SHARING YOU WITH YOU: INFORMATIONAL PRIVACY, GOOGLE, & THE LIMITS OF USE LIMITATION

*Kevin P. McLaughlin**

TABLE OF CONTENTS

Modern technology, as embodied by Google, increasingly utilizes user data to personalize and improve services.[1] This re-use of data sometimes occurs in unforeseen ways, yet creates substantial benefit for the user and, at times, for society at large.[2] This re-use of data also runs afoul of the traditional view of use limitation, which posits that personal information should only be used for the specific purposes for which it was collected.[3]

*B.A., U.C. San Diego, 1998; J.D., U.C. Hastings College of the Law, 2007.

[1] Pablo L. Chavez, *Comments of Google Inc. Re: Preliminary Staff Report on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"*, GOOGLE INC., 4 (Feb. 18, 2011), http://www.ftc.gov/os/comments/privacyreportframework/00417-58065.pdf [hereinafter Chavez Letter].

[2] *Id.*

[3] *See* FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS, FTC REPORT 33, 40 (2012) [hereinafter FTC PRIVACY REPORT], *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf (explaining that consumers are unaware that the data they share runs the risk of being used beyond the purpose for which they provided the information).

Technology is forcing society to define the parameters of privacy. Use limitation must be defined to allow for personalization and other positive re-uses of data while ensuring that users are not harmed by re-use of their data.[4] Recent efforts by the Federal Trade Commission (FTC) and others recalibrate use limitation in an effort to strike that balance.[5] Viewed through the lens of Google's privacy practices, this refined use limitation principle allows personalization and development but retains substantial privacy protection for users.[6]

I. PROTECTING YOU FROM YOU: PRIVACY AS CONTROL IN CONTEXT.

Privacy used to be a black-and-white matter. Your information was private if you kept it to yourself, and it was not private if you provided it to others.[7] This is particularly apparent in Fourth Amendment jurisprudence, where the Supreme Court has sought to provide bright-line rules for law enforcement.[8] Tort law treatment of privacy, while inherently tied to conceptions of

[4] *Id.* at 7–8 (discussing the need to balance privacy protections against the benefits of innovative technologies).

[5] *See, e.g.*, Edward Wyatt, *F.T.C. and the White House Push for Online Privacy Laws*, N.Y. TIMES, May 9, 2012, at B8 (calling for increased oversight "allow consumers to see and correct the information" that companies gather).

[6] *See* Chavez Letter, *supra* note 1, at 1–2 (stating the benefits of Google's privacy policy to both protection of private information and benefit to consumers).

[7] As noted by Professor Daniel Solove, legal notions of privacy developed not in an era of databases and concerns of informational privacy, but in an era where surveillance and "invasions into one's hidden world" were the primary concerns to be addressed. Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1431 (2001). This has led to an emphasis on secrecy and a view that, where information is not kept secret, it is not private. Informational privacy, however, "concerns the uses and practices associated with our information, not merely whether that information remains completely secret." *Id.* at 1439; *see also* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1177 (2002) (noting that the law often treats privacy in a black-and-white manner, either "wholly private or wholly public").

[8] *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."); *see also* United States v. Miller, 425 U.S. 435, 443 (1976) ("This Court has held repeatedly that the 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.").

reasonableness, has also proceeded by categorization of interests into different sorts of invasions of secrecy.[9] This binary approach is also apparent in sectoral privacy legislation, whereby certain categories of information, such as health, credit, and financial data[10] are given strong privacy protections, while most other information is left relatively unprotected.[11] This secret-or-not approach was also prevalent, until quite recently, in the law on waiver of privileges: disclosure of an attorney-client communication, for example, to any third party worked a waiver of the privilege.[12]

Privacy has moved from black-and-white to "shades of grey."[13] Modern privacy is not dependent upon secrecy; it is not the fact of disclosure that matters, but the context of the disclosure.[14] For nearly 50 years, privacy vis-à-vis law enforcement has struggled to be defined by citizens' reasonable expectations of

---

[9] William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 407 (1960). In Dean Prosser's seminal article, the "law of privacy comprises four distinct kinds of invasion of four different interests of the plaintiff .†.†. ." *Id.* at 389. Central to the first two torts is some invasion of that which the plaintiff considered secret. *Id.* at 407.

[10] *See* Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104–191, § 264(a)–(b), 110 Stat. 1936, 2033 (1996) (codified as amended at 42 U.S.C.A. § 1320d–2) (discussing privacy of health information); *see also* Fair Credit Reporting Act (FCRA), 15 U.S.C.A. § 1681(b) (2006) (discussing privacy of credit information); Financial Services Modernization Act (Gramm-Leach-Bliley), Pub. L. No. 106–102, § 501(a), 113 Stat. 1338, 1436 (1999) (codified as amended at 15 U.S.C.A. § 6801) (discussing privacy of financial information). Many other categories of private information are protected by specific federal and state legislation, *see Existing Federal Privacy Laws*, CTR. FOR DEMOCRACY & TECH, https://www.cdt.org/privacy/guide/protect/laws.php (last visited Oct. 2, 2012) (categorizing current federal privacy laws); Jeffery M. Shaman, *The Right of Privacy in State Constitutional Law*, 37 RUTGERS L.J. 971, 1085 (2006) (discussing different specific privacy rights under state law).

[11] *See* Individual Reference Serv. Grp., Inc. v. F.T.C., 145 F. Supp. 2d 6, 36 (D. D.C. 2001).

[12] The common law rule of waiver is set forth in Parkhurst v. Lowten, (1819) 36 Eng. Rep. 589, 596 (stating that when "the moment [of] confidence ceases, privilege ceases"). Evidentiary rules now allow the holder of the privilege to "claw back" any privileged document that is inadvertently disclosed, where the holder of the privilege took reasonable steps to prevent the disclosure and prompt steps to correct the error. FED. R. EVID. 502(b).

[13] Daniel J. Gervais & Daniel J. Hyndman, *Cloud Control: Copyright, Global Memes and Privacy*, 10 J. TELECOMM. & HIGH TECH. L. 53, 77 (2012) ("the binary approach [to privacy] is now a range of possibilities").

[14] *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 235–36 (2010) (setting forth a "framework of contextual integrity" for private disclosures).

privacy.[15] The Supreme Court has found constitutional privacy interests in other contexts: in zones, penumbras and emanations,[16] First Amendment corollaries,[17] and other conceptions of liberty[18] – hardly the stuff of bright-line rules. Sectoral legislation, while putting information in "protected" or "unprotected" categories, also recognizes that certain information is more private than other information, and should be protected even when disclosed to other parties.[19] As society moves from privacy by obscurity to privacy by design,[20] we are forced to confront our expectations of privacy, assess their reasonableness, and to identify the different contexts in which these expectations arise.

This call for privacy by design has been brought about by the rise of information technology.[21] From widespread public video

[15] *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (creating the reasonable expectation of privacy test regarding Fourth Amendment jurisprudence), *superseded by statute on other grounds*, Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C.A. §§ 2510–2520 (Supp. 2009). That is to say, in some instances reasonable expectations of privacy guide Fourth Amendment jurisprudence, which remains tethered, in many ways, to historical property rights and conceptions of secrecy. *See also* United States v. Jones, 132 S. Ct. 945, 949 (2012) (physically occupying private property in order to obtain information is deemed a "search" under the Fourth Amendment); Guest v. Leis, 255 F.3d 325, 335–36 (6th Cir. 2001) (finding no reasonable expectation of privacy in computer users' names, addresses, birthdates, and passwords, because they are communicated to third-party systems operators).

[16] *See* Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (discussing specific guarantees granted by the Fourth Amendment of the Constitution).

[17] "The essential thrust of the First Amendment is to prohibit improper restraints on the voluntary public expression of ideas; it shields the man who wants to speak or publish when others wish him to be quiet. There is necessarily, and within suitably defined areas, a concomitant freedom not to speak publicly, one which serves the same ultimate end as freedom of speech in its affirmative aspect." Harper & Row, Publishers, Inc., v. Nation Enters., 471 U.S. 539, 559 (1985) (quoting Estate of Hemingway v. Random House, Inc., 23 N.Y.2d 341, 348 (1968)).

[18] *See* Roe v. Wade, 410 U.S. 113, 152 (1973) (tying the right of privacy to the concept of personal liberty); Lawrence v. Texas, 539 U.S. 558, 578–79 (2003) (describing privacy as a component of liberty).

[19] *See* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy: (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, 28 (2001) (noting that American privacy law has evolved on a sector-specific basis, unlike the comprehensive privacy regimes of Europe).

[20] Peter Fleischer, *Altered Identities: The Internet and Genetic Engineering*, Address at the 13th Annual Harvard Journal of Law & Technology Symposium (Mar. 14, 2008), http://www.youtube.com/watch?v=JNu1OtkWrOY.

[21] *See* Kashmir Hill, *Why 'Privacy By Design' Is The New Corporate Hotness*,

surveillance to the intimacies of Internet use in the comfort of our living rooms, huge amounts of data about ourselves, often existing indefinitely, is held in the hands of others.[22] The Internet, in its initial forms, was not designed with privacy in mind – quite the opposite, for it has been about sharing, connecting, and access to information.[23] While widespread, accessible information about ourselves and others is empowering, it also creates feelings of vulnerability and paranoia.[24]

These feelings of vulnerability and concern are particularly acute where new technologies redefine our expectations.[25] There are undoubted benefits to being able to reconnect with former classmates or survey dating prospects with a few clicks of a mouse, or even to receiving routine updates on what a "friend" is having for breakfast.[26] But each of these interactions compromises some part of the user's privacy – as have all interactions since the dawn of time. Sometimes it does so purposefully, such as broadcasting your banana pancakes to

FORBES (July 28, 2011, 1:23 PM), http://www.forbes.com/sites/kashmirhill/2011/07/28/why-privacy-by-design-is-the-new-corporate-hotness (noting that "privacy by design" first appeared in proposed U.S. federal legislation in 2011 in the Commercial Privacy Bill of Rights).

[22] *See id.* (providing examples of third parties who have control over personal information).

[23] *See id.* (giving an example of social networking).

[24] The architecture of the Internet has been referred to not only as a potential architecture of control, as described by Professor Lawrence Lessig, but also an architecture of vulnerability, where people are vulnerable to significant harm and helpless to do anything about it. *See* LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD 15 (2001) (asserting that "changes in the architecture of the internet" are "[f]ueled by a bias in favor of control"); DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 149 (Jack M. Balkin & Beth Simone Noveck eds., 2004) (describing the realization that "individuals are no longer able to exercise control over their information" as "a deepening sense that one is at the mercy of others").

[25] *See* ELLEN ALDERMAN & CAROLINE KENNEDY, THE RIGHT TO PRIVACY 323 (1995) ("Whether computers will alter our notion of the human condition is in dispute, but what is inarguable is that we will have to change the way we think about keeping certain information private.").

[26] Sharing in new ways certainly carries benefits. "Indeed our culture would be healthier and happier if we diminished substantially the kinds of actions that we now feel comfortable doing only in private, or the kind of thoughts we now feel comfortable disclosing only to those with whom we have special relationships." Richard A. Wasserstrom, *Privacy: Some Arguments and Assumptions*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 317, 331 (Ferdinand D. Schoeman ed., 1984).

thousands of people you know. Each of these interactions, built upon the transmission of data between computers, also compromises the user's privacy in more subtle ways, for each interaction is necessarily recorded.[27] Use of these technologies shakes up our expectations of privacy, both where sharing and interacting is the purpose of the interaction,[28] and where the sharing is of an unconscious sort.[29]

Privacy is tied to the context of the interaction.[30] That context is in many ways synonymous with a reasonable expectation of privacy.[31] What sort of privacy an individual should expect is directly influenced by the context of the interaction.[32] Context, however, represents a shift to a standard that can be applied more concretely to specific situations, rather than a generic standard prone to shifting (or shrinking) as each new privacy-altering technology emerges.[33]

Data about each of us, held by persons and entities other than

---

[27] *See* SOLOVE, *supra* note 24, at 142 (discussing the transparency of personal information and the variety of information that is recorded).

[28] JEFF JARVIS, PUBLIC PARTS 2 (2011). The emergence of new tools for sharing is heralded by some as creating "profound change" – an "age of publicness." *Id.* Others have gone so far as to declare that "privacy is no longer a 'social norm.'" *Facebook's Zuckerberg Says Privacy No Longer A 'Social Norm,'* HUFFINGTON POST (Mar. 18, 2010, 6:12 AM), http://www.huffingtonpost.com/2010/01/11/facebooks-zuckerberg-the_n_417969.html.

[29] *Consumer Reports Poll: Americans Extremely Concerned About Internet Privacy*, CONSUMERSUNION (Sept. 25, 2008), http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html ("Consumers are aware that information about their surfing habits is being collected online, but many are not aware of what companies are able to do with their information.").

[30] *See* NISSENBAUM, *supra* note 14, at 233 (explaining that privacy expectations are tied to "context-relative informational norms").

[31] *See id.* at 233–36 (noting the similarities between reasonable expectations of privacy and a context of privacy, and arguing that a framework of contextual integrity can help courts identify relevant social norms of privacy).

[32] *See id.* at 233 (discussing how the judicial system will examine one's expectation of privacy "in relation to a certain activity or practice" in order to determine its reasonableness).

[33] *See* FTC PRIVACY REPORT, *supra* note 3, at 38. The FTC acknowledges this distinction in its new Privacy Framework by recognizing that certain re-uses of consumer data do not require consumer choice. The Commission

> "refine[d]" its principles regarding re-use to "focus on the *context of the interaction* between a business and the consumer. This new 'context of the interaction' standard is similar to the concept suggested by some commenters that the need for choice should depend on reasonable consumer expectations, but is intended to provide businesses with more concrete guidance." *Id.*

us, is proliferating.[34] We understand where and how some of this information is managed, and we do not understand where and how some of this information is managed.[35] That uncertainty is unsettling.[36] The core of informational privacy, in a world awash in data, has become control over that data.[37] Privacy as control over one's information is not a new formulation,[38] but it has increasingly become the focus of informational privacy regulation.[39]

Control of your information means, obviously, limiting uncontrolled uses of your information – protecting you from undesirable uses of information about you.[40] It is the ability to

---

[34] *See Consumer Reports Poll: Americans Extremely Concerned About Internet Privacy*, *supra* note 29 (explaining "how often" personal data is taken and distributed by internet companies).

[35] Polls repeatedly depict a populace often mistaken or unaware about how their personal information is used, and deeply concerned about their privacy. *Id. See also* Press Release, USC Dornsife/L.A. Times, *Voters Across the Political Spectrum Concerned About Tech Companies Invading Their Privacy* (Mar. 31, 2012), http://dornsife.usc.edu/usc-lat-poll-privacy-march-2012.

[36] *See* Bartnicki v. Vopper, 532 U.S. 514, 541 (2001) (Rehnquist, C.J., dissenting) ("We are placed in the uncomfortable position of not knowing who might have access to our personal and business e-mails, our medical and financial records, or our cordless and cellular telephone conversations.").

[37] *See* Letter from Michael Richter, Chief Privacy Counsel, Facebook, Inc. to FTC 4 (Feb. 18, 2012), *available at* http://www.ftc.gov/os/comments/privacyreportframework/00413-58069.pdf [hereinafter Richter Letter] (Though "Justice Brandeis may have famously defined privacy as 'the right to be let alone' .†.†. [a] better conception of privacy in the coming age is control over the 'digital me.'" (quoting Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting))).

[38] *See* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1463 (2000) (treating "informational privacy" as "the ability to control the acquisition or release of information about oneself"); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1203 (1998) ("information privacy concerns an individual's control over the processing – i.e., the acquisition, disclosure, and use – of personal information"); Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1109–15 (2002) (chronicling numerous arguments, including those of Charles Fried, Alan Westin, Arthur Miller and others, that privacy is fundamentally about control over information, and noting the difficulties in defining the scope of this conception of privacy).

[39] *See* Tanzina Vega, *For Online Privacy, Click Here*, N.Y. TIMES, Jan. 20, 2012, at B3, *available at* http://www.nytimes.com/2012/01/20/business/media/the-push-for-online-privacy-advertising.html (explaining legislators' introduction of bills pertaining to privacy and control as well a potential statement from the White House).

[40] *See* U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989) (noting that "both the common law and the literal understandings of privacy encompass the individual's control of information

keep you (in the form of information about you) from hurting you, through being blindsided by an unexpected use of your information (such as by law enforcement, business competitors, or even family members), discriminated against,[41] or manipulated by marketers and others who know all too much about you.[42] This notion of protecting information about you from causing you harm is the main thrust behind core notions of privacy embodied in the Fourth[43] and Fifth[44] Amendments, as well as sectoral legislation[45] and privacy torts.[46] While control

concerning his or her person"). For example, the Freedom of Information Act provides an exemption allowing for the right to limit dissemination of an individual's rap sheet. *Id.* at 763–65.

[41] While injuries through governmental misuse of private information or profiling by marketers are the most commonly discussed forms of harm, discrimination based on online profiling presents a very real form of harm. *See* LAWRENCE LESSIG, CODE: VERSION 2.0, 219–22 (2006) (explaining how companies can use information to profile people and discriminate against them based on their social or economic status); LORI ANDREWS, SOCIAL NETWORKS AND THE DEATH OF PRIVACY: I KNOW WHO YOU ARE AND I SAW WHAT YOU DID 47 (2011) (discussing problems of "weblining," and how unintentional negative information about someone can be used to their detriment).

[42] *See* LESSIG, *supra* note 41, at 204 (explaining how search engines keep copies of all search requests, linking the information to IP addresses and sometimes to user accounts); *id.* at 220 (noting that while television advertisements may not effectively control a person's desires, the use of an individual's data for marketing purposes, where "options just seem to appear right when you happen to want them," is more manipulative).

[43] The prohibition on unreasonable searches and seizures of one's person, house, papers, and effects is patently concerned with the use of one's information against oneself. *See* Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 807 (2005) (noting that the Fourth Amendment is "meant to protect 'reasonable expectations of privacy'").

[44] The privacy protections of the Fifth Amendment aren't what they once were. *See id.* at 809–10 ("The fact that the Court's early Fifth Amendment decisions were focused on protection of privacy suggests that, had the Court of one hundred years ago known its Fifth Amendment jurisprudence would be jettisoned, its Fourth Amendment jurisprudence might have been much more protective of documentary evidence that is personal in nature."). *See also* Fisher v. United States, 425 U.S. 391, 401 (1976) ("We adhere to the view that the Fifth Amendment protects against 'compelled self-incrimination, not the disclosure of private information.†.†. .'") (quoting United States v. Nobles, 422 U.S. 225, 233 n.7 (1975)). Nonetheless, the right against self-incrimination – and *Miranda's* warning that anything you say may be used against you – embodies a central aspect of privacy: control over certain personal information from being used against you. Robert S. Gerstein, *Privacy and Self-Incrimination*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY 245, 247 (Ferdinand D. Schoeman ed., 1984) (arguing that the primary purpose of the Fifth Amendment is to protect one's privacy).

[45] Sectoral legislation focuses on protecting private information from becoming public and thereby causing harm. *See supra* note 10 and

does not perfectly describe all notions of privacy,[47] it is the cornerstone of modern informational privacy.[48]

II. SHARING YOU WITH YOU.

Google wants to share you with you.[49] Where, depending on the definition, Web 2.0 was about collaboration, such as Wikipedia, social networking, exemplified by Facebook, and facilitating one-to-many communications, such as blogging and Tweeting,[50] the Internet today is becoming a world of information that is personalized.[51] This involves collaboration and networking not simply between people, but between information – your information.[52] While Google is hardly the only entity pursuing

accompanying text; Prosser, *supra* note 9, at 408–09 (discussing an individual's privacy rights, generally). As another example, the Privacy Act was enacted in 1974 to circumscribe disclosure of government records about an individual without the individual's consent. 5 U.S.C.A. § 552a(b) (West, Westlaw through P.L. 112–142 approved 7/9/12).

[46] Rotenberg, *supra* note 19, at 26 (discussing the various statutes designed to address issues of sectoral legislation).

[47] The importance of context is made clear by the recognition that control is irrelevant to privacy interests in certain situations. James H. Moor, *The Ethics of Privacy Protection*, 39 LIBR. TRENDS 69, 75 (1990) ("Although control of information is clearly an aspect of privacy, these definitions emphasizing control are inadequate for there are many situations in which people have no control over the exchange of personal information about themselves but in which there is no loss of privacy.").

[48] It is also central to new notions of privacy: control of one's self is the core of the evolving "right to be forgotten." *See* Karen Eltis, *Breaking Through the "Tower of Babel": A "Right to be Forgotten" and How Trans-Systemic Thinking Can Help Re-Conceptualize Privacy Harm in the Age of Analytics*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 69, 81–91 (2011) (characterizing the right to be forgotten as a "faddish" proposal, but noting that it reflects a conception of privacy as "power to control a measure of one's identity").

[49] *See* Caroline Daniel & Maija Palmer, *Google's Goal: to Organize Your Daily Life*, FIN. TIMES (May 22, 2007, 9:08 PM), http://www.ft.com/cms/s/2/c3e49548-088e-11dc-b11e-000b5df10621.html#axzz1sWxYfp8w (discussing Google services, such as personalized search options and "Google Recommendations," where a user's preferences play a key role).

[50] *See* Lev Grossman, *You – Yes, You – Are TIME's Person of the Year*, TIME (Dec. 25, 2006), http://www.time.com/time/magazine/article/0,9171,1570810,00.html (characterizing Web 2.0 as "a tool for bringing together the small contributions of millions of people and making them matter").

[51] Sramana Mitra, *Connecting You With Your Intimate Bot*, FORBES (Jan. 4, 2008, 6:00 AM), http://www.forbes.com/2008/01/03/semantic-web-facebook-tech-intel-cx_sm_1204web3.html (discussing how "Web 3.0" will offer a personalized experience for the user).

[52] The Semantic Web envisioned by Tim Berners-Lee is based upon

personalization, it is uniquely positioned because of the amount of information it possesses about its users.[53]

Google is focused on organizing the world's information,[54] and increasingly this means organizing the world's information in a user-centric way.[55] Google has long made public its desire to know as much about you as possible, and to even help you answer some of the most fundamental questions in your life.[56] It has increasingly ramped up its personalized or "omnivorous" search,[57] which, for signed-in Google+ users, is no longer simply about tailoring results to your location, your language, or your recent search and web surfing activity.[58] Search results now include relevant posts from members of your Circles and your

interoperability of programs and data. "We're not that far from the time when you can click on the web page for the meeting, and your computer, knowing that it is indeed a form of appointment, will pick up all the right information, and understand it enough to send it to all the right applications." James Hendler, Tim Berners-Lee & Eric Miller, *Integrating Applications on the Semantic Web*, 122 J. INST. ELECTRICAL ENGINEERS JAPAN 676, 680 (2002), *available at* http://www.w3.org/2002/07/swint.

[53] *See* Amir Efrati, *Google Notches One Billion Unique Visitors Per Month*, WALL ST. J. BLOGS (June 21, 2011, 5:24 PM), http://blogs.wsj.com/digits/2011/06/21/google-notches-one-billion-unique-visitors-per-month (noting that in May 2011, Google had millions more unique visitors than its nearest competitor). *See* Press Release, *comScore Releases April 2012 U.S. Search Engine Rankings*, COMSCORE.COM (May 11, 2012), http://www.comscore.com/Press_Events/Press_Releases/2012/5/comScore_Releases_April_2012_U.S._Search_Engine_Rankings (noting that as of April 2012 Google controlled over 66% of the U.S. search market).

[54] It is the company's mission statement. *Company Overview*, GOOGLE.COM, http://www.google.com/about/company/ (last visited Oct. 6, 2012) ("Google's mission is to organize the world's information and make it universally accessible and useful").

[55] *See Ten Things We Know to be True*, GOOGLE.COM, http://www.google.com/about/company/philosophy (last visited Oct. 6, 2012) ("Since the beginning, we've focused on providing the best user experience possible.").

[56] *See* Daniel & Palmer, *supra* note 49 (according to former CEO and current executive chairman Eric Schmidt: "The goal is to enable Google users to be able to ask the question such as 'What shall I do tomorrow?' and 'What job shall I take?' .†.†. We cannot even answer the most basic questions because we don't know enough about you. That is the most important aspect of Google's expansion.").

[57] Emma Barnett, *Marissa Mayer: An Omnivorous Google is Coming*, THE TELEGRAPH (Dec. 14, 2009, 1:16 PM), http://www.telegraph.co.uk/technology/google/6810021/Marissa-Mayer-An-omnivorous-Google-is-coming.html.

[58] *See* Amit Singhal, *Search, Plus Your World*, GOOGLE – OFFICIAL BLOG (Jan. 10, 2012), http://googleblog.blogspot.com/2012/01/search-plus-your-world.html (describing the further advancements of Google+).

photos from Picasa, and even tighter personalization is undoubtedly coming soon.[59]

Central to sharing you with you is centralized processing of data about you from different sources.[60] To be truly useful and personalized, using historical search information and IP addresses is not sufficient.[61] Google envisions personalization across its services.[62] For example: "[Google] can provide reminders that you're going to be late for a meeting based on your location, your calendar and an understanding of what the traffic is like that day. Or ensure that our spelling suggestions, even for your friends' names, are accurate because you've typed them before."[63] Google's new privacy policy, effective March 1, 2012, was enacted to simplify its multitude of different privacy policies into one policy applicable to all services, in order to make "clear that, if you're signed in, we may combine information you've provided from one service with information from other services. In short, we'll treat you as a single user across all our products, which will mean a simpler, more intuitive Google experience."[64]

The possibilities of sharing your own information with you extend far beyond spelling suggestions.[65] The example of combining location, calendar, and traffic information to provide reminders is of far greater utility.[66] The prospects for the individual extend even further. By gathering millions of data

---

[59] *See id.* (describing some of the product's features).

[60] *See id.* (discussing the importance of personalizing the search process).

[61] *See id.* (showing how Google+ is using query networks and other sharing capabilities to link users to stories, photos, and search results that friends or similar Google users have used).

[62] *See Google Accounts–Basics: Web History*, GOOGLE.COM, http://support.google.com/accounts/bin/answer.py?hl=en&answer=54068 (last visited Oct. 6, 2012) (explaining that personalized results based on one's "Web History is just one of the ways that Google helps you find personal content that's relevant to you.").

[63] Alma Whitten, *Updating Our Privacy Policies and Terms of Service*, GOOGLE - OFFICIAL BLOG (Jan. 24, 2012, 11:30 AM), http://googleblog.blogspot.com/2012/01/updating-our-privacy-policies-and-terms.html.

[64] *Id.*

[65] *See id.* ("But there's so much more that Google can do to help you by sharing more of your information with .†.†. well, you. We can make search better—figuring out what you really mean when you type in Apple, Jaguar or Pink.").

[66] This is remarkably similar to the Semantic Web example provided in 2002 by Hendler, Berners–Lee & Miller, *supra* note 52.

points on a user across different services, Google takes a step further towards its stated goal of helping to predict and answer fundamental life questions such as "'What shall I do tomorrow?' and 'What job shall I take?'"[67] The prospect of millions of objective data points across your online – and even offline – behavior presents untold riches for understanding your own psychology and behavior,[68] not to mention the assistance it can provide to your memory.[69] This impacts self-analysis, as well as predictive analysis, in vast, unforeseen ways.[70]

Of course, any individual would rightly be wary of this level of data about her being held by someone else.[71] For many of its users, Google has been something of a digital assistant, helping users find their way across the Internet and making new technologies especially user-friendly.[72] The role is akin to R2D2 in Star Wars: without ulterior motive, maintaining the ship and providing seamless technical solutions while the user steers the ship. Google is there to help you manage, synthesize, and explore your daily schedule, communications, recorded thoughts, and your curiosities.[73]

But Google is not a mere assistant. With all this centralized data, the potential for the user to be bushwhacked is enormous.[74] Google could, if improperly managed, shift from sidekick R2D2 into the omniveillant Hal 9000 from 2001: A Space Odyssey. Much angst is directed at Google on this basis: not based on what

---

67 Daniel & Palmer, *supra* note 49.

68 *Is that all that's left?*, PETER FLEISCHER: PRIVACY.†.†.? (Dec. 20, 2011, 4:09 PM), http://peterfleischer.blogspot.com/2011/12/is-that-all-thats-left.html.

69 *See id.* ("I suspect a future privacy debate will discuss whether 'memory deletion' is a fundamental human right, or deeply anti-social.").

70 *See id.* (discussing the "age of big data" and "whether humans and society can adapt to it as quickly as the technology will enable it.").

71 *See id.* (explaining that some pieces of information should not be shared on the internet).

72 *See Our Products and Services*, GOOGLE.COM, http://www.google.com/about/company/products (last visited Oct. 6, 2012) ("[O]ur goal is to make it possible for you to find the information you need and get the things you need to do done.").

73 *See Google – Products*, GOOGLE.COM, http://www.google.com/about/products (last visited Oct. 6, 2012) (providing a list of Google's products and a brief description of each).

74 *See, e.g.*, Omer Tene, *What Google Knows: Privacy and Internet Search Engines*, 2008 UTAH L. REV 1433, 1435 (2008) (discussing concern about the "potential abuse of [Google's] position as a central database for users' personal information").

Google has done wrong, but on what it could do wrong.[75] For law enforcement or identity thieves, it is the ultimate "honey pot" of personal information.[76] Access by business competitors, or even by friends and family members, could easily lead to disastrous consequences.[77] This level of access to the user's mind and personality also presents enormous opportunity for marketers, raising concerns not so much of sudden harm by unauthorized access to this information, but of the insidious, manipulative use of this information.[78] There is no promise the Google user will be given access to all of the potentially beneficial uses of this data.[79] The monetary value – and the danger – of this amount of personal information is exceedingly large,[80] and Google's concomitant responsibility to protect its users' privacy is equally large.[81] As the aggregator and distiller of a great deal of the world's data, Google is consistently in the crosshairs of privacy watchdogs.[82]

---

[75] *See id.* at 1452 ("At present, search engines do not sell users' personally identifiable information to third parties, yet they retain the ability to do so in the future.").

[76] *Id.* at 1435 ("'[t]he aggregate results of every search ever entered, every result list ever tendered, and every path taken as a result,' constitutes a honey pot for various actors") (quoting John Battelle, *The Database of Inventions*, JOHN BATTELLE'S SEARCH BLOG (Nov. 13, 2003), http://battellemedia.com/archives/2003/11/the_database_of_intentions.php).

[77] *See* Stephanie A. Kuhlmann, *Do Not Track Me Online: The Logistical Struggles Over the Right "To Be Let Alone" Online*, 22 DEPAUL J. ART, TECH. & INTELL. PROP. L. 229, 241-44 (2011) ("Harm to individuals from privacy breaches includes the potential for identity theft, financial loss, physical harm, blackmail, discrimination, and emotional or mental distress from embarrassment.").

[78] *See id.* at 244 (explaining that "companies often sell user data to other companies that then use the data for marketing or advertising" purposes).

[79] *See id.* at 273 (arguing that if websites enact "paywalls" this "may result in creating two options for consumers: free website entry in exchange for permission to track, and a paid subscription without tracking. This could result in lower income populations having less online privacy, or else being excluded from information which is currently freely available.").

[80] *See, e.g.*, *id.* at 241 (discussing the potential harmful financial effects of aggregated user data).

[81] *See* Tene, *supra* note 74, at 1490 (arguing that for privacy purposes search engines are in a fiduciary relationship with their users). Google is aware, at least to some extent, of its responsibility as steward of much of the world's data. *See* Chavez Letter, *supra* note 1, at 3 ("As consumers become more reliant on services provided by third parties, consumer privacy relies increasingly on those parties' internal practices, process, and controls. At Google, we understand our responsibility to our users and continually strive to improve our privacy process.").

[82] The Electronic Privacy Information Center's website lists five cases in

III. USE LIMITATION: AT ODDS WITH SHARING YOU WITH YOU.

If a primary concern of privacy is protecting you from you, Google's ambition to share you with you creates a lightning rod for privacy concerns. To lead the pack in the collection and use of personal information, as Google does, it must also lead the pack in protecting the privacy of that personal information. [83] Its record, despite its "do no evil" slogan, is mixed, as perhaps should be expected for an entity whose business model[84] is based in part on testing society's privacy thresholds.[85]

Key to sharing you with you is sharing your data across different sources.[86] Under many privacy frameworks, data is to be used only for the purposes for which it was obtained, often referred to as the twin concepts of purpose specification and use limitation (which are referred to here simply as use limitation).[87]

---

which EPIC has been opposed to Google – and that is only a limited sample. *Previous Top News: 2012*, EPIC.ORG, http://epic.org/news/2012/default.html (last visited Oct. 6, 2012). "Google" and "privacy" frequently appear in news headlines. *See, e.g.*, GOOGLE NEWS, https://news.google.com/ (last visited Oct. 6, 2012) (searching for "Google" and "privacy" produces a plethora of recent news articles concerning Google's privacy policy).

[83] *See* Tene, *supra* note 74, at 1434–35 (explaining that "Google dominates the Internet" and its "access to and storage of vast amounts of personal information create a serious privacy problem").

[84] *See Ten Things We Know to be True*, *supra* note 55 ("You can make money without doing evil."). Indeed, at least one commentator has stated that "*Google prices and monetizes the privacy rights of the world's citizens*." Karl. T. Muth, *Googlestroika: Privatizing Privacy*, 47 DUQ. L. REV. 337, 338 (2009) (emphasis in original).

[85] "Google's policy .†.†. is to get as close as possible to the 'creepy' line without going past it," according to former CEO and current executive chairman Eric Schmidt. Bianca Bosker, *Eric Schmidt: Google's Policy is To 'Get Right Up To The Creepy Line'*, HUFFINGTON POST (Oct. 4, 2010, 10:01 AM), http://www.huffingtonpost.com/2010/10/04/ eric-schmidt-google-creepy_n_748915.html.

[86] *See* Omar Tene, *supra* note 74, at 1435 (explaining that Google stores users' "entire digital lives").

[87] *See* U.S. DEP'T OF HEALTH, EDUC. & WELFARE, REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS: RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS pt. III (1973), *available at* http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm [hereinafter HEW REPORT] ("There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent."). *See also OECD Privacy Principals*, OECDPRIVACY.ORG, http://www.oecdprivacy.org (setting forth principles of purpose specification and use limitation) (last visited Oct. 6, 2012); Asia-Pacific Economic Cooperation, *APEC Privacy Framework* 2 (2005), *available at* http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx (setting

Specifying the reason that data is requested, and then using the data only for that reason, is seen as key to developing user trust and enabling users to exert a measure of control over the data they share.[88] This principle is found in the federal Privacy Act, which applies to information about you held by the government, and the European Union's Data Protection Directive,[89] as well as various sectoral legislation.[90]

Use limitation has never been a pure or absolute concept.[91] Personal information – including quite private sorts of information – has long been re-used in a wide variety of fields.[92] For example, census data has long exceeded its original purpose as a method to ensure accurate apportionment of seats in the House of Representatives, and is now used for wide-ranging academic, scientific, business, and local government purposes.[93] Markets in securities and commodities, amongst others, run entirely on the re-use of information regarding transactions that

forth a collection limitation principle tied to use and a notice principle that incorporates purpose specification).

[88] *See* DEP'T OF COMMERCE, INTERNET POLICY TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK 38 (2010) [hereinafter DEP'T. OF COMMERCE GREEN PAPER] *available at* http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf (stating that purpose specification and use limitation can help create better alignment between consumer expectations and actual information practices).

[89] Privacy Act of 1974, 5 U.S.C.A. § 552a(e)(3) (West, Westlaw through P.L. 112–142 approved 7/9/12) (requiring federal agencies to inform individuals who ask of the uses of the information stored about them); Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 6, 1995 O.J. (L 281) 31, 40 (requiring that data be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.").

[90] *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C.A. § 1681b (West, Westlaw through P.L. 112–142 approved 7/9/12) (defining limits on the use of consumer credit reports).

[91] *See Sharing Your Personal Information: It's Your Choice*, FED. TRADE COMM'N, http://www.ftc.gov/ privacy/protect.shtm (last visited Oct. 6, 2012) (showing that even when personal information is collected for administrative purposes, the dissemination of that information can be limited by "opting out" of information sharing services).

[92] *See id.* (explaining that organizations may use personal information in a number of ways).

[93] *See, e.g.,* THE COUNCIL OF ECONOMIC ADVISERS, THE USES OF CENSUS DATA: AN ANALYTICAL REVIEW (2000), *available at* http://clinton4.nara.gov/media/pdf/censusreview.pdf (describing the many uses of census data since the early 1800s).

are, on a personal level, quite private. [94] Actuarial studies rely on re-use of health and behavioral data that touches upon extremely private matters. These longstanding practices are viewed as unobjectionable because they are not based on personally identifiable information.[95] However, re-use of personally identifiable information has also become common in our society,[96] particularly in the arena of information technology. At the same time, the distinction between identifiable and non-identifiable information has become considerably weakened, both as a matter of scientific principle and a matter of policy.[97]

Innovation is eating away at the principle of use limitation.[98] This is because of the major benefits to consumers that have been achieved through secondary uses of individual data. The examples are many: telephone number transmission information utilized to provide caller ID; recommendations for movies on Netflix or purchases on Amazon based on the user's past behavior; and the widespread use of history-sensitive hyperlinks that indicate to a user when a link has previously been clicked.[99] Healthcare, retail, traffic management, and energy sectors are

[94] *See* 15 U.S.C.A. §§ 6802–6803 (West, Westlaw current through P.L. 112-142 approved 7/9/12) (allowing financial institutions to disclose nonpublic personal information as long as they disclose to the customers that they will do so).

[95] *See infra* note 106. More precisely, they are based on aggregate information that is not personally identifiable. *Id.*

[96] However controversial the use of state driver's licenses as national ID cards, few would complain at the basic prospect of using a driver's license as a shorthand means to prove one's age. Other commonly-accepted re-uses of personally identifiable information, according to the FTC, include product and service fulfillment, internal operations (such as improving website security), fraud prevention, legal compliance and similar public purposes, and first-party marketing. *See* FTC PRIVACY REPORT, *supra* note 3, at 36.

[97] *See id.* at 2 ("[T]he traditional distinction between personally identifiable information and 'anonymous' data has blurred."); Peter Eckersley, *A Primer on Information Theory and Privacy*, EFF.COM (Jan. 26, 2010), https://www.eff.org/deeplinks/2010/01/primer-information-theory-and-privacy (explaining how an otherwise-anonymous individual can be identified with 33 bits of data, including only a birth date, zip code, and gender); Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1703 (2010) (discussing the failure of anonymity of personal information and the growth of re-identification techniques).

[98] *See* Chavez Letter, *supra* note 1, at 22–24 (noting the change in the landscape of data transfer as technology progresses, including "the increasingly global nature of data transfers").

[99] *See* Richter Letter, *supra* note 37, at 7–8 (discussing examples where original information is re-used to benefit users).

making significant advances based on re-use of data collected for other purposes.[100] As a personal example, in my online account interface my bank has begun displaying a pie chart based on categories of spending to help me better understand where my money goes[101] – a re-use I did not consent to regarding a sensitive category of data, but a re-use I have no objection to as a safe form of sharing me with me.

Within Google, re-use of user information has enabled auto-completion and automated spell checking of search terms; spam, fraud and virus protection tools; Gmail's priority inbox; auto-completion of email addresses in Gmail; pre-population of contact information and Picasa photos in Android phones; and "mob"-based products such as Flu Trends, Traffic, and Translate.[102] Other benefits based on sharing your data – sometimes with you, sometimes with the world at large – are not far away.[103] The existing and potential benefits of re-use of both aggregate and individual personal data are tremendous.[104]

U.S. policymakers are coming to understand these benefits.

---

[100] *See* Omar Tene & Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 STAN. L. REV. ONLINE 63, 64–65 (2012), http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-63_1.pdf (explaining some benefits of using personally collected data for other applications).

[101] *See, e.g.*, *Track Spending*, BANK OF AM. (Jan. 2010), http://webmedia.bankofamerica.com/infocenter/assets/20100106-81325602-1004741/MyPortfolio_TrackSpending.pdf (depicting a bank's method of categorizing an individual's spending).

[102] *See* Chavez Letter, *supra* note 1, at 4 (discussing Google's creative and even serendipitous re-use of data).

[103] Tene & Polonetsky, *supra* note 100, at 68–69.

[104] Use of aggregate information, not tied to user identity, presents a minimal privacy concern compared to use of individual information because there is no real potential for the individual to be harmed by the use of this data. *Id.* Even if the user is given no notice, control, or choice in the matter, and even if the use defies the context in which the information was obtained, there is little possibility for the user to be harmed by an unforeseen use of the data. This is akin to historical examples of aggregate statistical information, such as those discussed above in the census, financial markets, actuarial studies, and similar settings. While "anonymous" data has imperfections, when balanced against the utility of this information there is simply no cognizable privacy interest in this sort of impersonal information, and therefore no concern about use of this data outside the context in which it was obtained. *Id.* at 66. Policymakers are heeding this advice, at least to some degree; the Staff Discussion Draft privacy bill, circulated by Representatives Boucher and Stearns, contains a carve-out for aggregate information that is categorical and has all identifying information removed. STAFF OF SUBCOMM. ON COMMC'NS, TECH, & THE INTERNET, 111TH CONG., 1ST SESS., DISCUSSION DRAFT OF PRIVACY LEGISLATION (2010).

The White House's recent Consumer Privacy Bill of Rights does not include use limitation, but incorporates the concept in a more nuanced "Respect for Context" principle.[105] This principle recognizes that re-use of user information, without express user consent, may be appropriate in some situations – depending on the context in which the information was originally obtained.[106]

The Federal Trade Commission's March 2012 report entitled "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers" breaks this concept of use limitation-in-context down even further.[107] Use limitation is subsumed in a broad category previously used by the FTC called "choice."[108] According to the FTC, re-use by first parties – entities who directly obtain information from the user – is acceptable, including for cross-marketing purposes, without affirmative user consent (i.e. "opting in").[109] This is so because this sort of use is likely to be consistent with the context of the user's relationship with the entity, and because other principles such as transparency help to protect the user.[110]

There are several caveats. First, re-use of sensitive information

---

[105] *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, THE WHITE HOUSE, 10, 16 (Feb. 23, 2012), [hereinafter WHITE HOUSE PRIVACY FRAMEWORK] http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[106] *Id. See also* FTC PRIVACY REPORT, *supra* note 3, at 47–48 (discussing policies, such as Netflix and Amazon's product recommendations, where customer choice is not necessary).

[107] *Id.*

[108] The FTC's concept of choice is not new, *see* F.T.C., PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, A REPORT TO CONGRESS 15 (2000) [hereinafter PRIVACY ONLINE], *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (identifying choice as a key component of consumer privacy); *see also U.S.-EU Safe Harbor Overview*, U.S. DEP'T OF COMMERCE, http://export.gov/safeharbor/eu/eg_main_018476.asp (last updated April. 26, 2012) [hereinafter *Safe Harbor Overview*] (requiring consumer choice as part of the self-certifying Safe Harbor Framework between the United States and European Union). Choice is, however, considerably more defined in the Commission's March 2012 Framework; the FTC's May 2000 report vaguely defined choice as "giving consumers options as to how any personal information collected from them may be used for purposes beyond those necessary to complete a contemplated transaction." *See* PRIVACY ONLINE at 15 (explaining the principle of choice in fair information practice).

[109] This represents a marked change for the FTC. Its 2000 Privacy Online report specifically stated that user choice regarding use of personal information "would encompass both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities)." PRIVACY ONLINE, *supra* note 108, at 36.

[110] *Id.* at 30.

– defined as "information about children, financial and health information, Social Security numbers, and precise, individualized geolocation data" – that is captured by design requires affirmative, express consent.[111] Second, if the user has no other practical alternatives for an important service, "meaningful choice" should be provided to the user.[112] Third, where a first-party entity tracks a user across third-party websites, "meaningful choice" should again be provided.[113] Finally, where re-use of data amounts to a "material change" in use, such that it defies the expectations of the user in the context of the original sharing of that data, affirmative express consent should be required.[114] The import of the FTC's Framework is that no affirmative express consent is needed for first-party re-use of data, except for intentionally-captured sensitive information or where a material change in use occurs.[115]

One additional caveat: there are important limitations on first-party governmental re-use of data, which are beyond the scope of this article.[116] Federal and state governments touch on many facets of life, and the potential for re-use of personal data by governments is tremendous for healthcare, law enforcement, utilities, and more.[117] But government also possesses the power to tax, to regulate, and to punish – to impinge freedoms in ways

---

111 *Id.* at 58–59. This concept is uncontroversial, though the U.S.-EU Safe Harbor identifies sensitive data somewhat differently, as "personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual." *See Safe Harbor Overview*, *supra* at note 109 (describing the privacy policies U.S. organizations should use to comply with the Safe Harbor Frameworks).

112 FTC PRIVACY REPORT, *supra* note 3, at 50–52 (discussing how this provision particularly applies to ISPs and similar services where there is little meaningful competition).

113 *Id.* at 40–41.

114 *Id.* at 57–58.

115 *Cf.* Sara Forden, *Google Privacy Criticized by State Attorneys General*, BLOOMBERG (Feb. 22, 2012, 5:14 PM), http://www.bloomberg.com/news/2012-02-22/state-attorneys-general-tell-google-privacy-policy-is-a-concern.html.

116 They are obviously beyond the bounds of the FTC's jurisdiction. *See* Tal Z. Zarsky, *Governmental Data Mining and its Alternatives*, 116 PENN ST. L. REV. 285, 295–97 (2011) (providing thorough treatment of governmental data mining).

117 *See, e.g.*, Rob Shaw, *How Google Earth Ate Our Town*, TIME (Mar. 10, 2008), http://www.time.com/time/world/article/0,8599,1720932,00.html (demonstrating the different ways in which Google Earth has impacted local government in Nanaimo, British Columbia).

private actors cannot.[118] Use limitation in America initially spawned as a limit on cross-use of personal information in the federal government,[119] and it remains an important bulwark against a Big Brother-like future.[120]

The standards set out by the White House and the FTC do not have the force of law.[121] However, they demonstrate that major stakeholders in the U.S. privacy landscape are prepared to move beyond a broad, vague use limitation concept that does not comport with modern reality.[122] The FTC's Report also demonstrates a substantial shrinking of first-party use limitations that aligns with current understandings.[123] The struggle for Google and others is to "adopt business models that are consistent with baseline [privacy] principles but use personal data in ways that we have not yet contemplated"[124] – including ways that may stretch baseline privacy principles.[125] "Consumers

---

[118] *See* FTC PRIVACY REPORT, *supra* note 3, at 41–42 (defining affiliates as third parties, important to a more expansive concept of re-use by first parties); ANDREWS, *supra* note 41, at 47 (examining how the broad re-use of data across affiliates in a wide-range of sectors can nearly match the reach of the government and contribute to problems of "weblining").

[119] *See* HEW REPORT, *supra* note 87 (asserting that information collected for one purpose must not be used for another without consent).

[120] *See id.* at 87 (requiring that no record keeping systems be kept secret, along with there must be a way for individuals to know how information about them is being used).

[121] *See* Allison M. Dodd & Daren M. Orzechowski, *New FTC Report Recommends Changes to United States Privacy Law*, WHITE & CASE TECH. NEWSFLASH (Apr. 18, 2012), http://www.whitecase.com/articles-04082012 (explaining that the FTC report is not law but a "set of proposals").

[122] The European Union appears less ready to permit incursions on the use limitation principle. Google's new privacy policy has come under fire from the EU largely because it permits the sharing of data across Google's services. Letter from Isabelle Falque-Pierrotin, President of the Commission Nationale de l'Informatique et des Libertés, to Larry Page, CEO of Google (Feb. 27, 2012) [hereinafter Falque-Pierrotin Letter], http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120227_letter_cnil_google_privacy_policy_en.pdf. The Staff Discussion Draft privacy bill circulated by Representatives Boucher and Stearns also adheres to a strict purpose specification principle, even for first-party re-use. WHITE HOUSE PRIVACY FRAMEWORK, *supra* note 105, at 12–13.

[123] FTC PRIVACY REPORT, *supra* note 3, at 6, 13–16.

[124] *Protecting Consumers in the Modern World: Hearing on Privacy & Data Security Before the Comm. on Commerce, Sci. & Transp.*, 112th Cong. 27 (2011) (testimony of Cameron F. Kerry, General Counsel, U.S. Dep't of Commerce).

[125] *Id.* at 26–27 (As the government becomes "nimble enough to respond quickly to consumer data privacy issues as they emerge and that incorporate the perspectives of all stakeholders to the greatest extent possible," Google and others will be required to adjust to the new requirements).

need to know that when their data are re-used, the re-use will not cause them harm or unwarranted surprise."[126] Incursions on use limitation, which necessarily impinge on principles of context and control,[127] ultimately must not use your information in a way that can cause you harm.[128]

IV. IV.SHARING YOU WITH GOOGLE: TWO CONCERNS WITH THE FTC'S USE LIMITATION.

Use limitation has become a more complicated concept – but it is very much alive.[129] It retains its greatest vitality as a limitation on the sharing of data with third parties.[130] Indeed, data in the hands of unknown third parties, where it cannot be ascertained or managed, defies perceptions of context and control, and is where it poses the greatest risk of harm to the user.[131] Focusing use limitation primarily on the third-party

---

[126] DEP'T. OF COMMERCE GREEN PAPER, *supra* note 88, at 39.

[127] *See, e.g.*, Tom Krazit, *Google: Android Won't Share Personal Info with Apps Unless You Let It*, PAID CONTENT (Feb. 16, 2012, 5:27 AM), http://paidcontent.org/2012/02/16/419-google-android-wont-share-personal-info-with-apps-unless-you-let-it (explaining that re-use of data can occur with explicit user consent and control, for example, Google's Android operating system requires the user to expressly consent to use Google's location-based features).

[128] *See* DEP'T. OF COMMERCE GREEN PAPER, *supra* note 88, at 1, 18–19 (discussing ways in which use of certain data harms consumers and creates distrust; also discussing consumer privacy expectations).

[129] Letter from Sen. Al Franken, Chairman, S. Judiciary Subcomm. on Privacy, Tech. & the Law, to Hon. Lawrence E. Strickling, Assistant Sec'y for Commc'n & Info., Nat'l Telecomm. & Info. Admin. (Apr. 2, 2012) [hereinafter Franken Letter] *available at* http://www.ntia.doc.gov/files/ntia/4_2_12_sen_franken_comment.pdf (Senator Franken characterizing privacy in regards to use limitation as not being an "outmoded model" and that privacy laws must keep up with the changes in technology).

[130] *See id.* at 19 (discussing "choice" and "respect for context," Senator Franken, states that "[w]eb sites must maintain a clear boundary between internal uses and external uses and make sure that where data could be used outside its original context, user transparency and control are enhanced."). *See also* FTC PRIVACY REPORT, *supra* note 3, at 47 ("as a general rule, most first-party marketing presents fewer privacy concerns.†.†."); H.R. 5777, 111th Cong. (2d Sess. 2010) (reflecting a strong distinction between first-party and third-party use of data).

[131] *See* Mindi McDowell & Damon Morda, *Socializing Securely: Using Social Networking Services*, U.S. COMPUTER EMERGENCY READINESS TEAM (2011), http://www.us-cert.gov/reading_room/safe_social_networking.pdf (discussing the risks of using social networking sites and expounding on how third party use of personal information made available through social networking can be harmful); *see also* Dennis O'Reilly, *How to Prevent Identity Theft*, CNET NEWS

context should pose little obstacle to Google's ambition to share you with you.[132] But the FTC's take on use limitation does pose several issues for Google's current practices, specifically for Google's tracking of users of third-party websites and for current and future material changes in Google's use of user data.[133]

A. Google's Third-Party Tracking.

The relationship for many users with Google is a sprawling one, extending well beyond a search portal to email, smart phones, and web browsing, amongst other things.[134] It is the interface of choice for many of the world's new consumer technologies.[135] It is a well-recognized brand, and using its search feature has become its own verb.[136] But to most users, Google is not a network of non-Google websites.[137] To the extent Google tracks user behavior

(Sept. 13, 2011, 3:33 PM), http://howto.cnet.com/8301-11310_39-20105419-285/how-to-prevent-identity-theft (identifying the threat of identity theft).

[132] As Google notes, "[t]he use of a primary privacy policy that covers many products and enables the sharing of data between them is an industry standard approach adopted by companies such as Microsoft, Facebook, Yahoo! and Apple." Letter from Peter Fleischer, Global Privacy Counsel, Google France SARL, to Isabelle Falque-Pierrotin, President, CNIL (Apr. 5, 2012) [hereinafter Fleischer Letter], http://rms3647.typepad.com/files/france-google.-1.pdf.

[133] *See* Joanna Stern, *Google Ordered to Pay a Record $22.5 Million for Violating Privacy*, ABC NEWS, (Aug. 9, 2012), http://abcnews.go.com/Technology/google-ordered-pay-ftc-225-million-violating-privacy/story?id=16968371#.UCvpYN1lRcQ (explaining the FTC's current actions against Google related to the tracking of user cookies).

[134] *See* Sebastian Anthony, *Google's Indecipherable Foray into Consumer Electronics*, EXTREMETECH (Feb. 10, 2012, 8:03 AM), http://www.extremetech.com/computing/117843-googles-indecipherable-foray-into-consumer-electronics?print (examining Google's presence in the consumer electronic market); *see also* Vadim Kotelnikov, *Examples of Acquisitions by Google*, INNOVARSITY, http://www.innovarsity.com/coach/bp_venture_acquisition_google.html (last visited Oct. 6, 2012) (listing examples of acquisitions by Google).

[135] *See* Matt Hamblen, *Half a Million Android Smartphones Activated Daily, Google Says*, COMPUTERWORLD (June 28, 2011), http://www.computerworld.com/s/article/9217994/Half_a_million_Android_smartphones_activated_daily_Google_says (discussing the popularity of Google's Android software platform).

[136] *Definition of 'Google'*, MERRIAM-WEBSTER.COM, http://www.merriam-webster.com/dictionary/google (last visited Oct. 6, 2012).

[137] *See* Dawn Kawamoto & Anne Broache, *FTC Allows Google-DoubleClick Merger to Proceed*, CNET NEWS (Dec. 20, 2007, 1:30 PM), http://news.cnet.com/FTC-allows-Google-DoubleClick-merger-to-proceed/2100-1024_3-6223631.html (explaining the interaction between Google and third-party websites); *see also List of Subsidiaries of Registrant: Google Inc.*, S.E.C., http://www.sec.gov/Archives/edgar/data/1288776/000119312507044494/dex2101.

across the Internet, the practice does not comport with the context of the user's relationship with Google.[138]

Tracking users across non-Google websites or sharing user information with entities other than Google is inherently outside the context of the user's interaction with Google.[139] It leaves the user uncertain what is being tracked and where, leaving open the possibility that information will be used or misused to cause the user harm.[140] It undercuts the user trust that is central to Google's business.[141]

It may be that users willingly allow this sort of tracking across third-party websites.[142] According to Google, of those users who visit its Ad Preference Manager, for every user that opts out, seven others elect to remain opted in to its third-party tracking.[143] If Google's services develop to the point that it can identify positive uses of this information in a clear manner, beyond using the information to market to the user, other

htm (last visited Oct. 6, 2012) (listing all of the registered subsidiaries of Google).

[138] This dissonance was, at least arguably, at the heart of the widespread objections to Google's merger with online advertising network and adserving company DoubleClick. *See* Kawamoto & Broache, *supra* note 137.

[139] *See* Michael Zimmer, *Privacy on Planet Google: Using the Theory of "Contextual Integrity" to Clarify the Privacy Threats of Google's Quest for the Perfect Search Engine*, 3 U. MD. J. BUS. & TECH. L. 109, 111–12 (2008) (explaining the relationship that users of Google believe exists between them and the company).

[140] *See id.* at 111 (recognizing the balance between the benefits and detriments that technology creates); *see also Privacy Concerns About Cookies*, WELCOME TO ALL ABOUT COOKIES, http://www.allaboutcookies.org/privacy-concerns (last visited Oct. 6, 2012) (explaining what cookies are and why users have legitimate privacy concerns related to their usage and distribution).

[141] *See* Zimmer, *supra* note 139, at 111 (examining the relationship between Google and its users); *see also* Press Release, FTC., Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), *available at* http://ftc.gov/opa/2012/08/google.shtm (discussing Google's recent fine related to its misrepresentations concerning cookie usage).

[142] Note Bing's relationship with Facebook, and its current effort to incorporate Friends' information in user search results, more plainly involves third-party tracking. Nick Wingfield, *A Revamping of Bing in the Battle for Search Engine Supremacy*, N.Y. TIMES (May 10, 2012), http://www.nytimes.com/2012/05/11/technology/bing-search-engine-to-be-revamped-as-war-against-google-intensifies.html; *see also* Chavez Letter, *supra* note 1, at 4–5 (explaining that many more users opt into the cookie usage policy than opt out).

[143] *See* Chavez Letter, *supra* note 1, at 4–5 (arguing that this would demonstrate that users become more comfortable with data collection and use when they see that it happens on their terms and in full view.").

informed users may find value in the tracking.[144] But until such time as the context of the user interaction with Google shifts to incorporate third-party tracking, Google should require express affirmative consent.[145]

Continuing with passive user consent to this sort of tracking suggests a motivation not to provide helpful services and to protect user privacy,[146] but to bamboozle the user – to cross the "creepy" line and shift from helpful R2D2 to harmful Hal 9000.[147] The practice of third-party tracking without express consent may meet the FTC's "meaningful choice" standard (or it may not), but it does not meet Google's own recognized business need to obtain user trust and lead the pack in protecting user privacy. Particularly where Google's privacy policy offers a "take-it-or-leave-it" choice to users, it should require an express affirmative consent for any of its third-party data tracking and use.[148]

B. Google & Material Changes In Use.

What constitutes a material change in use under the FTC's Framework is unclear.[149] Put broadly, a material change would

---

[144] The value of third-party tracking beyond marketing to the user is not apparent at this time, but it is hardly impossible. Technology inarguably has a crucial role in shaping privacy norms. *See, e.g.*, Jeffrey Rosen, *The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google*, 80 FORDHAM L. REV. 1525, 1535 (2012).

[145] According to Commissioner Roesch, it is unclear if Google's failure to obtain affirmative express consent for third-party tracking complies with the Framework. *See* FTC PRIVACY REPORT, *supra* note 3, at C-7 to C-8.

[146] Zimmer, *supra* note 139, at 112 (examining the uneasy feeling created by Google's collection of user data); *see also*, FTC PRIVACY REPORT, *supra* note 3, at 58 (discussing affirmative consent).

[147] *R2-D2*, INTERNET MOVIE DATABASE, http://www.imdb.com/character/ch0000054 (last visited Oct. 6, 2012); *HAL 9000*, INTERNET MOVIE DATABASE, http://www.imdb.com/character/ch0002900 (last visited Aug. 15, 2012).

[148] According to FTC Chairman Jon Leibowitz, regarding Google's new privacy policy: "Other than saying that they have been clear, and that it's a fairly binary and somewhat brutal choice that they are giving consumers, I think I can't say much more." *See* Juliana Gruenwald, *FTC Chairman: Google Offers 'Brutal Choice' on Privacy Policies*, NAT'L J., TECH DAILY DOSE (Feb. 26, 2012, 11:59 AM), http://techdailydose.nationaljournal.com/2012/02/ftc-chairman-google-giving-con.php (discussing Google users lack of choice in regards to changes in Google policies).

[149] "In response to the request for clarification on what constitutes a material change, the Commission notes that, at a minimum, sharing consumer information with third parties after committing at the time of collection not to share the data would constitute a material change. There

be a change that, "if known to the consumer, would likely affect the consumer's conduct or decisions with respect to the company's products or services."[150] "[A] material change could include . . . using data for different purposes than described at the time of collection, or . . . sharing data with third parties, contrary to promises made at the time of collection."[151] It may include the merger of personally identifiable information with non-identifiable information.[152] Retroactive changes are more likely to be material.[153] As a concrete example of a material change, the FTC found Gateway Learning's renting of user information to third parties, without notice or consent, after it had promised not to do so at the time the user gave Gateway her data, to be a material change in use and a deceptive practice.[154] As the FTC recognizes, whatever may constitute a material change in use must depend on the context of existing uses and the context in which data was initially shared.[155]

Other concrete examples exist.[156] Google itself made a material change in its use of user data with Google Buzz.[157] Google's

---

may be other circumstances in which a change would be material, which would have to be determined on a case-by-case basis, analyzing the context of the consumer's interaction with the business."

FTC PRIVACY REPORT, *supra* note 3, at 57–58.

150 FTC, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING, FTC STAFF REPORT 41 n.73 (2009) [hereinafter FTC ONLINE ADVERTISING REPORT], http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

151 Other than addressing concerns with unspoken third-party sharing, defining a material change as "using data for different purposes than described at the time of collection.†.†." begs the question and does not answer it. *Id.* at 41.

152 *See Self-Regulatory Principles for Online Behavioral Advertising*, INTERACTIVE ADVER. BUREAU, 39 (July 1, 2009), http://www.iab.net/media/file/ven-principles-07-01-09.pdf. The IAB, perhaps surprisingly given its role as an industry representative, requires not simply choice, but consent – meaning an individual's action in response to a clear notice – to any material change in use.

153 *See* FTC ONLINE ADVERTISING REPORT, *supra* note 150, at 41–42 (differentiating between prospective and retroactive change, where the former is less likely to be considered material because it involves new data rather than previously obtained data).

154 Gateway Learning Corp., FTC Docket No. C–4120, Complaint at 6 (2004) [hereinafter *Gateway Complaint*].

155 *See* FTC PRIVACY REPORT, *supra* note 3, at 58 (discussing how case-by-case analysis will be conducted to determine what constitutes a material change).

156 *See* FTC ONLINE ADVERTISING REPORT, *supra* note 150, at 41 (discussing two circumstances where change in policy is considered material).

157 *See* Peter Nowak, *Privacy Commissioner Reviewing Google Buzz*, CBC NEWS (Feb. 16, 2010, 9:55 PM), http://www.cbc.ca/news/technology/story/2010/02/16/google-buzz-privacy.html

privacy policy at the time Buzz was launched stated that it would request user consent before using information for a different purpose than the purpose for which it was collected.[158] Buzz users were surprised by several ways in which Buzz re-used user data, but particularly by how Buzz made public the identity of those individuals with whom Gmail users emailed most frequently.[159] Buzz was slammed by the public, withdrawn as a product, and ultimately forced Google to enter into a Consent Order with the FTC.[160]

Facebook's mutable privacy practices have also drawn the FTC's ire.[161] Facebook has made several material changes to its privacy practices, including in December 2009 making it so users can no longer restrict access to their publicly available information and so that existing choices to restrict access to publicly available information were overridden.[162] These material changes, without meaningful consent from Facebook's users, eventually forced Facebook into a Consent Order with the FTC.[163] More recently, Myspace also found itself facing FTC scrutiny for sharing user information with third parties without express user consent.[164]

These examples illustrate a common theme underlying material changes in use: making public, even if only to "Friends" or discrete third parties, that which was previously designated

(discussing Google's privacy policy change and its exposure of user's sensitive information); *see also Gateway Complaint*, *supra* note 154, at 6 (describing Google's policy change as being a deceptive practice).

158 *Google Policies & Principles, Privacy Policy*, GOOGLE.COM (Mar. 11, 2009), http://www.google.com/policies/privacy/archive/20090311.

159 *See* Nowak, *supra* note 157, at 1 (discussing an example of a user's ex-boyfriend being automatically exposed to her private communications); *see also Gateway Complaint*, *supra* note 154, at 5 (discussing Google users' confusion and lack of awareness involving the exposure of their private information).

160 Google Inc., FTC Docket No. C–4336, Decision & Order at 1 (2011) (discussing consent order executed by Google and Counsel for the Commission).

161 *See* Facebook, Inc., FTC Docket No. C–4365, Complaint at 11 (2011) [hereinafter *Facebook Complaint*] (discussing Facebook's "false and misleading" policy changes between May 2007 to July 2010 that the FTC seek to address).

162 *See* Kurt Opsahl, *Facebook's Eroding Privacy Policy: A Timeline*, ELEC. FRONTIER FOUND. (Apr. 28, 2010), https://www.eff.org/deeplinks/2010/04/facebook-timeline (illustrating the shrinking of Facebook's privacy policy that has occurred over time).

163 Facebook, Inc., FTC Docket No. C–4365, Decision & Order at 1 (2012).

164 Edward Wyatt, *F.T.C. Charges Myspace with Breaking U.S. Law in Sharing Users' Personal Information*, N.Y. TIMES, May 9, 2012, at B3, *available at* http://www.nytimes.com/2012/05/09/technology/myspace-agrees-to-privacy-controls.html.

private.[165] That making public things that were private is a material change may seem self-evident.[166] A corollary is that keeping private that which is private – such as first-party re-use of non-sensitive personal information – would not rise to the level of a material change in use.[167] Somewhere in between would be changes in use of already-public information to make it even more public, such as Facebook's News Feed, which shifted users from "pulling" to find their Friends' updates to having those updates "pushed" to them.[168] This change generated a massive public outcry, but has since become accepted by Facebook users, raising questions of whether affirmative express consent should have been provided for such a change.[169]

The threshold for a material change in use, requiring affirmative express consent, should be a high one, only implicated when the change in use involves sensitive data or the mutation of a first-party use into a third-party use, or in contexts where the user has no meaningful choice (including governmental re-use).[170] If a core concern of informational privacy is keeping your information from harming you, there is little need to require affirmative express consent in order to share your information with you.[171] Other changes in use may be major, but not material, and are better addressed as issues of

---

[165] *See Facebook Complaint*, *supra* note 161, at 7, 9 (discussing Facebook overriding previous privacy policies with new policies which allowed users to gain access to information previously believed to be private).

[166] *See* FTC PRIVACY REPORT, *supra* note 3, at 8 (discussing restrictions placed on users' privacy settings without their knowledge is considered material regardless of actual physical or economic harm).

[167] *Id.* at 15–16.

[172] *See* Christopher M. Hoadley, et al., *Privacy as Information Access and Illusory Control: The Case of the Facebook News Feed Public Outcry*, ELEC. COMM. RES. & APPL. 2 (May 4, 2009), http://steinhardt.nyu.edu/scmsAdmin/uploads/004/303/sdarticle.pdf (discussing Facebook's News Feed which undoubtedly raised concerns regarding context and control, but whether it really wrought a material change in use, where the information involved was already published to each user's Friends, seems unlikely).

[169] Bing's "social search" endeavor, sharing Facebook Friends' data across each others' searches on Bing, stretches the matter even further, and clearly involves third-party sharing of data. Under any framework, affirmative express consent is indicated for this sort of service. Wingfield, *supra* note 142.

[170] FTC PRIVACY REPORT, *supra* note 3, at 57.

[171] *See* DEP'T. OF COMMERCE GREEN PAPER, *supra* note 88, at 38 (discussing purpose specification, which provides consumers with notice of specific objectives regarding use of first-party information rather than obtaining affirmative consent for such use).

notice and transparency.[172] Beneficial first-party re-uses should not require express affirmative consent:

> Providing consumers with notice of a change and an opportunity to consent to new uses of existing data may address the legal issues that companies face when making retroactive privacy policy changes, but these steps do little to clarify whether certain kinds of changes are especially likely to bring social benefits (or harms) and thus should be subject to lesser (or greater) scrutiny.[173]

Re-uses of data can be jarring, but often in ways that are ultimately acceptable.[174] Advance knowledge of major changes, and allowing the user to test, manage, and grow accustomed to these changes avoids much of the shock and harm while allowing technology that appropriately stretches current paradigms to gain acceptance and evolve.[175] Particularly for an entity like Google, which has a complex, multi-faceted relationship with its users,[176] major changes that involve first-party re-use of data may stretch the context of the user's relationship with Google, but do not fundamentally alter the relationship.[177]

Requiring proper notification and transparency, but not necessarily express affirmative consent for major (but not "material") changes in first-party use is beneficial to users and to the development of technologies that share you with you.[178] It avoids much of the controversy over what constitutes a "material

---

[172] *See id.* at 39 (indicating that issues of re-use may often be treated as issues of transparency, the Department of Commerce notes: "As valuable as that re-use may be, failures in current transparency regimes may come as a surprise to users.").

[173] *Id.*

[174] *See* FTC PRIVACY REPORT, *supra* note 3, at 39–40 (discussing the fine line between practices considered unacceptable and instances where "repurposing" of data meet the revised FTC guidelines).

[175] *See* Letter from Jules Polonetsky & Christopher Wolf, Future of Privacy Forum, to Donald S. Clark, Sec'y of the FTC at 5 (Feb. 18, 2011) [hereinafter Polonetsky Letter], http://www.ftc.gov/os/comments/privacyreportframework/00341-57842.pdf (discussing user notification and knowledge of privacy changes stating, "[i]f the new use is transparent and obvious to users, and also provides added value to the user, then an opt-out system would appear permissible as long as the opt-out is clear and conspicuous.").

[176] *See* Richter Letter, *supra* note 37, at 21 (discussing Google Reader's use of multiple service and content providers).

[177] *See id.* (discussing Google's re-use of data as an integral aspect of its services, which is expected by consumers).

[178] *See* DEP'T. OF COMMERCE GREEN PAPER, *supra* note 88, at 39 (discussing the beneficial aspect of first party re-use to each individual so long as there is transparency and notice of such re-use).

change" in use, and the concomitant "race to the bottom" in drafting privacy policies so broad and vague that no change becomes material.[179]

Much of the dispute with Google's new privacy policy surrounds the simplification of the policy.[180] Simplified privacy policies have long been desired, in contrast to the lengthy tome many websites require users to read (and which few users actually do read).[181] But broad, vague policies can also obfuscate.[182] The European Union favors a "layered" approach, allowing the user to drill down from general terms to specifics.[183] Google contends that this is just the sort of "short notice/long notice" privacy policy it offers, and its new broad, general policy combined with its Dashboard supports this position.[184] The balance is in some respects akin to that for product warning labels, where, depending on the context of the use, a reasonable warning often merits some combination of simple images and diagrams with a more lengthy textual description of the dangers.[185]

Allowing first-party re-use of all but sensitive data puts the focus on effective communication with users regarding the use of their data.[186] Empowerment and control – even if it is the take-it-or-leave-it sort of control – are the result of effective notice and transparency.[187] Meanwhile, positive re-uses of data can freely

---

179 *See* Richter Letter, *supra* note 37, at 10 (arguing that under a broad definition of "material," substantial detail in a privacy policy would create a "one-way ratchet" where any subsequent change would require affirmative express consent).

180 *See* Falque-Pierrotin Letter, *supra* note 122, at 2 (stating that simplifying privacy policy should not be conducted at the expense of transparency and comprehensiveness).

181 *See id.* (commending the simplicity efforts, but stating that more needs to be done).

182 *See id.* at 1–2 (discussing challenges users face when trying to understand privacy policies).

183 *See id.* at 2 (explaining the layered approach recommended for Google).

184 *See* Fleischer Letter, *supra* note 132, at 2, 11 (discussing use of a layered privacy policy for Google's Find my Face service).

185 *Cf.* Corey A. Ciocchetti, *The Future of Privacy Policies: A Privacy Nutrition Label Filled With Fair Information Practices*, 26 J. MARSHALL J. COMPUTER & INFO. L. 1, 4, 28 (2009) (suggesting adoption of standardized nutrition label-type privacy policies).

186 *See* Polonetsky Letter, *supra* note 175, at 6 (discussing the definition of sensitive data and the use of research to better define this area).

187 *See* Ciocchetti, *supra* note 185, at 13–15 (stating that notice is an important practice to make consumers aware of companies information sharing policies).

develop.[188] For a populace that is increasingly technologically savvy and increasingly concerned about privacy, limits on first-party re-use should properly be placed in the hands of the user, but in a way that does not stifle development.[189] An emphasis on notice and transparency in the context of first-party re-use of user data is the best means to accomplish this goal.

[188] *See id.* at 4–5 (stating that properly drafted policies allow executives to use the information properly, and allows consumers to be fully aware of how the information is being used).

[189] *See* Polonetsky Letter, *supra* note 175, at 3–4 (stating the benefits of having a "Do Not Track" option on websites that gives the user control of whether or not the website can track personal information).