Before the
Department of Commerce
Washington, DC 20230

In the Matter of

Docket No. 101214614–0614–01

COMMENTS
OF
THE AMERICAN CIVIL LIBERTIES UNION ("ACLU")

Do Not Track: A Fundamental Civil Liberties Protection for the 21st Century

Christopher Calabrese
American Civil Liberties Union
915 15th Street, NW
Washington, DC 20005

Dated: January 28, 2011

We applaud the Department of Commerce for addressing internet privacy and reform of the Electronic Communication Privacy Act (ECPA) in its report, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework.* But we also believe the Commerce report is deficient in one key respect. The report should have called for the creation of a "Do Not Track" option like that described in the Federal Trade Commission (FTC) report *Protecting Consumer Privacy in an Era of Rapid Change*. A "Do Not Track" option and limitations on data sharing are crucial civil liberties protections necessary to safeguard Americans' First and Fourth Amendment rights online.

The American Civil Liberties Union (ACLU) has more than half a million members, countless additional activists and supporters, and fifty-three affiliates nationwide. We are one of the nation's oldest and largest organizations advocating in support of individual rights in the courts and before the executive and legislative branches of government.

Rapid technological advances and the lack of an updated privacy law have resulted in a system where Americans are routinely tracked as they surf the internet. The result of this tracking – often performed by online marketers – is the collection and sharing of Americans' personal information with a variety of entities including offline companies, employers and the government. As greater portions of our lives move online, unregulated data collection has become a growing threat to our civil liberties.

As both the Commerce and FTC reports explain, the internet has been the engine of radical, positive changes in the way we communicate, learn, and transact commerce. The internet allows us to connect to one another and share information in ways we never before could have imagined. Many of the civil liberties benefits of the internet – ability to read provocative materials, associate with non-mainstream groups, and voice dissenting opinions – are based on the assumption of practical anonymity. Americans assume that there is no central record of what they do and where they go online. However in many instances that is no longer the case. Behavioral marketers are creating profiles of unprecedented breadth and depth that reveal personal aspects of people's lives including their religious or political beliefs. Behavioral targeting is still in its infancy, but it has already demonstrated a disturbing ability to track and monitor.

If this collection of data is allowed to continue unchecked, then capitalism will build what the government never could – a complete surveillance state online. Without government intervention we may soon find the internet has been transformed from a library and playground to a fishbowl, and that we have unwittingly ceded core values of privacy and autonomy.

I. Americans have embraced technology, but they still expect privacy

Technology has moved rapidly and Americans have adopted these changes into their lives:

- Over 50% of American adults use the internet on a typical day.[1]
- 62% of online adults watch videos on video-sharing sites, [2] including 89% of those aged 18–29.[3]
- Over 70% of online teens and young adults[4] and 35% of online adults have a profile on a social networking site. [5]
- 83% of Americans own a cell phone and 35% of cell phone owners have accessed the Internet via their phone.[6]

Companies continue to innovate and create new ways for Americans to merge technology with daily activities. Google has spent the last five years building a new online book service and sales of digital books and devices have been climbing.[7] Americans increasingly turn to online video sites to learn about everything from current news to politics to health.[8] Location-based services[9] are a burgeoning market.[10]

However this rapid adoption of new technology has not eliminated Americans' expectations of privacy. To the contrary, Americans still expect and desire that their online activities will remain private, and express a desire for laws that will protect that privacy.

---

[1] Common daily activities include sending or receiving email (40+% of all American adults do so on a typical day), using a search engine (35+%), reading news (25+%), using a social networking site (10+%), banking online (15+%), and watching a video (10+%). Pew Internet & American Life Project, *Daily Internet Activities, 2000–2009*, http://www.pewinternet.org/Trend-Data/Daily-Internet-Activities-20002009.aspx.

[2] A "video-sharing site" or "video hosting site" is a website that allow users to upload videos for other users to view (and, often, comment on or recommend to others). Wikipedia, *Video Hosting Service*, http://en.wikipedia.org/wiki/Video_sharing (as of January 21, 2011). YouTube is the most common video-sharing site today.

[3] Pew Internet & American Life Project, *Your Other Tube: Audience for Video-Sharing Sites Soars*, July 29, 2009, http://pewresearch.org/pubs/1294/online-video-sharing-sites-use

[4] Pew Internet & American Life Project, *Social Media & Young Adults*, Feb. 3, 2010, http://www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx.

[5] "Social networking sites" allow users to construct a "semi-public" profile, connect with other users of the service, and navigate these connections to view and interact with the profiles of other users. danah m. boyd & Nicole B. Ellison, *Social Networking Sites: Definition, History, and Scholarship,* 13 J. of Comp.-Mediated Comm. 1 (2007); Pew Internet & American Life Project, *Adults & Social Network Sites*, Jan. 14, 2009, http://www.pewinternet.org/Reports/2009/Adults-and-Social-Network-Websites.aspx.

[6] Pew Internet & American Life Project, *Internet, Broadband, and Cell Phone Statistics*, Jan. 5, 2010, http://www.pewinternet.org/Reports/2010/Internet-broadband-and-cell-phone-statistics.aspx.

[7] *See generally* ACLU of Northern California, *Digital Books: A New Chapter for Reader Privacy*, Mar. 2010, *available at* http://www.dotrights.org/digital-books-new-chapter-reader-privacy.

[8] "More Americans are watching online video each and every month than watch the Super Bowl once a year.." Greg Jarboe, *125.5Million Americans Watched 10.3 Billion YouTube Videos in September*, SEARCHENGINEWATCH.COM, Oct. 31, 2009, http://blog.searchenginewatch.com/091031-110343.

[9] "Location-based services" is an information service utilizing the user's physical location (which may be automatically generated or manually defined by the user) to provide services. Wikipedia, *Location-Based Service*, http://en.wikipedia.org/wiki/Location-based_service (as of January 21, 2011).

[10] Recent location-based service Foursquare built a base of 500,000 users in its first year of operation. Ben Parr, *The Rise of Foursquare in Numbers [STATS]*, MASHABLE, Mar. 12, 2010, http://mashable.com/2010/03/12/foursquare-stats/.

- 69% of Internet users want the legal right to know everything that a Web site knows about them.[11]
- 92% want the right to require websites to delete information about them.[12]

Nor do consumers favor online tracking:

- 67% rejected the idea that advertisers should be able to match ads based on specific websites consumers visit;[13] and
- 61% believed these practices were not justified even if they kept costs down and allowed consumers to visit websites for free.[14]

In sum, while Americans make great use of the internet, they are very concerned about their privacy and specifically troubled by the practice of behavioral targeting.

II. The data collected by behavioral marketers forms a personal profile of unprecedented breadth and depth.

Behavioral targeting contravenes many American's expectation of privacy and how they should be treated online. Online advertising is one of the fastest growing businesses on the internet and it is based on collecting a staggering amount of information about people's online activities. Advertising has always been prevalent online, but instead of targeting websites – such as advertising shoes on a shoe store site - advertisers now use personal information to target individuals directly.

They do this using different surveillance tools. The simplest tools are cookies. A cookie is a file that a website can put on a user's computer when the user visits it so that when the user returns, or visits another affiliated site, it remembers certain information about the user. Cookies were initially used to help websites remember user passwords or contents in shopping bags, but as online marketing grew more sophisticated, cookies did too. Advertisers and aggregators modified cookies to track people's web page visits, searches, online purchases, videos watched, posts on social networking, and so on. Another popular and even more invasive tool for tracking is the flash cookie. Flash cookies are often used by data aggregators to re-install a regular cookie that a user had detected and deleted. The newest and most aggressive form of tracking is the beacon. Beacons, also known as web bugs, are often used by sites that hire third party services to monitor user actions. These devices can track a user's movements extremely closely; to the point that they can monitor keystrokes on a page or movements by a user's mouse. The result of these practices is the collection and sale of a wealth of consumer data without any legal limits or protections for individuals.

---

[11] Joseph Turow, et al., *Americans Reject Tailored Advertising* 4 (2009), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.
[12] *Id.*
[13] Lymari Morale, *U.S. Internet Users Ready to Limit Online Tracking for Ads*, USA TODAY, December 21, 2010
[14] *Id.*

As targeted ads become increasingly profitable, behavioral marketers are growing more ambitious and seeking to form an even more complete picture of unsuspecting citizens. The *Wall Street Journal* recently conducted a comprehensive study on the effects of online marketing on individual privacy and the results were alarming. The study found that the nation's 50 top websites installed an average of 64 pieces of tracking technology on user's computers, usually with no warning. A dozen sites installed over a hundred. For example, the study found that Microsoft Corp.'s popular website, MSN.com, attached a tracking device that identified and stored user's detailed personal information. According to the tracking company that created the file, it could predict a user's age, ZIP code and gender, as well as an estimate of a user's income, marital status, family status and home ownership status.[15] These new technologies allow marketers to combine a vast amount of information gleaned from different web sites over time in order to paint an extremely detailed profile of potential consumers. Any particular website may have little information and this may not alarm some, but when a large number of these data points are aggregated, an extremely detailed picture results.

In addition, the *Wall Street Journal* found that tracking technology has become so advanced and covert that the website owner is often not even aware of its presence. Microsoft, one of the largest developers of computer software in the world, said it did not know about the tracking devices on its site until informed by the *Journal.*[16] If these technologies have become as surreptitious as to slip past sophisticated website owners, it is completely unreasonable to believe that the average user would be able to avoid their spying.

III. Merger of online and offline identity

The collection of this online information is frequently matched with real-world, offline identities. In 2009, Professor Edward W. Felten testified before the House Subcommittee on Communications, Technology and the Internet about the process by which an online ad service might combine its user profile with information purchased from a commercial database: "If the ad service does know the identity, then third party services can provide a wealth of additional information, such as the user's demographics, family information, and credit history, which can be incorporated into the ad service's profile of the user, to improve ad targeting."[17] While Professor Felten was careful to make clear that "the fact that something is possible as a technical

[15] Angin Win, *The Web's New Gold Mine: Your Secrets*, The Wall Street Journal, July 30, 2010
[16] *Id.*
[17] *Behavioral Advertising: Industry Practices and Consumers' Expectations: Hearing before the H. Subcomm. on Communications, Technology and the Internet of the H. Comm. on Energy and Commerce, and the H. Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 111th Cong. (2009) (Statement of Edward W. Felten, Professor of Computer Science and Public Affairs, Princeton University)

matter does not imply that reputable ad services actually do it,"[18] we now know the process is not uncommon.

Online and offline data companies are combining forces to get an even more detailed profile of consumers. For example, Comscore, a leading provider of website analytic tools, boasts that "online behavioral data can…be combined with attitudinal research or linked with offline databases in order to diagnose cross-channel behavior and streamline the media planning process."[19] In another example, the data firm Aperture has made the connection between online and offline identities by collecting data from offline data companies like Experian or Nielsen's Claritas and then combining it with a huge database of email addresses maintained by their parent company, Datran Media[20].

This information allows advertisers to categorize people into demographics important to marketing- such as men earning $40,000 to $50,000 - so when that person visits an automotive website, for example, the advertiser will know whether to highlight a Subaru or a Range Rover.[21] The prevalence of online marketing is growing and according to one online advertising CEO's statement "[m]oving from site-targeting to *people-targeting* is the central dynamic of the industry".[22] (italics added)

IV. Regulation of behavioral targeting does not threaten the "Free Internet"

The ACLU believes the internet is one of the greatest tools ever created for advancing American's First Amendment rights. We would never endorse any regulation that endangered the robustness and variety of this medium. We strongly believe that the creation of a "Do Not Track" mechanism and regulation of data sharing would not harm the internet or free products or services.

Behavioral targeting is different than "contextual advertising," another type of online ad service which shows ads to users based on the contents of the web page they are currently viewing or the web search they have just performed. When this pairing of ads to users' interests is based only on a match between the content of an ad and a single page or search term, a website or advertising network requires no personal information about a user beyond an I.P address. The practice does not raise significant privacy concerns.

---

[18] *Id.*
[19] Why Comscore?, http://comscore.com/About_comScore/Why_comScore (last visited January 21, 2011).
[20] Learmonth Michael, *Holy Grail of Targeting is Fuel for Privacy Battle*, Advertising Age, March 22, 2010
[21] *Id.*
[22] Robert D. Hof, *Ad Networks Are Transforming Online Advertising*, BUSINESS WEEK, Feb. 19, 2009 (quoting Matt Spiegel of Omnicom Media) *available at* http://www.businessweek.com/magazine/content/09_09/b4121048726676.htm (last visited January 21, 2011).

Nor would a "Do Not Track" mechanism necessarily impact the ability of first parties – the initial websites visited by users such as Google and Amazon – to gather information on their users or to employ that information to provide more targeted services or advertisements. A consumer's relationship with a first party is fundamentally different than with a third party like a behavioral targeter. In the case of a first party the consumer already has a relationship with the provider of the service which he or she can terminate. In addition, the consumer has an expectation that when a service is provided, the first party may collect information as part of that service. Contrast this with behavioral targeting, where the collection is often surreptitious and the consumer has no relationship with the company. The distinction between first and third party tracking is not always perfectly clear. For example, we believe that so-called affiliates of first parties (which do not provide a service directly to the consumer) should be treated as third parties and that first parties should not be able to sell or share customer data. Nevertheless, we believe the distinction between first and third parties provides a useful basis for distinguishing between harmful and beneficial tracking.

Finally, content has been supported for years (and in many cases for decades and centuries) through advertising without the need for detailed targeting and tracking of consumers. In fact, studies have demonstrated that the vast majority of the revenue from tracking consumers goes not to content providers but rather to the behavioral targeters themselves. Industry sources say that 80% of the revenue from targeting – 4 in 5 dollars – went to create and enhance the targeting system, not to publishers.[23] Major publishers like the New York Times have endorsed a "Do Not Track" mechanism – clearly they are not concerned that such a mechanism will harm their ad revenue.[24]

V. Governmental access to extensive personal profiles threatens the First and Fourth Amendment

It is no exaggeration to say that data profiles—which may combine records of a person's entire online activity and extensive databases of real-word, personally identifiable information—draw a personal portrait unprecedented in scope and detail. Because the internet has become intertwined with so many personal facets of our lives, the same technology that has provided such tremendous advances also creates the possibility of tremendous intrusion, and not just by companies, but also by the government.

As their contracts with the data aggregator industry demonstrate, government and law enforcement agencies have found these personal data profiles irresistible. In 2006 the *Washington Post* reported that the federal government and states across the country have

[23] The Jordan Edmiston Group, *M&A Overview and Outlook*, Slide 13, can be found at: http://www.jegi.com/files/docs/IABMIXX.pdf

[24] *Protecting Online Privacy*, New York Times Editorial, December 4, 2010

developed relationships with private companies that collect personal information about millions of Americans, including unlisted cell phone numbers, insurance claims, driver's license photographs and credit reports through private data aggregators including Accurint, Entersect and LexisNexis. In fact Entersect boasts that it is "the silent partner to municipal, county, state, and federal justice agencies who access our databases every day to locate subjects, develop background information, secure information from a cellular or unlisted number, and much more."[25]

The Central Intelligence Agency (CIA), via its investment arm In-Q-Tel, has invested in a software company that specializes in monitoring blogs and social networks[26] and the Department of Defense, the CIA, and the Federal Bureau of Investigation (FBI) have all purchased use of private databases from Choicepoint, one of the largest and most sophisticated aggregators of personal data[27]. In the words of the FBI, "We have the legal authority to collect certain types of information" because ChoicePoint is "a commercial database, and we purchase a lot of different commercial databases….They have collated information that we legitimately have the authority to obtain."[28]

The government has demonstrated an increasing interest in online user data in other ways as well. In 2006 the Department of Justice (DOJ) subpoenaed search records from Google, Yahoo!, and other search providers in order to defend a lawsuit.[29] In 2007, Verizon reported receiving 90,000 requests per year and in 2009, Facebook told *Newsweek* it was getting 10 to 20 requests each day. In response to increasing privacy concerns, Google started to publish the number of times law enforcement asked for its customers' information and reported over 4,200 such requests in the first half of 2010 alone. In the words of Chris Hoofnagle, a senior fellow at the Berkeley Center for Law and Technology, "These very large databases of transactional information become honey pots for law enforcement or for litigants."[30] Given the government's demonstrated drive to access both online data and commercial databases of personal information, it seems nearly certain that law enforcement and other government actors will purchase or

---

[25] O'Harrow Jr Robert, *Centers Tap into Personal Databases*, WASHINGTON POST, April 2, 2008
[26] Noah Shactman, *U.S. Spies Buy Stake in Firm That Monitors Blogs, Tweets*, WIRED, Oct. 19, 2009 *at* http://www.wired.com/dangerroom/2009/10/exclusive-us-spies-buy-stake-in-twitter-blog-monitoring-firm (last visited January 21, 2011).
[27] Shane Harris, *FBI, Pentagon Pay For Access to Trove of Public Records*, NAT'L J., Nov. 11, 2005, *available at* http://www.govexec.com/story_page.cfm?articleid=32802 (last visited January 21); Robert O'Harrow Jr., *In Age of Security, Firm Mines Wealth Of Personal Data*, WASHINGTON POST at A01, Jan. 20, 2005, *available at* http://www.washingtonpost.com/wp-dyn/articles/A22269-2005Jan19.html (last visited January 21, 2011).
[28] Harris, supra n. 16 (quoting F.B.I. spokesman Ed Cogswell)
[29] Hiawatha Bray, *Google Subpoena Roils the Web, US Effort Raises Privacy Issues*, BOSTON GLOBE, January 21, 2006, *available at* http://www.boston.com/news/nation/articles/2006/01/21/google_subpoena_roils_the_web/ (last visited January 21, 2011).
[30] Miguel Helft, *Google Told to Turn Over User Data of YouTube*, NEW YORK TIMES, July 4, 2008 *available at* http://www.nytimes.com/2008/07/04/technology/04youtube.html (last visited January 21, 2011).

otherwise access the type of detailed profiles of online behavior compiled by behavioral marketers.

Our First Amendment rights to freedom of religion, speech, press, petition, and assembly are based on the premise that open and unrestrained public debate empowers democracy by enriching the marketplace with new ideas and enabling political and social change through lawful means. The Fourth Amendment shields private conduct from unwarranted government scrutiny. Together the exercise of these rights online has allowed the internet marketplace of ideas to expand exponentially.

Courts have uniformly recognized that government requests for records of which books, films, or other expressive materials individuals have received implicate the First Amendment and trigger exacting scrutiny.[31] These cases are grounded in the principle that the First Amendment protects not only the right of individuals to speak and to express information and ideas, but also the corollary right to receive information and ideas through books, films, and other expressive materials.[32] Within this protected setting, privacy and anonymity are vitally important. Anonymity "exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular," because, among other things, it serves as a "shield from the tyranny of the majority."[33] An individual may desire anonymity when engaging in First Amendment activities—like reading, speaking, or associating with certain groups—because of "fear of economic or official retaliation, . . . concern about social ostracism, or merely . . . a desire to preserve as much of one's privacy as possible."[34]

The Supreme Court has also recognized that anonymity and privacy are essential to preserve the freedom to receive information and ideas through books, films, and other materials of one's choosing. For example, in *Lamont v. Postmaster General* the Court invalidated a postal regulation that required the recipient of "communist political propaganda" to file a written request with the postmaster before such materials could be delivered.[35] The regulation violated the First Amendment because it was "almost certain to have a deterrent effect": "Any addressee [was] likely to feel some inhibition" in sending for literature knowing that government officials were scrutinizing its content.[36] Forced disclosure of reading habits, the Court concluded, "is at

---

[31] *In re Grand Jury Subpoena to Kramerbooks & Afterwords Inc.*, 26 Med. L. Rptr. 1599, 1600-01 (D.D.C. 1998) (Dkt. No. 21, Ex. B) (requiring government to show compelling interest and a sufficient connection between its investigation and its request for titles of books purchased by Monica Lewinsky); *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044, 1053 (Colo. 2002) (holding that search of bookseller's customer purchase records necessarily intrudes into constitutionally protected areas)

[32] *See, e.g.*, *Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council*, 425 U.S. 748, 757 (1976) (right to receive advertisements); *Stanley v. Georgia*, 394 U.S. 557, 564 (1969) (films); *Bantam Books v. Sullivan*, 372 U.S. 58, 64 n.6 (1963) (books).

[33] *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 357 (1995).

[34] *Id.* at 341-42.

[35] *Lamont v. Postmaster General*, 381 U.S. 301, 302 (1965).

[36] *Id.* at 307.

war with the 'uninhibited, robust, and wide-open' debate and discussion that are contemplated by the First Amendment."[37]

These words ring equally true today in the Information Age, with the prevalence of the internet and other new technologies. Although these technological advances provide valuable tools for creating and disseminating information the unprecedented potential for government and companies to store vast amounts of personal information for an indefinite time poses a new threat to the right to personal privacy and free speech. For example, in *In re Grand Jury Subpoena to Amazon.com*, the district court recognized this reality in holding that a grand jury subpoena to Amazon requesting the identities of buyers of a certain seller's books raised significant First Amendment concerns.[38] The court explained its concern over the chilling effect that would flow from enforcing such a subpoena in the age of the internet, despite its confidence in the government's good-faith motives:

> [I]f word were to spread over the Net—and it would—that [the government] had demanded and received Amazon's list of customers and their personal purchases, the chilling effect on expressive e-commerce would frost keyboards across America. Fiery rhetoric quickly would follow and the nuances of the subpoena (as actually written and served) would be lost as the cyberdebate roiled itself to a furious boil. One might ask whether this court should concern itself with blogger outrage disproportionate to the government's actual demand of Amazon. The logical answer is yes, it should: well-founded or not, rumors of an Orwellian federal criminal investigation into the reading habits of Amazon's customers could frighten countless potential customers into canceling planned online book purchases, now and perhaps forever. . . . Amazon . . . has a legitimate concern that honoring the instant subpoena would chill online purchases by Amazon customers.
> *In re Grand Jury Subpoena to Amazon.com*, 246 F.R.D. at 573.

The internet is, and must remain, the most open marketplace of ideas in the history of the world. In order to guarantee this we must provide consumers with a simple and meaningful mechanism for assuring their privacy and protecting the robust protections established by the Constitution.

VI. Electronic Communications Privacy Act

[37] *Id.* (quoting *New York Times Co. v. Sullivan*, 376 U.S. 254, 270 (1964)).
[38] 246 F.R.D. at 572-73

The ACLU applauds the Department of Commerce for recognizing the need to update ECPA, the law which governs law enforcement and government access to electronic communications. We reiterate our support for the changes we described in our June 11, 2010 comments to Docket No. 100402174-0175-01, *Information Privacy and Innovation in the Internet Economy*.

Without reiterating those comments in full we note that ECPA has not been substantially updated since 1986 – before the advent of the World Wide Web. We believe the following measures are critical to that update.

1. **Robustly Protect All Personal Electronic Information.** Our personal and private information – whether documents and correspondence, or records of what we search and read online – reveals a tremendous amount about us. The disclosure of any of this information to the government without a warrant based on probable cause and without notice violates our rights to privacy, and also implicates our right to free speech, and free association. Current loopholes in our privacy laws need to be closed to protect electronic information without regard to its age, whether it is "content" or "transactional" in nature, or whether an online service provider has access to it to deliver services.

2. **Safeguard Location Information.** As of June 2009, there were an estimated total of 277 million cell phone service subscribers in the United States – about 90% of the overall population.[39]. The location information transmitted by these phones every minute of every day reveals not only where people go, but often what they are doing and who they are talking to. Location information, whether it is ongoing tracking or records of previous location, is clearly personal information. The law should require government officials to obtain a warrant based on probable cause before allowing access.

3. **Institute Appropriate Oversight and Reporting Requirements**. Because electronic record keeping enables easy collection and aggregation of records, current low standards under ECPA allow the government to engage in a largely unsupervised and unreported "shopping spree" through the treasure trove of personal information held by private companies. To ensure adequate oversight by Congress and adequate transparency to the public, existing reporting requirements for wiretap orders must be extended to all types of law enforcement surveillance requests.

4. **Require a Suppression Remedy**. If a law enforcement official obtains non-electronic information illegally, that information usually can't be used in a court of law. The same rule, however, doesn't apply to illegally-obtained electronic information. Such a rule only encourages government overreaching and must be changed to require a judge to bar the use of such unlawfully obtained information in court proceedings.

---

[39] As of June 2009, there were an estimated 276,610,580 wireless phone subscribers in the United States. *See* CTIA The Wireless Association, *CTIA's Semi-Annual Wireless Industry Survey* (2009) at 5, *available at* http://files.ctia.org/pdf/CTIA_Survey_Midyear_2009_Graphics.pdf (last viewed Nov. 14, 2009). The Central Intelligence Agency estimates that the United States population in July 2009 was 307,212,123. *See* Central Intelligence Agency, The World Factbook: United States, https://www.cia.gov/library/publications/the-world-factbook/geos/us.html (last viewed Nov. 18, 2009).

5. **Craft Reasonable Exceptions.** Overbroad exceptions are also depriving Americans of their rightful privacy protection. Currently ECPA sometimes allows access to the content of communications without a true emergency, without informed consent and without prompt notice to the subject. ECPA must be amended on each of these fronts if electronic records are to receive the protections Americans need.

Since 1986, technology has advanced at breakneck speed while electronic privacy law remained at a standstill. The American people have received a great inheritance from our Founders and past generations, and we cannot let those rights slip away just because people communicate with each other using a newer form of technology. Privacy law doesn't auto-update. It's time for Congress to modernize ECPA.

VII. Conclusion

For years government agencies have called on industry to provide privacy protections for consumers however, as the FTC report explains self regulatory efforts "have been too slow, and up to now have failed to provide adequate and meaningful protection."[40] Though industry has taken some steps there is still neither a widespread basis for implementing choice mechanisms nor any legally enforceable basis for relying on them. This lack of competition means that only a clear and easy to use "Do Not Track" option offers Americans real control over their personal information.

Americans want and need legal protections for privacy that reflect the technology they use every day. The time has come for a "Do Not Track" option coupled with limitations on sharing personal information in order to protect our privacy in a 21st century digital world.

The internet is the greatest tool we have seen to practice our First Amendment rights as we communicate, learn and express ourselves on a global scale. If Americans begin to feel that their actions online are being monitored by law enforcement their movements will undoubtedly be influenced and the internet will no longer be the open and innovative medium that has allowed it to thrive. A straightforward "Do Not Track" option along with limitation on the sharing of personal information must be made available to individuals in order to protect our First Amendment rights, maintain our right to privacy and support the growth of the internet.