the government.

Nearly a decade later, the Court reaffirmed its reasoning in *Smith* in its final third-party-doctrine case, *California v. Greenwood*.[116] In *Greenwood*, the Court applied the third-party doctrine when the defendant placed a bag of trash on the curb outside his home, finding that the defendant had "volunteered" its

---

109 385 U.S. at 302.

110 401 U.S. at 752 ("[O]ne contemplating illegal activities must realize and risk that his companions may be reporting to the police. If he sufficiently doubts their trustworthiness, the association will very probably end or never materialize. But if he has no doubts, or allays them, or risks what doubt he has, the risk is his.").

111 442 U.S. 735, 745–52 (1979).

112 A pen register is a device that tracks the numbers dialed from a phone. *Id.* at 736 n.1.

113 *Id.* at 737.

114 *Id.* at 743–45.

115 *Id.* at 742.

116 486 U.S. 35 (1988).

contents to a third party.[117] The Court explained that most people realize that almost anyone could access the contents of the trash, despite the low probability that anyone besides a trash collector would.[118]

### *C. Responses to the Third-Party Doctrine*

Since its inception, the third-party doctrine has elicited resistance from lawmakers.[119] For example, in response to *Miller*, Congress passed the Right to Financial Privacy Act of 1978 to provide protection for financial records,[120] and after *Smith*, Congress enacted the Pen Register Act to protect telephone call records.[121] Further, courts at both federal and state levels have been reluctant to apply the doctrine. The Third Circuit, for example, declined to apply the third-party doctrine in a case involving historical cell-site location information, on the basis that a cell phone user "has not 'voluntarily' shared his location information with a cellular provider in any meaningful way."[122] At least eleven state supreme courts have refused to use the doctrine to interpret their own constitutions, and ten states have shown signs that they might follow suit.[123]

Legal commentators generally disagree with the soundness of the doctrine,[124] criticizing the Court's understanding of what constitutes

---

[117] *Id.* at 39–41.

[118] *Id.* at 41.

[119] *See* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE § 2.7(b)–(c), at 736, 747 (4th ed. 2004) (calling the third-party doctrine "dead wrong," "a crabbed interpretation" that "makes a mockery of the Fourth Amendment").

[120] Pub. L. No. 95-630, tit. XI, 92 Stat. 3697 (codified as amended at 12 U.S.C. §§ 3401–3422 (2006)).

[121] Pub. L. No. 99-508, tit. III, 100 Stat. 1868 (1986) (codified as amended at 18 U.S.C. §§ 3121–3127).

[122] *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317 (3d Cir. 2010). *But see, e.g.*, Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) ("[C]omputer users do not have a legitimate expectation of privacy in their [Internet Service Provider] subscriber information because they have conveyed it to another person—the system operator."); United States v. Hambrick, No. 99-4793, 2000 U.S. App. LEXIS 18665, at *12 n.4 (per curiam) (4th Cir. Aug. 3, 2000) ("While the Court is aware of the 'revolutionary' nature of the Internet as well as the vast extent of communications it has initiated, the [Internet Service Provider subscription] information at issue in this case is not distinguishable from the materials in *Miller* and *Smith* . . . .").

[123] Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 395 tbl.1 (2006).

[124] As Professor Orin Kerr notes, "A list of every article or book that has criticized the doctrine would make [for] the world's longest law review footnote." Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 n.5 (2009).

"reasonable" expectations of privacy as out of touch with reality.[125] Many of their arguments trace back to the Court's assumption-of-risk justification, which, upon close scrutiny, seems inherently flawed. Assumption of risk is a theory based in contract, in which a person who assumes a risk receives some benefit or consideration in return, and in which—but for a particular benefit—she would not assume the risk.[126] But a person can only truly "assume" a risk if she is both informed of the risk—meaning she understands and appreciates its potential consequences and the possibility that they might occur—and has the ability to either accept or reject the risk.[127] If these two conditions are satisfied, then by assuming a risk, a person effectively consents to bear the risk's consequences should they come to pass. Assumption of risk, then, is synonymous with voluntary consent.

Assumption of risk, however, must be distinguished from the concept of "notice." When a person has notice of a risk, she has satisfied only one of the two conditions required for assumption of risk: while she has *knowledge* of a risk, she does not necessarily accept it or consent to it.[128] For example, drawing from an analogy offered by Professor Epstein, a pedestrian who decides to go for a walk knows, at a certain level, that she could be run over by a car, but she has not agreed to be run over.[129] Under tort law, the pedestrian does not assume the risk that she will be run over by simply going for a walk, even though the pedestrian has some notice of the risk.[130]

The notice principle has no place in the Fourth Amendment and especially in the third-party doctrine. As Professor Epstein observes, the Court's "false equation of knowledge of a risk with the assumption of the risk" leads to a "potential source of abuse" by the government[131]: if the government notifies everyone that it can search every house, then everyone has "assumed the risk"

---

125 *See id.* at 571 ("Such expectations of privacy are common and reasonable, and Justices who cannot see that are simply out of touch with society and are misapplying the Fourth Amendment.").

126 Professor Richard Epstein charts the doctrinal origins of the assumption-of-risk theory under the third-party doctrine. *See* Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 BERKELEY TECH. L.J. 1199 (2009).

127 *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting) ("Implicit in the concept of assumption of risk is some notion of choice."); Epstein, *supra* note 126, at 1204.

128 *See* Epstein, *supra* note 126, at 1204. Under common law, this concept is known as *sciens non est volens* ("knowing is not volunteering").

129 *Id.*

130 *Id.*

131 *Id.*

that their houses will be searched merely because they *know* their houses will be searched.[132] The result is absurd.

Nevertheless, the notice principle is central to the third-party doctrine. In its strictest form, the Court equates notice of risk with assumption of risk in two instances. First, under the third-party doctrine, a person is said to have "volunteered" information to a third party as long as society in general is aware that a third party is capable of collecting information.[133] Thus, if the Court decides that *people in general* have notice of a risk, the Court treats *any given individual* as having consented to the risk as though the individual had both actual knowledge of the risk and an opportunity to reject it.

Second, even in situations where a person has truly consented to sharing information with a third party, the Court treats this limited consent as consent to allow the third party to share that information with the government—or, stated another way, as consent to a *government search*.[134] Again, the Court's reasoning depends on equating society's general awareness of the risk—the possibility that a third party might share information with the government—with an individual's actual knowledge and acceptance of the risk. And while there are circumstances in which a person can simply choose not to share information with a third party, in many situations, that option is unrealistic or effectively unavailable. Indeed, participating in everyday life more or less requires sharing information with many third parties. Thus, the inherent flaw in the third-party doctrine is that the assumption-of-risk rationale "leaves nothing to the underlying substantive right at all."[135]

### *D. New Technology and the Hopeful Demise of the Third-Party Doctrine*

Despite the lack of enthusiasm toward the third-party doctrine shared by Congress, lower federal courts, state courts, and commentators, the Supreme

---

[132] *See id.* at 1205.

[133] *See* California v. Greenwood, 486 U.S. 35, 39–41 (1988). Moreover, as Justice Marshall noted in his dissenting opinion in *Smith v. Maryland*, the Court seems too comfortable imputing to society a general awareness of third parties' capabilities to access information, as, for example, in the situation of the telephone company's use of a pen register to track phone numbers. *See* 442 U.S. 735, 749 n.1 (1979) (Marshall, J., dissenting) ("Lacking the Court's apparently exhaustive knowledge of this Nation's telephone books and the reading habits of telephone subscribers, I decline to assume general public awareness of how obscene phone calls are traced." (citation omitted)).

[134] *See* Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 122 (2002) (noting that the third-party doctrine is flawed in that "it treats exposure to a limited audience as morally equivalent to exposure to the whole world").

[135] Epstein, *supra* note 126, at 1205.

Court has never seriously questioned the doctrine. But two of the Court's more recent cases offer hope that the third-party doctrine may not survive in its harshest form, especially when applied in the context of new technology.

First, in the 2001 case *Ferguson v. City of Charleston*, the Court indicated that it might be shifting away from the notice-based meaning of "volunteer" under the third-party doctrine.[136] *Ferguson* was a case in which the third-party doctrine arguably should have applied but which, curiously, was decided under the "special needs doctrine"—an exception to the warrant requirement, applicable when the government conducts a suspicionless search that is motivated by non-law-enforcement purposes.[137] At issue was the validity of a policy initiated by a hospital and implemented by local law enforcement, requiring pregnant women to submit to drug tests in the course of prenatal treatment if they met specified criteria indicating cocaine use.[138] If a woman's urine tested positive for cocaine, the results "would be turned over to the police and . . . could be admissible in subsequent criminal prosecutions."[139] Justice Stevens, writing for the majority, held that the maternity patient had a reasonable expectation of privacy that "the results of [her urine] tests [would] not be shared with nonmedical personnel without her consent."[140]

Only Justice Scalia, in his dissent, argued that the case fell squarely within the third-party doctrine.[141] As he correctly pointed out, the Court had "*never* held—or even suggested—that material which a person voluntarily entrusts to someone else cannot be given by that person to the police, and used for whatever evidence it may contain."[142] The majority responded to Justice Scalia's argument by stating that, because its decision proceeded on the assumption that "the patients [had] *not* consent[ed] to the searches," the patients had not "voluntarily entrust[ed]" any information to a third party.[143] Thus, Justice Stevens suggested that some form of actual consent, as opposed to mere notice, was required to trigger the third-party doctrine.

---

136 532 U.S. 67 (2001).

137 *Id.* at 78–81. Under the special needs doctrine, the Court applies a balancing test to determine whether a suspicionless search is nevertheless reasonable under the Fourth Amendment. *Id.* at 78. The government's non-law-enforcement interest must outweigh the person's privacy interest. *See id.*

138 *Id.* at 70–72.

139 *Id.* at 86.

140 *Id.* at 78.

141 *See id.* at 94 (Scalia, J., dissenting) ("Because the defendant had voluntarily provided access to the evidence, there was no reasonable expectation of privacy to invade.").

142 *Id.* at 95. Justice Scalia noted that the *Ferguson* decision "opens a hole in [the Court's] Fourth Amendment jurisprudence, the size and shape of which is entirely indeterminate." *Id.*

143 *Id.* at 85 n.24 (majority opinion).

However, Justice Stevens did not clarify the nature of the consent to which he was referring: Would he have required the patients' consent for the purpose of a government search or, alternatively, only for the limited purpose of medical treatment?[144] Adopting the former interpretation would effectively overrule *Miller*. Adopting the latter interpretation would narrow the third-party doctrine so that it would only apply to cases in which a person actually consents to giving information to a third party. This would mean that the doctrine would not apply in cases like *Smith*, in which the Court held that the defendant had "volunteered" information to the phone company simply because people in general were on notice of the third party's capacity to gather the information. Whatever meaning Justice Stevens intended, courts apparently have not read the dictum as either eliminating or limiting the doctrine. Regardless, *Ferguson* may prove important in redefining, or perhaps reigning in, the meaning of the word "volunteer" under the third-party doctrine in the future.[145]

The Court's 2010 decision in *City of Ontario v. Quon* suggests that other factors could impose broader limitations on the third-party doctrine.[146] In *Quon*, a police officer alleged that the city had violated his Fourth Amendment rights when the city obtained from a mobile-service provider a transcript of text messages the officer had sent from his city-issued pager.[147] The transcript revealed that the officer had sent non-work-related text messages in violation of the city's policy.[148] Although the Court deferred the question of whether the police officer had a reasonable expectation of privacy in the text messages, it found for the city, explaining that the search, whatever its nature, was reasonable.[149] Importantly, the Court stressed the need for lower courts to exercise caution when applying the Fourth Amendment within the context of new technology:

---

144 *Id.* Professor Thai suggests that, in applying *Ferguson* in future third-party-doctrine cases, "one might ask whether other disclosures to third parties fairly constitute general relinquishments of privacy or serve the more limited function of obtaining services that have become essential to life in our society." Thai, *supra* note 35, at 1749.

145 *See* Christopher Slobogin, *Transactional Surveillance by the Government*, 75 MISS. L.J. 139, 190 (2005); Thai, *supra* note 35, at 1748–49 (arguing that *Ferguson* limits the third-party doctrine to situations in which "volunteering" information is truly elective).

146 *See* 130 S. Ct. 2619 (2010).

147 *Id.* at 2624–26.

148 *Id.* at 2626.

149 *Id.* at 2630. To the frustration of lower courts, *see, e.g.*, Rehberg v. Paulk, 611 F.3d 828, 845–46 (11th Cir. 2010), *cert. granted*, 131 S. Ct. 1678 (2011), the Court sidestepped the Fourth Amendment issue almost entirely, *see Quon*, 130 S. Ct. at 2630.

> The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear. . . .
>
> Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. . . .
>
> . . . Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy.[150]

The excerpt reveals the Court's sensitivity toward two important factors. First, courts should be wary of *society's* real expectations of privacy, and judges should avoid imposing their own conceptions of when privacy is reasonable. Second, courts should be alert for circumstances in which technology might be a necessary medium for protected First Amendment activity, suggesting that expectations of privacy in "self-expression" and "self-identification" warrant protection under the Fourth Amendment. Though the effect of *Quon* has yet to be seen, the case offers some hope that the Court might be willing to limit the third-party doctrine in certain situations involving new technology.

### *E. Does the Third-Party Doctrine Apply to Behavioral Targeting?*

Many commentators fear that the third-party doctrine applies to personal information collected by commercial databases. These commentators, including Christopher Slobogin,[151] Stephen Henderson,[152] and Daniel Solove,[153] have noted the very real danger the doctrine poses in a world of increasing digitization and automation.[154] As Daniel Solove puts it, the Court's third-party doctrine is "not responsive" to the fact that most people's personal

---

150 *Quon*, 130 S. Ct. at 2629–30.

151 *See* Slobogin, *supra* note 145, at 155–57.

152 *See* Henderson, *supra* note 123, at 392–93 (arguing that the third-party doctrine "provides no leash at all" on government access to third-party databases); Henderson, *supra* note 19, at 39–40 (explaining that the doctrine, as it stands today, would seemingly apply to information in commercial databases but hoping that "the Fourth Amendment Third Party Doctrine . . . has at least taken ill, and it can be hoped it is an illness from which it will never recover").

153 *See* Solove, *supra* note 94, at 1137–38.

154 Other scholars have adopted this view. *See* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595, 621–22 (2004); Thai, *supra* note 35, at 1745 ("[A]ny expectation of privacy that we may have [about third-party databases] would be unreasonable under *Miller* and *Smith*'s risk-assumption rationale."); Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 638 (2011) (arguing that a person has a reasonable expectation of privacy in information reviewed automatically by a computer and, therefore, the government infringes upon that expectation by accessing the information).

information is aggregated and stored by hundreds of different entities; as a result, Solove warns, the doctrine "poses one of the most significant threats to privacy in the twenty-first century."[155]

Assuming that the third-party doctrine applies to behavioral targeting, Solove does not overstate its potential danger. There are two arguments worth noting, however, that call into question the doctrine's inevitable application to behavioral targeting. First, most Internet users do not meaningfully consent to behavioral targeting—especially in its current, deregulated form—and many more are not even aware of its existence.[156] If most Internet users are not even *aware* of tracking, then an individual might not be said to have "volunteered" information to an ad network. In turn, if an individual does not "volunteer" her information, she also does not assume the risk that an ad network will share her information with the government. Second, if the Court adopts Justice Stevens's dictum in *Ferguson*—which suggested, at the very least, that a person only "volunteers" information to a third party if she affirmatively consents to sharing information with the third party[157]—the doctrine is even less likely to apply.[158] Even if Internet users are fully aware of online tracking, they are not given a chance to meaningfully consent to it, short of having the option to forgo use of the Internet entirely. These considerations arguably provide some basis for finding that an Internet user has a reasonable expectation of privacy in information collected by an ad network.

The possibility that the third-party doctrine does not apply to behavioral targeting because of either of the preceding two arguments creates a paradoxical situation with regard to privacy. On the one hand, the fact that most people are unaware they are being tracked on the Internet is beneficial to the extent that, because of their shared ignorance, their Fourth Amendment privacy in the information collected about them would be preserved. On the other hand, it is difficult to find comfort in the fact that people are

---

155 Solove, *supra* note 94, at 1087.

156 One study concluded that users are only "passingly familiar" with cookies, and their understanding of behavioral targeting is fraught with "widespread confusion." McDonald & Cranor, *supra* note 49, at 7–8.

157 *See* Ferguson v. City of Charleston, 532 U.S. 67, 84–85 (2001)

158 Given the current state of online privacy policies, it would be a stretch to say that Internet users meaningfully "consent" to their terms. *See Consumer Online Privacy: Hearing Before the S. Comm. on Commerce, Sci., & Transp.*, 111th Cong. 14–15 (2010) (statement of Hon. Jonathan D. Leibowitz, Chairman, Federal Trade Commission) ("[P]rivacy policies have become complicated legal documents that often seem designed to limit companies' liability, rather than to inform consumers about their information practices. . . . [C]onsumers do not understand the extent to which companies are collecting, using, aggregating, storing, and sharing their personal information."); sources cited *supra* note 63.

unknowingly subjected to constant surveillance. To that end, recall the possible improvements on the horizon: the FTC's proposed "Do Not Track" list, which, if implemented, would allow consumers to choose to definitively opt out of behavioral targeting.[159]

But the consequence of adopting the FTC's proposals (or anything like them) is that the application of the third-party doctrine would be seemingly unavoidable when Internet users choose to "opt in" to behavioral targeting. Granting Internet users the power to opt in or out means that both the individual Internet user and people in general will have notice that behavioral targeting occurs. As a result, those Internet users who decide to opt in will have effectively consented to tracking. But Internet users who decide to opt out will face another set of consequences. According to one industry expert, "[o]pting out of tracking may actually harm consumers" because "[m]uch of the free content online today may be[come] unavailable."[160] Assuming that those who opt out would be barred from accessing ad-supported online content, the unavoidable conclusion is that, in the very near future, a person will only be able to access the Internet to the extent it is available today if she agrees to be tracked by a third party—and, by extension, the government.[161] In light of this conclusion, it would seem that the third-party doctrine cannot, in the words of Professor Stephen Henderson, "withstand the pressures which technology and social norms are placing upon it."[162] In the event that the Supreme Court does revisit the doctrine, the question is how it should go about doing so. The following Part offers one possible solution.

## III. A POSSIBLE SOLUTION

> *We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files.*
>
> *—Whalen v. Roe*[163]

---

159 *See supra* note 78.

160 Tanzina Vega & Verne Kopytoff, *The Opt-Out Question*, N.Y. TIMES, Dec. 6, 2010, at B1.

161 Chances are Internet users would likely not opt out of online tracking if a more secure Internet experience meant a more expensive one. *See* Alastair R. Beresford et al., *Unwillingness to Pay for Privacy: A Field Experiment* (Inst. for the Study of Labor, Discussion Paper No. 5017, 2010).

162 Henderson, *supra* note 19, at 51. Professor Henderson offers his own solution—a four-factor test—for determining reasonable expectations of privacy in information given to a third party. *Id.* at 50–51.

163 429 U.S. 589, 605 (1977).

Commentators who argue that the third-party doctrine applies to commercial databases focus on the government's invasion of people's "information privacy."[164] Information privacy, as distinct from "autonomy privacy," is best defined as a person's right to control the gathering, use, and dissemination of personal information.[165] Autonomy privacy, by contrast, is a person's privacy interest in acting in certain ways and making decisions.[166] Though information privacy and autonomy privacy are often described as distinct ideas, the two interests are actually "intimately intertwined."[167] Information reflects a person's actions or choices because any action or choice will generate some information, by way of inference, about the underlying act.[168] For example, in the context of behavioral targeting, an Internet user may have an information-privacy interest in the information collected about her online activity but an autonomy-privacy interest in choosing to access the various types of online content reflected in the information. The two interests are inseparable because the information an ad network collects about the user will necessarily represent what content the user chooses to access.

Though information and autonomy interests are difficult to sever conceptually, the law treats them as separate and discrete.[169] As the Supreme Court recently explained, privacy is typically characterized in the law as "involv[ing] 'at least two different kinds of interests': one, an 'interest in avoiding disclosure of personal matters'; the other, an interest in 'making

---

164 *See* Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1089 (2006) (reviewing DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004)) (observing the "collective effort by a group of scholars to identify a law of 'information privacy' and to establish information privacy law as a valid field of scholarly inquiry" (footnote omitted)).

165 C. Edwin Baker, *Autonomy and Informational Privacy, or Gossip: The Central Meaning of the First Amendment*, SOC. PHIL. & POL'Y, July 2004, at 215, 216–17; Dorothy Glancy, *At the Intersection of Visible and Invisible Worlds: United States Privacy Law and the Internet*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 357, 361 (2000); Richards, *supra* note 164.

166 *See* NASA v. Nelson, 131 S. Ct. 746, 755 (2011).

167 Glancy, *supra* note 165, at 360.

168 *See id.* at 360–62.

169 So do commentators. Professor Richards describes the phenomenon:

> Understandings of the privacy right recognized in [the Court's autonomy-privacy cases] as being related to informational meanings of the word are generally considered by scholars to be beside the point. To the extent that they consider informational meanings of the word 'privacy' in connection with [autonomy-privacy cases], scholars generally either note the ambiguity and move on, or expressly reject any reading of it as an information privacy case.

Richards, *supra* note 164, at 1107 (footnote omitted).

certain kinds of important decisions' free from government interference."[170] Or, in the words of Professor Neil Richards, information privacy is "a limit on the state's power to scrutinize" personal information representing autonomous acts, whereas autonomy privacy is "the individual right to make certain kinds of fundamental decisions without state interference."[171] Professor Richards emphasizes the meaninglessness of this distinction, noting that the legal difference between the two is a matter of definitional subtlety.[172] And indeed, this distinction is circular: limiting the state's power to scrutinize an interest *necessarily* results in less state interference with the interest; in turn, if the state cannot interfere with an interest, it also cannot scrutinize the interest.

Nevertheless, the categorization of privacy as either informational or autonomy-based has led to the development of divergent bodies of constitutional jurisprudence dealing with each.[173] Information privacy tends to be the subject of the Fourth Amendment, whereas autonomy privacy is associated with substantive due process protections found in the Fifth and Fourteenth Amendments,[174] and expressive and associational freedoms

---

[170] *Nelson*, 131 S. Ct. at 755 (footnote omitted) (quoting Whalen v. Roe, 429 U.S. 589, 599–600 (1977)). In January 2011, the Supreme Court handed down an opinion in which it stated that a person's "'interest in avoiding disclosure'[ of personal information] . . . may 'arguably ha[ve] its roots in the Constitution.'" *Id.* at 751 (third alteration in original) (quoting *Whalen*, 429 U.S. at 599, 605). In *NASA v. Nelson*, the Court assumed for its analysis that the Constitution protects "information privacy"—at least defined as the right to control *dissemination* of personal information—under substantive due process. *Id.* The case involved NASA employees who were challenging the government agency's intrusive background checks. *Id.* In an 8–0 opinion, the Court held that the government had a rational basis for conducting the background checks, and as a result, the employees' hypothetical information privacy was not violated. *Id.* at 758–59. Notably, the employees' Fourth Amendment challenge was not at issue on appeal; the Ninth Circuit had discarded it under the third-party doctrine. Nelson v. NASA, 530 F.3d 865, 876–77 (2008), *rev'd*, 131 S. Ct. 746. Justice Scalia, in his concurring opinion, rejected the notion of a constitutional right to informational privacy and warned, in reference to the clear applicability of *United States v. Miller*, that "[c]ourts should not use the Due Process Clause as putty to fill up gaps they deem unsightly in the protections provided by other constitutional provisions." *Nelson*, 131 S. Ct. at 765 (Scalia, J., concurring in the judgment). Though the implications of *Nelson* are far from clear, the case seems to forecast an increasing segmentation and categorization of constitutional privacy. Rather than exploring that forecast in detail, this Comment seeks to resolve the problems arising from categorizing privacy that manifest in the Fourth Amendment third-party doctrine. As such, "information privacy" in this Comment refers to the right to control not only the *dissemination* but also the collection and retention of personal information.

[171] Richards, *supra* note 164, at 1112.

[172] *Id.* at 1115–16.

[173] Glancy, *supra* note 165, at 360.

[174] *See* DANIEL J. SOLOVE ET AL., INFORMATION PRIVACY LAW 1 (2d ed. 2006) (distinguishing between "decisional privacy" and "information privacy," and stating that decisional privacy falls under substantive due process); Thomas P. Crocker, *From Privacy to Liberty: The Fourth Amendment After* Lawrence, 57 UCLA L. REV. 1, 3–4 (2009) (describing the different doctrinal frameworks under which the Fourth Amendment and Due Process Clauses of the Fifth and Fourteenth Amendments protect privacy).

guaranteed by the First Amendment.[175] For the most part, the categorization works well enough. In certain cases, however, distinguishing between two types of constitutionally protected privacy is problematic.[176] The third-party doctrine offers a prime example. Under the third-party doctrine, if a person "volunteers" information to a third party, she loses all constitutional protection for the information, regardless of whether it reflects an underlying autonomy interest that is otherwise protected by the Constitution.[177] The result is that the third-party doctrine permits the government to indirectly interfere with a person's constitutionally protected *autonomy privacy* under the pretext that the person is not entitled to *information privacy* under the Fourth Amendment. Stated differently, the third-party doctrine works as a vehicle to circumvent constitutional protections beyond the Fourth Amendment.

The remainder of this Comment will explore the nuances of constitutional privacy interests in relation to the third-party doctrine, with the goal of reconciling the problems that arise in the context of behavioral targeting. The following section discusses two initial premises that are critical to resolving problems inherent in the third-party doctrine. First, Fourth Amendment privacy consists of both information- and autonomy-privacy interests—what will be referred to as "information/autonomy privacy." Second, the third-party doctrine is better justified by a rationale that takes into account the *third party's* privacy interests—specifically, the third party's autonomy interest in sharing information with the government, referred to in this Comment as the "third-party-privacy justification." With these two concepts in mind, the Comment then offers a new analytical framework for the doctrine, called the "competing-interests test." Under the competing-interests test, the result in any third-party-doctrine case will depend on a weighing of the individual's information/autonomy interest against the third party's competing autonomy interest. Depending on which party's interest prevails, the individual's autonomy/privacy interest will either be subject to the third-party doctrine or be deserving of Fourth Amendment protection. The Comment concludes by applying the competing-interests test in the context of behavioral targeting and by then addressing possible criticisms of the competing-interests test.

---

175 *See* Crocker, *supra* note 174, at 12, 20, 22.

176 According to Professor Richards, the "informational/decisional binary"—as he calls it—is "imperfect—a crude sorting of cases that does not hold up well to careful analysis." Richards, *supra* note 164, at 1115. Richards concludes that the "ambiguity has persisted [in constitutional privacy] such that informational elements can be found even in cases falling undoubtedly on the decisional [or autonomy] side of the binary." *Id.* at 1114.

177 *See* United States v. Miller, 425 U.S. 435, 443 (1976).

### *A. Reconceptualizing the Third-Party Doctrine: Information/Autonomy Privacy and Third-Party Autonomy*

This section explains two concepts that are key to understanding and reconceptualizing the third-party doctrine. First, as already described, Fourth Amendment protections encompass both information- and autonomy-privacy interests—what can be described as a single information/autonomy interest. Second, a better justification for the third-party doctrine lies in protecting the third party's autonomy interest in sharing information with the government, not in an individual's assumption of the risk that a third party will share information with the government.

First, reconceptualizing the third-party doctrine requires accepting, as an initial premise, that privacy cannot be viewed in a vacuum—as relating either to personal information or to personal choices—because personal information inevitably must reflect personal choices. Denying protection for personal information results in a denial of protection for the underlying act. Thus, one of the main flaws in the third-party doctrine is that it applies only to *information* volunteered to a third party. In the three main third-party-doctrine cases, for example, the Court consistently speaks of "information" volunteered to a third party and frames the individual's expectation of privacy as being in information. The *Miller* case dealt with information from the defendant's financial records,[178] *Smith* with telephone calling records,[179] and *Greenwood* with the information gleaned from the content of trash.[180] This makes sense: What else could a third party ever receive from an individual (short of tangible objects) that she could then share with the government? But by rigidly categorizing an individual's Fourth Amendment privacy as solely informational, the Court overlooks the individual's underlying autonomy-privacy interests. For example, in *Miller*, the Court overlooked the defendant's interest in using a bank account; in *Smith*, the defendant's interest in making phone calls; and in *Greenwood*, the defendant's interest in disposing of trash. The case of behavioral targeting is no different: a person has an information-privacy interest in information collected by an ad network and, necessarily, an autonomy-privacy interest in accessing the Internet.

Recognizing one sweeping Fourth Amendment information/autonomy privacy interest is especially important because, in some circumstances, the

---

178 *Id.* at 437–38.
179 442 U.S. 735, 737–38 (1979).
180 486 U.S. 35, 37–38 (1988).

individual's underlying autonomy interest is otherwise protected by the Constitution.[181] As already noted, the third-party doctrine has the power to eviscerate those protections and could even be used to purposely circumvent them.

For example, the third-party doctrine would seem to apply to information even when it reflects an underlying autonomy interest protected by the Due Process Clauses of the Fifth and Fourteenth Amendments. By way of background, the Court first recognized a constitutional right to autonomy privacy under the Due Process Clause in *Griswold v. Connecticut*, in which it held that people have a right to marital privacy, which includes the right to use contraceptives.[182] The Court has since expanded autonomy-privacy interests emanating from substantive due process to protect decisions and activities related to family,[183] reproduction,[184] sex,[185] and medical treatment.[186] Generally speaking, the reasoning behind these cases stems from the notion that substantive due process protects the right to make intimate decisions without government interference. In other words, as the Court recently explained, substantive due process protects what society considers "the most *private* human conduct."[187]

---

[181] For example, in the case of behavioral targeting, an Internet user may have an underlying autonomy interest in engaging in protected First Amendment activity. If the information collected about such activity is not protected by the Fourth Amendment, then the Internet user's First Amendment rights are effectively curtailed, either because she will be substantially deterred from engaging in protected activity or because the information gathering itself constitutes a direct interference with her expressive freedoms.

[182] 381 U.S. 479, 485 (1965).

[183] *See, e.g.*, Santosky v. Kramer, 455 U.S. 745, 753 (1982) (recognizing that "freedom of personal choice in matters of family life is a fundamental liberty interest protected by the Fourteenth Amendment," including "[t]he fundamental liberty interest of natural parents in the care, custody, and management of their child"); Moore v. City of E. Cleveland, 431 U.S. 494, 501, 505–06 (1977) (plurality opinion) (upholding the right of a non-nuclear family to live and stay together); Loving v. Virginia, 388 U.S. 1, 11–12 (1967) (upholding marriage as a "basic civil right[] of man" and rejecting a restriction that prohibited interracial marriages (quoting Skinner v. Oklahoma, 316 U.S. 535, 541 (1942)) (internal quotation marks omitted)).

[184] *See, e.g.*, Roe v. Wade, 410 U.S. 113 (1973); *Griswold*, 381 U.S. at 485–86 (finding that the right to purchase and use contraceptives is constitutionally protected); *Skinner*, 316 U.S. at 541 (recognizing procreation as "one of the basic civil rights of man" and "fundamental to the very existence and survival of the race").

[185] Lawrence v. Texas, 539 U.S. 558, 567 (2003) (establishing the right to engage in private, sexual conduct).

[186] Cruzan v. Dir., Mo. Dep't of Health, 497 U.S. 261, 278 (1990) ("[A] competent person has a constitutionally protected liberty interest in refusing unwanted medical treatment . . . ."); Vitek v. Jones, 445 U.S. 480, 493–94 (1980) (holding that a prison cannot involuntarily subject prisoners to psychiatric treatment without additional due process protections).

[187] *Lawrence*, 539 U.S. at 567 (emphasis added).

Similarly, the third-party doctrine in theory applies to information that reflects protected First Amendment activity as well.[188] The First Amendment protects another type of autonomy-privacy interest, distinct from the autonomy interest established in the *Griswold* line of cases and stemming from substantive due process.[189] The First Amendment safeguards autonomy in the realm of religious practice, democratic participation, and, as Justice Thurgood Marshall once noted, "the human spirit—a spirit that demands self-expression."[190] Indeed, freedom of speech is perhaps the ultimate autonomy interest, providing the key to "individual self-realization"[191] and "autonomous self-determination."[192] These protections provide not only for individual autonomy but also for broader, societal autonomy, because freedom of speech furthers society's ability to seek out knowledge and truth, and to engage in collective decision making.[193] Society's autonomy interest is manifest in the right to engage in the political process and, ultimately, "the right to participate in the building of the whole culture."[194] The First Amendment provides broad privacy protections to further these autonomy interests, including the rights to explore ideas, to associate freely, and to remain anonymous.[195]

---

[188] *See, e.g.*, Stanley v. Georgia, 394 U.S. 557 (1969). Professor Daniel Solove has written about the problematic intersection of the First and Fourth Amendments, arguing that the Founders intended the Fourth Amendment to act as a first line of defense for First Amendment rights. Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112 (2007).

According to Solove, the Fourth Amendment's warrant requirement is supposed to protect First Amendment activity, such that when First Amendment activity is implicated, the Fourth Amendment should *always* require the government to obtain a warrant. Solove, *supra*. Solove draws from Supreme Court precedent demanding that the Fourth Amendment warrant requirement be observed with "scrupulous exactitude" when First Amendment interests are implicated. *Id.* at 128–32; *accord* Stanford v. Texas, 379 U.S. 476, 484–85 (1965). Nevertheless, the third-party doctrine creates the possibility that First Amendment activity might fall outside the ambit of the Fourth Amendment and, as a result, receive no protection at all.

[189] Under the First Amendment, "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; of the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." U.S. CONST. amend. I.

[190] Procunier v. Martinez, 416 U.S. 396, 427 (1974) (Marshall, J., concurring), *overruled by* Thornburgh v. Abbott, 490 U.S. 401 (1989).

[191] Martin H. Redish, *The Value of Free Speech*, 130 U. PA. L. REV. 591, 593 (1982) (internal quotation marks omitted).

[192] David A.J. Richards, *Free Speech and Obscenity Law: Toward a Moral Theory of the First Amendment*, 123 U. PA. L. REV. 45, 62 (1974).

[193] C. EDWIN BAKER, HUMAN LIBERTY AND FREEDOM OF SPEECH 47 (1989).

[194] *Id.* (quoting THOMAS EMERSON, THE SYSTEM OF FREEDOM OF EXPRESSION 7 (1970)) (internal quotation mark omitted).

[195] *See* Solove, *supra* note 188, at 121 (arguing that government information gathering can threaten privacy protections of the First Amendment); *see also* Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Village of Stratton, 536 U.S. 150, 165–67 (2002) (invalidating an ordinance that required a government permit

The third-party doctrine is at odds with constitutionally protected autonomy interests emanating from substantive due process and the First Amendment, placing them in tension with the Fourth Amendment. Thus, one key to reconciling conflicting notions of constitutional privacy is to recognize an expansive conception of Fourth Amendment privacy that encompasses both information and autonomy interests.

Second, in addition to adopting a broader Fourth Amendment privacy interest, the Court must replace its flawed assumption-of-risk rationale for the third-party doctrine with an alternative justification—referred to here as the third-party-privacy justification. Under the third-party-privacy justification, the third-party doctrine is a mechanism for protecting the *third party's* autonomy interest in sharing information with the government, rather than a limit on an individual's privacy based on assumption of risk.[196] Mary Coombs argues in favor of such an approach, explaining that "[t]o deny even the possibility of such a decision [by the third party] is to turn a freely chosen relationship [between the third party and an individual] into a status, denying one person's full personhood to protect another's interests."[197] In other words, the third-party doctrine is necessary for protecting the third party's "full personhood," even at the expense of the individual's Fourth Amendment privacy.

When viewed through the lens of the third-party-privacy justification, the third-party doctrine, as it exists now, represents a compromise between two competing interests: the individual's Fourth Amendment privacy interest—what the Court perceives as a limited information-privacy interest—weighed against a third party's autonomy interest in sharing information with the government. If viewed from this perspective, one of the inherent problems with

---

before the distribution of religious pamphlets as a violation of the First Amendment right to anonymous political speech); Bates v. City of Little Rock, 361 U.S. 516, 522–23, 527 (1960) (holding that municipalities could not require the disclosure of NAACP membership lists and that such a requirement significantly interfered with members' freedom-of-association rights); NAACP v. Alabama, 357 U.S. 449, 462–63, 466 (1958) (holding that state scrutiny of NAACP membership lists violated members' rights to associate freely and privately).

196 *See* SLOBOGIN, *supra* note 90, at 159; Mary I. Coombs, *Shared Privacy and the Fourth Amendment, or the Rights of Relationships*, 75 CALIF. L. REV. 1593, 1643–44 (1987); Slobogin, *supra* note 145, at 185 ("The reason we should treat [personal] interviews differently from [impersonal, automated] records requests is not because privacy somehow is irrelevant in the former situation, but because the target's interest in privacy is countered by an even stronger interest—the third party's autonomy.").

197 Coombs, *supra* note 196, at 1644. On the other hand, Stephen Henderson has described the third party's interest in sharing information with the government as a "good citizen" as irrelevant and insufficient to overcome an individual's Fourth Amendment rights. Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 1015 (2007).

the Court's third-party doctrine becomes that, as a rule, the result of weighing the two competing interests is always the same. Under the Court's third-party doctrine, the third party's interest *always* prevails. In essence, the third party's autonomy interest in sharing information with the government is treated as absolute.

In light of the third-party-privacy justification, this result makes the most sense when the third party is a *person*, or *people in general* (the public), as opposed to an entity. As Professor Slobogin observes, the notion that "no person should be able to prevent another from providing information to the government" is virtually "incontestable."[198] In cases that involve human third parties, such as the undercover-agent and confidential-informant cases (which, to recall, were precursors to *Miller*[199]), placing a high value on the third party's autonomy interest is not particularly troubling.[200]

On the other hand, when the third party is not a person, the result of the third-party doctrine under the third-party-privacy justification is less compelling.[201] Why should a person's privacy be compromised for the sake of an entity's seemingly lesser autonomy interest? While, at times, the Court has reserved a lesser privacy interest for "collective" entities—in one instance stating that "corporations can claim no equality with individuals in the enjoyment of a right to privacy"[202]—the Court has also affirmed the notion that corporate entities possess broad autonomy interests under the Constitution, including, for example, in the realm of the First Amendment.[203] The current state of the third-party doctrine reflects the latter sentiment, at least to the extent that entities prevailed in all three of the Court's traditional third-party-doctrine cases. Recall that, in *Miller*, the third party was a bank; in *Smith*, a phone company; and, in *Greenwood*, a refuse collection company. But regardless of the Court's position on entities' privacy or autonomy interests—

---

198 SLOBOGIN, *supra* note 90, at 159.

199 *See* discussion *supra* Part II.B.

200 *See supra* note 196.

201 According to Professor Slobogin, "A bank, hospital, or ISP is not denied its 'personhood' when its ability to turn information over to the government is restricted." SLOBOGIN, *supra* note 90, at 159. Slobogin argues that entity third parties by their nature do not have any autonomy privacy. *See id.* (explaining the justification for the low relevancy requirement to support a subpoena duces tecum for corporate records).

202 United States v. Morton Salt Co., 338 U.S. 632, 652 (1950). Within the context of the Fifth Amendment, for example, an organization that has an identity separate from its individual members does not have a right to resist a documentary subpoena, because its records lie outside the "zone of privacy." SLOBOGIN, *supra* note 90, at 187; *see also, e.g.*, Hale v. Henkel, 201 U.S. 43, 73–75 (1906).

203 *See* Citizens United v. FEC, 130 S. Ct. 876, 913 (2010) (holding that corporations have a First Amendment interest in political speech).

which is far from clear—instinct suggests that a corporation's autonomy interest in sharing information with the government should yield, at times, to an individual's Fourth Amendment privacy. Thus, in adopting the third-party-privacy justification for the third-party doctrine, it is essential to recognize that the third party's interest should not be treated as absolute.

To summarize, then, reconceptualizing the third-party doctrine requires that the Court recognize the two important points discussed so far. First, Fourth Amendment privacy consists of a broad information/autonomy privacy interest, which may implicate autonomy interests that are otherwise protected by the Constitution. Second, the third-party doctrine is better justified as a means of protecting the third party's autonomy interest in sharing information with the government. The third party's interest, while valuable, is not absolute, and perhaps there are circumstances in which the third party's autonomy interest should yield to an individual's Fourth Amendment information/autonomy interest.

### *B. The "Competing-Interests Test"*

With these ideas in mind, the Court should adopt a new analytical framework for the third-party doctrine—what will be referred to as the "competing-interests test" for the purposes of this discussion. The competing-interests test is comprised of a two-step analysis. First, the Court must assign independent values to both the individual's and the third party's competing interests, which include the individual's information/autonomy interest on the one hand and the third party's autonomy interest in sharing information with the government on the other. Second, the Court must weigh the two interests against each other as part of the second prong of the *Katz* test, which will determine whether an individual's expectation of privacy is reasonable as to information held by a third party. Under this framework, the third-party doctrine will apply as usual when the third party's autonomy interest outweighs the individual's information/autonomy privacy interest. However, the third-party doctrine will *not* apply when an individual's information/autonomy interest outweighs the third party's autonomy interest in sharing information with the government. Thus, when the individual's interest prevails, the individual's expectation of privacy should be deemed reasonable within the meaning of the Fourth Amendment.

In the first step of the competing-interests test, the Court should assign a value to the two competing interests at stake according to three guiding

principles. The first guiding principle is that, when the third party is reporting information pursuant to government compulsion—for example, in compliance with a warrant or subpoena—the third party's autonomy-privacy interest should be given little, if any, weight. Under these circumstances, the third party's autonomy privacy is nonexistent because she is not exercising any choice about whether to share information with the government. Instead, the third party effectively is acting *as* the government.[204] This conclusion has some important consequences depending on the nature of the government compulsion. First, if the compulsion is made pursuant to a warrant, then the requirements of the Fourth Amendment are satisfied notwithstanding the third-party doctrine. Second, in all other circumstances, the third-party doctrine typically would not apply at all: because the third party's autonomy interest is so diminished, it will almost always be outweighed by the individual's information/autonomy interest. This conclusion does not mean that government compulsion short of a warrant is per se unconstitutional, however. Rather, it means that the third-party doctrine cannot be the basis for its validity under the Fourth Amendment.

Under the second guiding principle, the third party's autonomy-privacy interest generally should weigh less when the third party is an entity as opposed to when the third party is a human. This principle is based on the premise that entities need not enjoy constitutional rights to the same extent that individuals do when they come at the expense of individuals.[205] In the context of behavioral targeting, this means that, because an ad network is an entity, its autonomy interest carries less weight in the competing-interests calculus than if it were a person. Accordingly, whether the ad network's diminished autonomy interest would prevail in any given situation would depend on the relative weight given to the individual's competing information/autonomy interest. Admittedly, this principle creates a gray area because the outcome depends on how the Court chooses to value the individual's information/autonomy interest. In turn, how the Court chooses to value an individual's interest might also depend on how it *defines* the nature of the individual's underlying autonomy interest. Happily, the next principle helps resolve some of the blurriness in this area.

---

[204] *See* Henderson, *supra* note 197, at 992 ("If the third party obtaining the information is effectively law enforcement, or if that party is obtaining or retaining the information for law enforcement, and it is obtained or retained solely for a law enforcement purpose, unfettered collection and/or access [should be considered] unreasonable.").

[205] *See* discussion *supra* notes 32–33.

Under the third—and final—guiding principle, the individual's information/autonomy interest should carry the most weight when it involves an underlying autonomy interest that is otherwise protected by the Constitution,[206] such that, when the third party is an entity, the individual's interest should always prevail and the third-party doctrine should never apply. The same is not true when the third party is a person, however. Even when an individual's underlying autonomy interest is constitutionally protected, the third party's interest nevertheless should prevail. While this outcome places the third party's interest in sharing information with the government above the individual's constitutional autonomy interest, to hold otherwise would result in "denying one person's full personhood to protect another's interests," as Professor Coombs observes.[207] In the case of behavioral targeting, then, because the Internet user's information/autonomy privacy arguably implicates substantive due process or First Amendment rights, the Internet user's information/autonomy interest outweighs the autonomy interest of the ad network, an entity. As a result, information collected by ad networks would be protected by the Fourth Amendment and inaccessible to the government absent a warrant. Importantly, however, the result would be different if the ad network were a person, instead of an entity. Under those circumstances, the ad network's autonomy interest would always outweigh the Internet user's information/autonomy interest.

The three guiding principles leave one circumstance unaccounted for—the circumstance in which the third party is an entity, but the individual's underlying autonomy interest is not otherwise constitutionally protected. In this scenario, the Court would still need to assign values to each party's interest and weigh them against each other accordingly. How the Court would value each interest might depend on a variety of other factors, however. As for a third-party entity, perhaps a partnership might have a stronger autonomy interest than a publicly traded corporation. As for an individual, perhaps her autonomy interest should be given greater weight when it reflects an activity that is essential to everyday life or which is more or less involuntary. As a general rule, an entity's autonomy interest should prevail against an

---

[206] Professor Crocker makes a similar, but narrower, argument: "[T]he Fourth Amendment protects not only privacy, but also liberty. . . . If the [government] intrusion implicates a protected interpersonal relationship, then the State must follow default Fourth Amendment procedures in order to conduct a valid search." Crocker, *supra* note 175, at 9.

[207] Coombs, *supra* note 196, at 1644.

individual's only if it is extremely compelling.[208] Concededly, the competing-interests test threatens to become quite complicated and nuanced under this category. The possibility of complication alone should not defeat the test, however. While it is possible to imagine any number of factors that would help courts navigate the nuances of this category, such an exercise exceeds the scope of this Comment.

Thus, the possible results of applying the guiding principles to the competing-interests test is illustrated below:

[208] Perhaps, for example, an entity's autonomy interest might prevail when it seeks to share information about an individual to prevent an imminent national emergency.

| | **Is the third party a person or an entity?** | **Is the individual's underlying autonomy interest protected under the Due Process Clauses or the First Amendment?** | **Prevailing party** | **Is the individual's expectation of privacy reasonable under *Katz*?** |
|---|---|---|---|---|
| **I** | Third party is a person | Yes | Third Party | No |
| **II** | Third party is a person | No | Third Party | No |
| **III** | Third party is an entity (diminished autonomy interest) | Yes | Individual | Yes |
| **IV** | Third party is an entity (diminished autonomy interest) | No | Individual or Third Party, depending | Yes or No, depending |
| **V** | Person or entity **No autonomy interest: third party is required to report information to the government* | N/A | Individual | Yes, if government compulsion was not pursuant to a warrant or otherwise-appropriate individualized suspicion |

### *C. Applying the New Third-Party Doctrine to Behavioral Targeting*

The competing-interests test would resolve the fears surrounding a strict application of the third-party doctrine to personal information gathered by ad networks for behavioral targeting. In particular, the test would permit Internet users to consent to behavioral targeting to access online content for free without simultaneously relinquishing all Fourth Amendment protections. As a result, Internet users could enjoy increased online privacy as to both ad networks *and* the government. The competing-interests test also takes into account the reality of today's increasingly digitized world in which participation in everyday life requires sharing information. If, in some not-too-

distant future, every facet of life is recorded by third parties and kept in a database accessible by the government, the third-party doctrine will allow modern technology to swallow the Fourth Amendment.[209] Behavioral targeting offers proof that comprehensive, real-time recordation of people's personal lives is not only possible but already happening.

Applying the competing-interests test to the case of behavioral targeting is fairly straightforward. The first step requires the Court to assign a value to each party's interest—the individual's information/autonomy interest, on the one hand, and the third party's interest in sharing information with the government, on the other—taking into account the three guiding principles. The first principle would not apply to behavioral targeting unless the government compelled the third party, the ad network, to provide information pursuant to a law. Assuming no such compulsion exists, the case does not fall under situation V in the table above. Under the second principle, because the ad network is an entity, rather than a person, the Court would assign a diminished value to the ad network's interest in sharing information with the government. Therefore, depending on how the Court valued the Internet user's information/autonomy interest, the case would fall under situation III or IV.

How the Court would value the Internet user's information/autonomy interest would depend on how it defined the user's underlying autonomy interest. According to the third principle, if the Court defined the interest as one protected under substantive due process or the First Amendment, then the Internet user's interest would prevail. For example, an Internet user arguably has a substantive due process right in gathering information about medical treatment, or perhaps about issues relating to sexuality on the Internet, because exploring information is critical to, or perhaps represents in itself, an intimate choice regarding those protected areas.[210] The user's underlying autonomy interest might also be defined as a broad First Amendment freedom.[211] When a person browses the Internet, she engages in protected First Amendment activity—she explores and receives ideas, she associates freely, and she may have a right to anonymity.

If the Internet user's underlying autonomy interest were found to implicate either substantive due process or First Amendment autonomy interests, then

---

[209] According to estimates, the volume of the world's collected data *doubles* every year. THE CONSTITUTION PROJECT, *supra* note 91, at 8.

[210] *See* Solove, *supra* note 188, at 122.

[211] *See id.* at 121–23.

under the second prong of the competing-interests test, the Internet user's information/autonomy interest would prevail over the ad network's interest in sharing information with the government and, therefore, would be subject to Fourth Amendment protection.[212] The result would be the same even if the Internet user consented to being tracked when, if given the option to join a "Do Not Track" list, she declined in order to access ad-supported online content. In other words, the fact that an Internet user consents to being tracked by a third party does not mean she enjoys a lesser Fourth Amendment privacy interest as to the government.

On the other hand, the Court might define the Internet user's underlying autonomy interest as one that does *not* implicate some constitutional right. For example, the Court could view the Internet user's underlying autonomy interest as the right to be able to access online content for free. This interest—access to *free* online content—likely garners no support from the Court's substantive due process or First Amendment jurisprudence. As another example, the Court could define the autonomy interest as the right to access any given *single* webpage (rather than the Internet in its entirety) without government interference. Similarly, this interest may not trigger constitutional protection because the amount of interference would be de minimis. Under these narrow definitions, the case would fall under the gray area of situation IV, and the individual's information/autonomy interest would only prevail if the Court assigned her underlying autonomy interest a higher value (based on nonconstitutional considerations) than the ad network's interest in sharing information with the government.

Though there is no way of knowing how the Court would define the Internet user's underlying autonomy interest, the Court's recent direction in *City of Ontario v. Quon* suggests that it would be willing to view the interest as one that is constitutionally protected.[213] To recall, the Court expressed sensitivity toward the potential privacy implications of new technology that is "so pervasive" that it is an "essential means or necessary instrument[] for self-expression, even self-identification."[214] The Internet is not only a pervasive fixture in everyday life; it is also a permanent and essential one. Tied up in the Internet's role is behavioral targeting, and tied up in behavioral targeting is, quite literally, information reflecting self-expression and self-identification.

---

212 The case would fall under situation III in the table.

213 *See supra* notes 146–50 and accompanying text.

214 City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010).

Ultimately, if the government's unfettered access to this information were reasonable under the Fourth Amendment, then the Court's language in *Quon* would be stripped of its meaning. At least in light of *Quon*, it seems that the Internet user's underlying autonomy interest would be constitutionally protected, thus triggering Fourth Amendment protection under the competing-interests test.

## CONCLUSION

Justice Brandeis once described the right to privacy—what he termed "the right to be let alone"—as "the most comprehensive of rights and the right most valued by civilized men."[215] Fearing that "[w]ays may some day be developed by which the Government, without removing papers from secret drawers, [could] reproduce them in court . . . to expose . . . the most intimate occurrences of the home,"[216] the Justice urged a reading of the Fourth Amendment that would allow for adaptation in a world of technological change: "Clauses guaranteeing to the individual protection against specific abuses of power, must have a . . . capacity of adaptation to a changing world. . . . '[I]n the application of a constitution, our contemplation cannot be only of what has been but of what may be.'"[217] Justice Brandeis's words resonate even more ominously with the advance of behavioral targeting. Never before have third parties held so much personal information about so many people—a reality likely irreversible given the central and permanent role the Internet plays in everyday life. Indeed, "[a]s a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression" by comparison.[218] In light of these technological developments, it is imperative that the Supreme Court reevaluate its third-party doctrine.

This Comment has argued that the Court could limit the third-party doctrine by adopting a new analytical framework called the competing-interests test. The competing-interests test would require the Court to broaden its conception of Fourth Amendment privacy while acknowledging that the third-party doctrine is justified as a safeguard of third-party autonomy interests in sharing information with the government. Importantly, instead of categorically barring Fourth Amendment protection for any information an

---

[215] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

[216] *Id.* at 474.

[217] *Id.* at 472, 474 (quoting Weems v. United States, 217 U.S. 349, 373 (1910)).

[218] *Id.* at 476.

individual volunteers to a third party, the competing-interests test would safeguard an individual's Fourth Amendment privacy when that interest is most compelling. Accordingly, the competing-interests test contemplates not only what has been but also what may be, so to better secure "the most comprehensive of rights and the right most valued by civilized men"—the right to privacy.

ELSPETH A. BROTHERTON*

* Articles Editor, *Emory Law Journal*; J.D. Candidate, Emory University School of Law (2012); Bachelor of Music in Musicology, Oberlin Conservatory (2008). I would like to extend my most sincere gratitude to Professor Sara Stadler, whose support, enthusiasm, and candor proved invaluable while writing this comment. I would also like to thank Sarah Stein, Andrew McKinley, and Daniel Reach for their detailed and thoughtful feedback throughout the writing and editing process. I would be remiss if I did not mention Professor Thomas Arthur, whose immeasurable kindness and support throughout law school played a critical, if indirect, role in this project. Finally, I am indebted to my family for their love and encouragement.