I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Are IP Addresses "Personally Identifiable Information"?

FREDERICK LAH*

Abstract: This note frames the major issues surrounding the definition of "personally identifiable information," otherwise known as "personal data," and focuses on the question of whether Internet Protocol ("IP") addresses fall into the parameters of this definition. In WP 148, Opinion 1/2008 on Data Protection Issues Related to Search Engines, the Article 29 Data Protection Working Party of the European Union concluded that IP addresses are personal data, and subsequently held that search engines and other websites that collect IPs should be subject to heightened regulations. While the Working Party's findings are persuasive to the European Union Member States, they are not binding on the Member States, nor are they binding on any countries outside of the European Union. In the United States, for example, websites that collect IPs will continue to run their businesses essentially only bound by the promises made in their privacy policies. The classification of IP addresses is of particularly great interest to search engines since the quality of their searches and the revenue from their advertisements may depend on their ability to use IPs. In light of WP 148 and recent court decisions, the debate surrounding the proper classification of IPs has intensified.

* The author is a Juris Doctor Candidate at The Ohio State University Moritz College of Law (expected date of graduation May 2009). Frederick Lah is also a Certified Information Privacy Professional; he earned his accreditation from the International Association of Privacy Professionals in March 2008.

I. INTRODUCTION

According to one definition, "personally identifiable information" ("PII"), or "personal data," is any data used to identify, contact, or locate a person.[1] Certain types of information, such as name, social security number, mailing address, and phone number are traditionally accepted as personal information. These pieces of information—alone or in combination with other pieces of information—may be used to identify an individual.[2] As new technology emerges, it is unclear whether other types of information should be classified as PII.

At the forefront of the debate over what qualifies as PII are Internet Protocol ("IP") addresses. An IP address is a 32-bit (or 128-bit) unique string of numbers that identifies a computer, printer, or other device connected to the Internet.[3] Websites, particularly search engines, have a variety of uses for IP addresses, most of which will be discussed below. While IP addresses have been used since the inception of the Internet, their classification has recently become the subject of an intensifying debate. If IP addresses are classified as PII, then processors and controllers[4] of IP addresses will be burdened by heavier regulations, and their use of this data will be restricted. If, on the other hand, IP addresses are not classified as PII, websites will continue to treat them relatively free of regulation.

---

[1] NAI: Network Advertising Initiative, Frequently Asked Questions, http://www.networkadvertising.org/managing/faqs.asp#question_3 (last visited Jan. 27, 2009).

[2] NAI: Network Advertising Initiative, Principles Overview, http://www.networkadvertising.org/networks/principles.asp (last visited Jan. 27, 2009).

[3] CNET Glossary, http://reviews.cnet.com/4520-6029_7-6160768-1.html (last visited Jan. 27, 2009).

[4] The E.U. Data Protection Directive defines a "processor" as a "natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller." The Directive defines a "controller" as a "natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations . . ." Council Directive 95/46, art. 28, 1995 O.J. (L 281) 47 (EU) [hereinafter Council Directive 95/46], *available at* http://www.cdt.org/privacy/eudirective/EU_Directive_.html.

The Article 29 Data Protection Working Party[5] of the European Union has decided that IP addresses do, in fact, qualify as personal data.[6] While the Working Party's findings are only considered advisory to the E.U. Member States,[7] if a State decides to adopt the Working Party's findings, then such a decision will affect how search engines operate their services in the State; the collection and use of IP addresses would consequently have to comply with the E.U. Data Protection Directive.[8] In the United States, no comprehensive legislation regarding personal information exists,[9] so it is unclear whether such a widespread decision to change the classification of IPs could even be implemented. In any event, search engines in the United States will continue to run their businesses only bound by the promises made in their privacy policies.[10]

This note frames the major issues surrounding the definition of PII, focusing on the debate of whether IP addresses should be classified as PII. This note is divided into five parts. The first section provides a comparison of how the privacy regimes in the United States and the European Union define PII, focusing on the terms "reasonably linked" and "identifiable person." The second section provides a basic

---

[5] The Data Protection Working Party was established under Article 29 of the Data Protection Directive. It is an independent European advisory body on data protection and privacy. It was set up to provide expert opinion about data protection from state-level members to the European Commission and to advise the Commission on any measures affecting the rights and freedoms of natural persons with regard to the processing of personal data and privacy. *Id.*

[6] Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data*, 16, 01248/07/EN/WP 136 (June 20, 2007) [hereinafter *Opinion 4/2007*], http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf. Article 29 Data Protection Working Party, *Opinion 1/2008 on Data Protection Issues Related to Search Engines*, 8, 00737/EN/WP 148 (Apr. 4, 2008) [hereinafter *Opinion 1/2008*], http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf.

[7] *See generally*, Tasks of the Article 29 Data Protection Working Party, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/tasks-art-29_en.pdf (last visited Jan. 27, 2009).

[8] *Opinion 1/2008*, *supra* note 6, at 24.

[9] PETER P. SWIRE & SOL BERMANN, INFORMATION PRIVACY: OFFICIAL REFERENCE FOR THE CERTIFIED INFORMATION PRIVACY PROFESSIONAL 14 (Peter Kosmala ed., Int'l Ass'n of Privacy Prof'ls 2007).

[10] Fed. Trade Comm'n, Enforcing Privacy Promises: Section 5 of the FTC Act, http://www.ftc.gov/privacy/privacyinitiatives/promises.html [hereinafter Enforcing Privacy Promises] (last visited Jan. 27, 2009).

tutorial on how IP addresses work, and the following section explains how an IP address can be used to identify an individual. The fourth section highlights some of the findings made by the Working Party in WP 148, *Opinion 1/2008 on Data Protection Issues Related to Search Engines* and also discusses some recent court decisions concerning IPs. The final section presents some expert opinion from both sides of the debate.

II. DEFINING PII: FROM THE EUROPEAN UNION TO THE UNITED STATES

The European Union and the United States differ markedly in their approaches to data protection, and specifically in their approaches to defining PII. As stated earlier, there is no comprehensive data protection legislation in the United States; instead, U.S. privacy law is sector-specific.[11] As a result, there is no uniform definition of personally identifiable information in the United States. Rather, U.S. laws typically define the term by providing various examples.[12] Additionally, these laws generally set restrictions on the collection and use of such information.[13] While U.S. privacy laws may use different terms and govern different kinds of information, they share similarities with the E.U. privacy laws throughout.[14]

Where no laws exist for a particular sector, companies in these sectors essentially function on a system of self-regulation, only bound

---

[11] Sector-specific means that each U.S. privacy law pertains to a specific issue, i.e., health information, financial institutions, credit reporting, Internet use for children. SWIRE & BERMANN, *supra* note 9.

[12] See the Appendix to this note for numerous examples of how U.S. privacy laws define "personal information."

[13] Due to the sector-specific approach, privacy laws in the United States are enforced by various players, such as the Federal Trade Commission, the Federal Communications Commission, and state Attorneys General. SWIRE & BERMANN, *supra* note 9, at 14–15. In contrast, the European Union's Data Protection Directive requires each member country to establish its own Data Protection Authority ("DPA") as a means to ensure compliance with its privacy laws. Council Directive 95/46, *supra* note 4.

[14] Many of these commonalities are based on the Fair Information Practice Principles of Notice/Awareness, Choice/Consent, Access/Participation, Integrity/Security, and Enforcement/Redress. Fed. Trade Comm'n, Fair Information Practice Principles, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last visited Jan. 27, 2009).

by their self-proclaimed privacy policies.[15] Many search engines define personal information in their privacy policies by simply providing examples of the term,[16] while others explicitly set forth their own definition of personal information in their privacy policies. Ask.com, for example, defines PII as "information you provide to us that is uniquely associated with you, such as your name or e-mail address."[17] Similarly, Google defines personal information as "information that you provide to us which [sic] personally identifies you, such as your name, email address or billing information, or other data which can be *reasonably linked* to such information by Google."[18] What the term "reasonably linked" means is a pivotal issue for Google as IP addresses could potentially fall into the PII category. If, in fact, IP addresses can be reasonably linked to a person's identity, then Google would be obligated to treat such data as personal information, as set forth in its Privacy Policy.[19] Failure to comply with its Privacy Policy could result in a lawsuit under Section 5 of the Federal Trade Commission ("FTC") Act.[20]

---

[15] Enforcing Privacy Promises, *supra* note 10. In December 2007, the FTC proposed self-regulatory principles for online behavioral advertising. Press Release, Fed. Trade Comm'n, FTC Staff Proposes Online Behavioral Advertising Privacy Principles (Dec. 20, 2007), *available at* http://www.ftc.gov/opa/2007/12/principles.shtm.

[16] Microsoft's Privacy Statement provides examples of "personal information" on its website: "[a]t some Microsoft sites, we ask you to provide personal information, such as your e-mail address, name, home or work address, or telephone number. We may also collect demographic information, such as your ZIP code, age, gender, preferences, interests and favorites. If you choose to make a purchase . . . we will ask for additional information, such as your credit card number and billing address." Microsoft Online Privacy Statement, http://privacy.microsoft.com/en-us/fullnotice.mspx (last visited Jan. 27, 2009).

[17] Privacy Policy for Ask.com, http://about.ask.com/en/docs/about/privacy.shtml#1 (last visited Jan. 27, 2009).

[18] Google Privacy Glossary, http://www.google.com/privacy_glossary.html#personalinfo (last visited Jan. 27, 2009) (emphasis added).

[19] Google Privacy Policy, http://www.google.com/privacypolicy.html (last visited Jan. 27, 2009).

[20] "Using its authority under Section 5 of the FTC Act, which prohibits unfair or deceptive practices, the Commission has brought a number of cases to enforce the promises in privacy statements, including promises about the security of consumers' personal information. The Commission has also used its unfairness authority to challenge information practices that cause substantial consumer injury." Enforcing Privacy Promises, *supra* note 10.

In response to a questionnaire presented by U.S. House Representative Joe Barton, Google attempted to clarify the term "reasonably linked."[21] Following Google's acquisition of DoubleClick, which was under FTC review at the time, a number of Senators and Representatives called for a closer look into the privacy issues that were raised by the merger.[22] Representative Barton[23] addressed many of those issues in the questions he posed to Google.[24] Google's answer to a question about the term "reasonably linked" highlights many of the key factors privacy regimes must consider in defining PII:

> [W]hether information can be 'reasonably linked' to an identifiable individual turns on (i) what the data itself is– and in particular how frequently it accurately and reliably describes an individual; (ii) what kind of

---

[21] Letter from Alan Davidson, Senior Policy Counsel, Google, to Joe Barton, U.S. Representative (Dec. 21, 2008), *available at* http://searchengineland.com/pdfs/071222-barton.pdf.

[22] Letter from Herb Kohl & Orrin Hatch, U.S. Senators, to Deborah Platt Majoras, Fed. Trade Comm'n Chairman (Nov. 19, 2007), *available at* http://epic.org/privacy/ftc/google/sen_anti_111907.pdf; Letter from Cliff Sterns, U.S. Representative, to Bobby L. Rush, Chairman, Subcomm. on Commerce, Trade and Consumer Protection (Nov. 6, 2007), *available at* http://republicans.energycommerce.house.gov/Media/File/News/11.06.07_Hearing_Request_Letter.pdf.

[23] According to one report, while Barton's letter stated that he was "concerned about the 'privacy implications of the merger,' he has a long history of voting for legislation that has been criticized by privacy groups such as the Electronic Privacy Information Center. Those bills include the Real ID Act, the Patriot Act, another bill to expand Internet surveillance performed without a court order, and a requirement to disclose federal agencies' data-mining programs to the U.S. Congress (Barton opposed that last requirement)." Declain McCullagh, *House Republican Targets Google on Privacy Grounds*, CNET NEWS, Dec. 12, 2007, http://news.cnet.com/8301-13578_3-9832985-38.html.

[24] In addition to asking Google about the term "reasonably linked," Representative Barton also asked the following questions: please identify the sections of Google's privacy policy that address the retention and use of the data [collected from cookies]; please explain how and why information is combined or shared across platforms when consumers opt-in for personalized services and whether Google first requires consent prior to such information-sharing; please explain in what circumstances Google links information such that an individual can be identified; please explain whether Google considers an IP address to be "personal information." In response to the last question, Google answered in the negative: "An IP address cannot necessarily be tied to any individual user or even to an individual machine– multiple unrelated users can easily show the same IP address in their web requests." Letter from Alan Davidson, *supra* note 21, at 10, 13.

> additional information is needed to identify the specific person to whom that data relates; (iii) who has access to the additional data needed; and (iv) the circumstances under which the additional data will be made available to others.[25]

Unlike the United States, the European Union has comprehensive legislation directly related to data protection known as the Data Protection Directive.[26] The Directive defines personal data as "any information relating to an identified or identifiable natural person."[27] Although the European Union has a uniform definition of personal data, Member States' application of the definition in practice has not been exactly consistent.[28] In response to this inconsistency, the Data Protection Working Party released WP 136, *Opinion 4/2007*.[29] The *Opinion* discussed the concept of personal data in June 2007 and clarified some of the issues surrounding its definition.[30] The Working Party, in its analysis, broke down the definition of personal data into four elements: (1) any information (2) relating to (3) an identified or identifiable (4) natural person.[31] In addressing the third element, WP 136 states that a person is identifiable when, "although the person has not been identified yet, it is *possible* to do it."[32]

---

[25] *Id.* at 13.

[26] Council Directive 95/46, *supra* note 4.

[27] *Id.* at 38. In addition, the European Union has prohibitions on the processing of special categories of data, such as any personal data which reveals the "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and of data concerning health or sex life." Council Regulation 45/2001, art. 10, 2000 O.J. (L8) 8 (EC), ec.europa.eu/justice_home/fsj/privacy/docs/application/286_en.pdf. The Asia-Pacific Economic Cooperation uses a definition of "personal information" similar to that of the European Union. Chris Pounder, *Why the APEC Privacy Framework is Unlikely to Protect Privacy*, OUT-LAW.COM, Oct. 15, 2007, http://www.out-law.com/page-8550.

[28] *Opinion 4/2007*, *supra* note 6.

[29] *Id.*

[30] *Id.*

[31] *Id.* at 6.

[32] *Id.* at 12.

Drawing upon the Directive's definition of an "identifiable person,"[33] WP 136 states that "a person may be identified *directly* by name or *indirectly* by a telephone number, a car registration number, a social security number, a passport number or by a combination of significant criteria which allows him to be recognized by narrowing down the group to which he belongs."[34] According to the *Opinion*, this is not to say that any hypothetical possibility of identifying an individual suffices to make that person identifiable.[35] As Recital 26 of the Directive reads, "to determine whether a person is identifiable, account should be taken of *all the means likely reasonably* to be used either by the controller or by any other person to identify the said person."[36] Because third parties can—using reasonable means—identify users to whom they have attributed an IP address, the Working Party has determined that users are identifiable through their IPs, thus, qualifying them as personal data.[37] Before exploring how identification can be achieved through an IP address, it is first necessary to understand how IP addresses work.

III. HOW IP ADDRESSES WORK

IP addresses consist of two components: (1) the Network ID, which is the set of numbers that is used to identify the network where the host is located, and (2) the Host ID, the remaining set of numbers

---

[33] The Directive provides that an "identifiable person" is a person "who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." Council Directive 95/46, *supra* note 4.

[34] *Opinion 4/2007*, *supra* note 6, at 13.

[35] *Id.* at 15.

[36] Under the Directive, factors such as the cost of conducting identification, "the intended purpose, the way the processing is structured, the advantages expected by the controller, the interests at stake for the individuals, as well as the risk of organisational dysfunctions (e.g., breaches of confidentiality duties) and technical failures should all be taken into account." *Id.*

[37] Article 29 Data Protection Working Party, *Working Document: Privacy on the Internet– An Integrated EU Approach to On-line Data Protection*, 21, 5063/00/EN/FINAL/WP 37 (Nov. 21, 2000) [hereinafter *Privacy on the Internet– An Integrated EU Approach*], ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf.

identifying the network.[38] In most cases, IP addresses are assigned automatically by a special server computer called a DHCP (Dynamic Host Configuration Protocol) Server.[39] Internet Service Providers ("ISPs"), such as Comcast and AT&T, typically have their own DHCP Servers that assign IP addresses for Internet users.[40]

IP addresses can be either dynamic or static.[41] Internet Service Providers assign dynamic IP addresses to a computer for only as long as the current user's Internet session lasts; a new IP address is assigned for each subsequent Internet session.[42] With dynamic IPs, the DHCP typically works in conjunction with a Domain Name System ("DNS")[43] to allow users to search the Web.[44] In theory, the address a user gets from the DHCP can change over time, but in practice servers often return the same address to the same client for weeks to months at a time.[45]

Static IP addresses do not change; the same number is assigned to the same computer consistently over time.[46] Static IP addressing is

---

[38] *The TCP/IP Guide: A TCP/IP Reference You Can Understand*, http://www.tcpipguide.com/free/t_IPBasicAddressStructureandMainComponentsNetworkIDa.htm (last visited Jan. 27, 2009).

[39] DOUG LOWE, NETWORKING FOR DUMMIES 199 (4th ed. 1999).

[40] If the user does not connect to the Internet via an ISP, then the user can configure a server computer to operate as a DHCP server for his or her own network. *Id.*

[41] CNET Glossary, *supra* note 3.

[42] *Id.*

[43] In general, a Domain Name System is a database that translates host names into IP addresses. Paul Vixie, *DNS Complexity*, ACM QUEUE, http://www.acmqueue.com/modules.php?name=Content&pa=showpage&pid=481 (last visited Jan. 27, 2009).

[44] "When you dial up to your Internet Service Provider (ISP), DHCP is used to assign an IP address to your connection. When you enter a "WWW" address in your browser address bar or select a human-readable link on a web page, a DNS is used to turn your URL request into an IP address for transmission." *TCP/IP Tutorial: Dynamic v. Static IP Addressing*, DPS TELECOM [hereinafter *TCP/IP Tutorial: Dynamic v. Static IP Addressing*], http://www.dpstele.com/protocol/2001/may_jun/ip_addressing.php (last visited Jan. 27, 2009).

[45] THOMAS NARTEN & RICHARD DRAVES, PRIVACY EXTENSIONS FOR STATELESS ADDRESS AUTOCONFIGURATION IN IPV6 3 (2001), http://tools.ietf.org/html/rfc3041.

[46] CNET Glossary, *supra* note 3.

useful in helping to eliminate the network traffic associated with the DHCP/DNS combination;[47] however, it is easier to identify Internet users who connect through static IPs because the website will recognize the user as the same user every time that person returns.[48] Historically, most Internet users have been assigned dynamic IP addresses, with static IPs being used primarily for servers,[49] but some cable and most new broadband connections also use static IPs.[50]

The current dominant version of IP is called IPv4. However, only about one third of the original pool of useable IPv4 addresses remains available.[51] IPv6 was designed to address the shortcomings of the IPv4 standard, particularly the potential shortage of addresses.[52] According to one study, there are just over four billion IPv4 addresses; in contrast, there are over sixteen billion IPv6 addresses.[53] IPv6 also provides numerous other beneficial features not included in IPv4.[54]

---

[47] *TCP/IP Tutorial: Dynamic v. Static IP Addressing*, *supra* note 44.

[48] *Privacy on the Internet– An Integrated EU Approach*, *supra* note 37, at 21.

[49] *Dynamic vs. Static IP Addresses*, WHATISMYIPADDRESS.COM, http://whatismyipaddress.com/staticpages/index.php/dynamicstatic (last visited Jan. 27, 2009).

[50] Press Release, Verizon, Verizon Introduces Its Revolutionary All-Fiber-Optic Network and FiOS Internet Service in Brooklyn (Aug. 20, 2007), *available at* http://newscenter.verizon.com/press-releases/verizon/2007/verizon-introduces-its.html.

[51] Alissa Cooper, *Future Prospects of "Potentially" Personal Information*, CTR. FOR DEMOCRACY & TECH., Feb. 29, 2008, http://blog.cdt.org/2008/02/29/future-prospects-of-%e2%80%9cpotentially%e2%80%9d-personal-information.

[52] *Id.* This shortage was aggravated due to the facts that portions of IP address space have not been allocated efficiently and that the traditional model of addressing does not allow the address space to be used to its maximum potential. 3COM, UNDERSTANDING IP ADDRESSING: EVERYTHING YOU EVER WANTED TO KNOW 1 (2001), http://www.3com.com/other/pdfs/infra/corpinfo/en_US/501302.pdf. A recent study suggests that the problem of a shortage may not be as serious as it seems. *First Broad Internet Census Since 1982 Reveals a Surprising Number of Unused IPv4 Addresses*, CIRCLEID, Oct. 15, 2008, http://www.circleid.com/posts/20081015_internet_census_ipv4_address.

[53] ARIN: AMERICAN REGISTRY FOR INTERNET NUMBERS, IPv4 & IPv6, http://www.arin.net/about_us/media/fact_sheets/IPv4_IPv6.pdf (last visited Jan. 27, 2009).

[54] Among some of these changes are a "streamlined IPv6 header, stateless configuration, built in security, better [support for quality of service], and increased real time performance." 3COM, *supra* note 52, at 51; for a detailed explanation of how IPv6 works,

IPv6 technology is not without its potential drawbacks though. With IPv6, the IP address can contain a Host ID, or interface identifier, that remains constant even when the Network ID, or topographic portion, of the address changes.[55] In this regard, the IPv6 may be considered a hybrid of the static and dynamic forms of IP addresses, with part of it remaining constant and the other part changing. The concern with IPv6 is that the constant interface identifier could potentially be used to track the movement and usage of a particular device as it connects from different locations.[56] As one report describes:

> [A] server that logs usage information together with a source addresses [sic], is also recording the interface identifier since it is embedded within an address. Consequently, any data-mining technique that correlates activity based on addresses could . . . be extended to do the same using the interface identifier. This is of particular concern with . . . network-connected devices (e.g., PDAs, cell phones, etc.) in which large numbers of devices are in practice associated with individual users . . . . Thus, the interface identifier embedded within an address could be used to track activities of an individual, even as they move topologically within the internet.[57]

The use of a constant interface identifier represents a stark contrast from IPv4, where the entire IP address usually changes.[58] With IPv6 already being implemented in many companies and agencies,[59] and soon to be implemented on an even larger scale, an

---

see STEPHEN DEERING & ROBERT HINDEN, INTERNET PROTOCOL, VERSION 6 (IPV6) SPECIFICATION (1998), http://www.ietf.org/rfc/rfc2460.txt.

[55] NARTEN & DRAVES, *supra* note 45, at 4.

[56] *Id.* at 5.

[57] *Id.*

[58] *Id.* at 4.

[59] Memorandum from Karen S. Evans, Office of E-Government and Information Technology Administrator to Chief Information Officers, Executive Office of the President (Aug. 2, 2005), http://www.whitehouse.gov/omb/memoranda/fy2005/m05-22.pdf.

increasing number of Internet users will have IP addresses that may be more susceptible to tracking. As a result, a greater number of IP addresses may be easily linked to the individual devices, and potentially to their users. As Marc Rotenberg, Executive Director of the public interest group Electronic Privacy Information Center ("EPIC"), states, "we are moving towards the IPv6 model, for which it will be even more the case that IP addresses will be personably [sic] identifiable."[60]

On the other hand, proponents of IPv6 have pointed out that communication initiated by an IPv6 device, such as requesting a Web page or accessing an email server, need not include or reveal a unique serial number.[61] Rather, other types of non-unique random numbers could be used instead, thus making it more difficult to match a particular user with an IP address.[62]

IV. TURNING AN IP INTO AN ID

Every time someone uses a search engine, the website automatically records information into a log file or server log.[63] Such information may include the user's Uniform Resource Locator ("URL"), search queries, browser type and language, the date and time of the search, and the IP address.[64] In addition to the information stored in log files, search engines deploy a Web cookie to be stored on the user's computer, which contains information about the user's operating system, browser, search preferences and tracking trends, and they also deploy a unique ID for each user account.[65]

---

[60] Mike Sachoff, *EU Wants IP Addresses To Be Personal*, WEBPRONEWS, Jan. 22, 2008, http://www.webpronews.com/topnews/2008/01/22/eu-wants-ip-addresses-to-be-personal.

[61] Steve Deering & Bob Hinden, *Statement on IPv6 Address Privacy*, Nov. 6, 1999, http://playground.sun.com/ipv6/specs/ipv6-address-privacy.html.

[62] "The initiating device may use any of the kinds of addresses currently used in IPv4, e.g., manually assigned, or dynamically assigned—perhaps only temporarily—by an address server such as DHCP or by a dial-up ISP. It may also use a new kind of address, available only in IPv6, that contains a random number in place of the factory-assigned serial number." *Id.*

[63] Google Privacy FAQ and Glossary, http://www.google.com/intl/en/privacy_faq.html (last visited Jan. 27, 2009).

[64] *Opinion 1/2008, supra* note 6.

[65] *Id.* at 7.

The information in log files, particularly the IP address, can serve a multitude of purposes for search engines and other websites. First, all websites need IP addresses to know where to transmit data.[66] IPs serve as the address used for the transmission of data packets over a network working with IP protocol.[67] Search engines also need IP addresses to detect "click fraud."[68] Because advertisers usually pay a search engine each time a different person views their ad, search engines need to provide advertisers with correct billing information to ensure that attackers are not racking up costs by systematically clicking on advertisements.[69] Search engines also utilize the information in log files to improve the quality of their searches, results, and advertisements.[70] Based on the user's log history of past search queries, search tendencies, and geographic data, search engines can—in theory—provide relevant personalized advertising.[71] In addition, IPs may be helpful in locating places in networks where there is too much latency or delay in response to a search query.[72]

Search engines have a great interest in collecting and retaining IP addresses, along with other information contained in log files. The

---

[66] Nadeem Unuth, *IP Addresses– What is an IP Address: IP Addresses, Their Meaning, Importance, Use and Assignment*, ABOUT.COM, http://voip.about.com/od/voipbasics/a/IPAddress.htm (last visited Jan. 27, 2009).

[67] *Id.*

[68] *Opinion 1/2008, supra* note 6, at 15.

[69] *Id.* Because Google's and other search engines' revenues are based on their advertising, these companies have a great interest in preventing click-fraud. "[IP addresses are] very helpful in helping to prevent fraud. For example, examining an IP address usually tells us which ISP that person is using. It is easy for people on most home Internet connections to get a new IP address by simply rebooting their DSL or cable modem. However, that new IP address will still be registered to their ISP, so additional ad clicks from that machine will still have something in common. Seeing an abnormally high number of clicks on a single publisher from the same ISP isn't necessarily proof of fraud, but it does look suspicious and raises a flag for us to investigate." Posting of Shuman Ghosemajumder to The Official Google Blog, http://googleblog.blogspot.com/2008/03/using-data-to-help-prevent-fraud.html (Mar. 18, 2008).

[70] *Opinion 1/2008, supra* note 6, at 15–16.

[71] *Id.* at 16.

[72] James Fallows, *Tinfoil Underwear*, THE ATLANTIC, May 2006, *available at* http://www.theatlantic.com/doc/200605/internet-privacy. Some search engines have also proffered that log files may be helpful in protecting systems from security threats by detecting abnormal behavior. *Opinion 1/2008, supra* note 6, at 15.

quality of their services and their resultant profitability may depend on such information. However, it is important for search engines to strike a balance between their legitimate business needs and the protection of their customers' personal data.[73] The concern with using IPs and other log information is that such an extensive collection of search histories may invade a person's privacy.[74] As the Working Party explained, an individual's search history may contain a "footprint on that person's interests, relations, and intentions."[75] Using the information stored in log files, a search engine may be able to link different requests and search sessions originating from a single IP address, making it possible to track and correlate any Web search originating from that address.[76] The chances of identification improve when the information deriving from the user's IP address is linked with the information from the user's unique ID cookie.[77] This may be especially problematic if a website has a large database containing PII or if a website is not entirely transparent with how it processes data.[78]

In most cases, a website's information, standing alone, will not be sufficient to directly identify a user, but the chances of identification may be improved with the assistance of a third party, such as the manager of a Local Area Network,[79] an ISP,[80] or the Domain Name

---

[73] *Opinion 1/2008, supra* note 6, at 4.

[74] *Id.* at 7.

[75] *Id.*

[76] *Id.* at 6.

[77] When a computer has a dynamic and variable IP address, and cookies are not erased at the end of a session, a unique ID cookie makes it possible to trace the user from one IP address to the next. In other words, this cookie will not change when the IP address is modified. *Id.* at 6–7.

[78] *Id.* at 21.

[79] "In this case, [the manager] will probably use a fixed IP addressing scheme and keep a list of correspondence between people's computers and IP addresses. If this person is using the *Dynamic Host Configuration Protocol* ("DHCP"), the *DHCP* program will typically keep a logbook containing the Ethernet card number. This unique world-wide number identifies a particular computer in the LAN." *Privacy on the Internet– An Integrated EU Approach, supra* note 37, at 9.

[80] "In this case, the ISP will typically keep a log file with the allocated IP address, subscriber's ID, date, time and duration of the address allocation. Furthermore, if the Internet user is using a public telecommunications network (mobile or terrestrial phone), the number called (and date, time and duration) will be registered by the phone company for billing purposes." *Id.*

Holder.[81] Using a publicly available search tool like RIPE Database Search,[82] it is possible to identify the party responsible for a particular IP address allocation.[83] The ISPs "normally systematically 'log' in a file the date, time, duration and dynamic IP address given to the Internet user" and have other information about their customers, such as names, addresses, and phone numbers.[84] These ISPs are generally prohibited from disclosing information about a customer to a third party without customer consent, and the use and retention of such information is restricted to the purpose for which it was collected.[85] Through a court order, though, ISPs may be forced to disclose this information.[86] The identity of an individual may also be uncovered with the "assistance" of other third parties, such as law enforcement agencies or national security authorities.[87] Many of these concerns were echoed in the Working Party's WP 148.

V. WORKING PARTY: "IP ADDRESSES ARE PERSONAL DATA"

In WP 148, *Opinion 1/2008 on Data Protection Issues Related to Search Engines*, the Working Party concluded that both IP addresses and cookies containing a unique ID qualify as personal data.[88] The

---

[81] "The Domain Name Holder which [may] be a company's name, the name of the employee of a company or a private citizen." *Id.*

[82] RIPE NCC Database Search, http://www.ripe.net/cgi-bin/whois (last visited Jan. 27, 2009).

[83] *Privacy on the Internet– An Integrated EU Approach*, *supra* note 37, at 9.

[84] *Id.* at 21.

[85] *See generally*, 47 U.S.C. § 551 (2006) (federal statute that details the protection of cable subscriber privacy).

[86] *See* Arista Records LLC et al. v. John Does, 551 F. Supp. 2d 1 (D.D.C. 2007) (copyright infringement action where district court subpoenaed third party ISP to obtain defendant's name, current and permanent address, telephone numbers, e-mail addresses, and media access control addresses to allow the suit to proceed).

[87] *Opinion 1/2008*, *supra* note 6, at 9.

[88] The *Opinion* states that, "[w]hen a cookie contains a unique user ID, this ID is clearly personal data. The use of persistent cookies or similar devices with a unique user ID allows tracking of users of a certain computer even when dynamic IP addresses are used. The behavioural data that is generated through the use of these devices allows focusing even more on the personal characteristics of the individual concerned." *Id.* at 9.

Working Party stated that unless an ISP is absolutely certain that the data corresponding to a user cannot be identified, all IP addresses should be treated as personal data to be on the "safe side."[89] Having determined that IP addresses and unique ID cookies do qualify as "personal data,"[90] the Working Party further concluded that search engines qualify as "processors" and "controllers" under the Directive.[91] As a result, if the Working Party's findings are adopted by the E.U. Member States, search engines would then have to process IP addresses "fairly and lawfully" and make sure that the data is only "collected for specified, explicit and legitimate purposes and not . . . processed for purposes incompatible with the purposes for which they were originally collected."[92] The processing of IP addresses would have to be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed."[93]

Among its other findings, the Working Party stated that a retention period of personal data for over one year is longer than necessary, and that the period should be reduced to six months in order "to improve transparency, to ensure fair processing, and to guarantee proportionality with the purpose that justifies such retention."[94] If providers retain personal data for longer than six months, the Working Party concluded the providers should "demonstrate comprehensively that it is strictly necessary for the service."[95] The Working Party also noted that once there is no longer a legitimate purpose for using the data, it must be deleted or made irreversibly anonymous.[96] While companies like Yahoo, Google, Microsoft, and Ask.com have all taken measures to make their IPs and

---

[89] *Id.* at 8.

[90] *Id.* at 9.

[91] Council Directive No. 95/46/, *supra* note 4.

[92] *Id.* at 15.

[93] *Id.*

[94] *Opinion 1/2008, supra* note 6, at 19.

[95] *Id.*

[96] *Id.* at 20.

cookies unreadable,[97] the Working Party suggests that these measures may not be enough:

> [A]nonymisation of data should exclude any possibility of individuals to be identified . . . . Currently, some search engine providers truncate IPv4 addresses by removing the final octet, thus in effect retaining information about the user's ISP or subnet, but not directly identifying the individual. The activity could then originate from any of 254 IP addresses. This may not always be enough to guarantee anonymisation.[98]

But perhaps the question should not be what will happen when the E.U. Member States adopt the Working Party's findings but rather *if* they will adopt them. In September 2008, a district court in Munich, Germany held that—despite the conclusions set forth in WP 148—dynamic IP addresses do not qualify as personal data.[99] The court held that dynamic IPs lack the necessary quality of "determinability"

---

[97] In December 2008, Yahoo announced it would anonymize the IP addresses it stores after three months by erasing the last few numbers in the IP address. This change gave Yahoo the lowest retention rate among its peers at that time. Kim Dixon, *Yahoo Cuts Data Retention to Three Months*, REUTERS, Dec. 17, 2008, http://www.reuters.com/article/technologyNews/idUSTRE4BG2VP20081217. Google anonymizes its IP addresses after nine months, also by erasing the last few numbers of the address. Another step to protect user privacy, Posting of Peter Fleischer, Jane Horvath & Alma Whitten to The Official Google Blog, http://googleblog.blogspot.com/2008/09/another-step-to-protect-user-privacy.html (Sept. 8, 2008). Microsoft anonymizes after eighteen months, but does so by permanently removing cookie IDs, the entire IP address, and other identifiers from search terms. This contrasts with Yahoo and Google's stance; both companies only anonymize IP addresses by erasing the last few numbers of the IP address. *Microsoft Announces Enhanced Privacy Protections for Customers*, July 22, 2007, http://www.microsoft.com/presspass/press/2007/jul07/07-22EnhancedPrivacyPrinciplesPR.mspx. Ask.com released AskEraser in 2007. This program allows all search activities to be deleted from Ask.com servers "within hours," opposed to the normal eighteen months. Ask.com asserts that the new search tool "will offer its searchers unmatched control over their privacy." Press Release, Ask.com, Ask.com to Give People Unmatched Privacy Control (July 19, 2007), *available at* http://www.ircconnect.com/askj/pages/news_releases.html?d=123324.

[98] *Opinion 1/2008*, *supra* note 6, at 20.

[99] *D: Court Declares IP Addresses are Non-Personal Data*, 2B ADVICE: THE PRIVACY BENCHMARK, Oct. 16, 2008, http://www.2b-advice.com/no_cache/service/meldungen/2b/news/2008/11/24/d-court-declares-ip-addresses-are-non-personal-data.html.

to be personal data.[100] According to the court, "[d]eterminability requires among others that the responsible party is able to identify the person behind a single data with the knowledge and utilities he normally has available."[101] Because ISPs are not legally permitted to hand over the information identifying an individual, the court opined that a potential illegal handover would not match the determinability requirement.[102] Interestingly, this decision conflicted with earlier decisions from another Berlin district court and a Berlin appellate court.[103] Both of these courts held that IP addresses are personal data and that the determinability requirement should not only account for legal means of transmission, but should also account for illegal means.[104]

Since the Directive does not apply to search engines outside of the European Union, search engines will not be forced to alter their operations in the United States.[105] As stated earlier, in the United States, search engines would essentially only be required to follow the promises laid out in their privacy policies. They may have to deal with additional pressure from public interest groups, such as EPIC, which

---

[100] *Id.*

[101] *Id.*

[102] *Id.*

[103] *Id.*

[104] *Id.* In 2007, the Paris Appeal Court handed down two separate decisions, concluding in both cases that the processing of IP addresses does not constitute a processing of personal data because the identifying numbers only relate to a machine, and not the individual behind the machine. Meryem Marzouki, *Is the IP Address Still a Personal Data in France?*, EUROPEAN DIGITAL RIGHTS, Sept. 12, 2007, http://www.edri.org/edrigram/number5.17/ip-personal-data-fr. In November 2008, at an information security conference in London, the European Union's Data Protection Supervisor, Peter Hustinx, disagreed with the September 2008 Munich decision, and sided with the Berlin decisions. He said that for IP addresses to count as personal data there was no requirement that the processing company know the name of the individual whose activity it was monitoring. "Identifiable in the sense of the word personal data is singling someone out. We do not need to know someone's birth date, address, surname, first name etc. . . . So if we deal with a computer, an IP address, which is showing special behaviour in terms of the transactions we can follow, then in a reasonable world that is individuals. Computers do not do this alone, this is individuals using this." *Hustinx: Nameless Data Can Still be Personal*, OUT-LAW.COM, Nov. 6, 2008, http://www.out-law.com/page-9563.

[105] Nate Anderson, *Google Argues Against Calling IP Addresses "Personal Data,"* ARS TECHNICA, Feb. 22, 2008, http://arstechnica.com/news.ars/post/20080222-google-no-black-and-white-regulation-of-ip-addresses.html.

have on occasion been successful in bringing about changes in company behavior.[106] However, this type of pressure has ordinarily been resolved on a case-by-case basis, rather than through the enactment of sweeping regulation. Therefore, absent Congress passing its own comprehensive privacy legislation, the only way that all search engines would be forced to treat IPs as PII in this self-regulating atmosphere would be if every search engine were to voluntarily agree to treat them as so. This seems unlikely—at least in the immediate future—due to the economic advantages that IP addresses provide search engines, as mentioned in Part III. Nonetheless, the debate over how IPs should be classified carries on, in both the United States and in the European Union.

VI. THE DEBATE: IS IT PERSONAL?

The debate of whether IP addresses should be included in the definition of PII is ongoing, and there is a great deal of expert opinion on both sides of the matter. Dr. Patrick Ho, the Secretary for Home Affairs in Hong Kong, has argued that IPs should not be considered personal data under Hong Kong's Personal Data Privacy Ordinance ("PDPO")[107]:

> [T]he exact location of a computer or the identity of a computer user cannot be traced using an IP address alone. To trace an account user . . . one must have the IP address, the time of use of the IP address and the appropriate IP assignment logs kept by the ISPs. The provisions of the PDPO together with the relevant license conditions in the [telecommunication] license

---

[106] For example, in 2000, EPIC filed a complaint with the FTC concerning the information collection practices of DoubleClick, a third party advertising network. The allegation stated that DoubleClick was, without the consent of its users, planning to correlate its online non-PII database with the recently-acquired AbacusDirect's offline PII databases. After the FTC opened its investigation on the matter, DoubleClick admitted its plans to match up such information, and subsequently agreed to withdraw from such plans and henceforth, entered into a self-regulatory program called the Network Advertising Initiative. In re DoubleClick Inc., Complaint and Request for Injunction, Request for Investigation and for Other Relief, before the Federal Trade Commission (Feb. 10, 2007), *available at* http://www.techlawjournal.com/privacy/20000210com.htm.

[107] *See* Press Release, Hong Kong Home Affairs Bureau, IP Addresses as Personal Data (May 3, 2006), *available at* http://www.info.gov.hk/gia/general/200605/03/P200605030211.htm.

> issued to ISPs should therefore be sufficient to prohibit the unauthorized disclosure of information collected by ISPs.[108]

Peter Fleischer, Global Privacy Counsel for Google, agrees with Dr. Ho. Because ISPs are prohibited from providing information to third parties, Fleischer argues that it is not pragmatically possible to identify users.[109] Fleischer states on his blog that "surely, illegal means are not 'reasonable' means in the terms of the Directive."[110] Even assuming that such a prohibition did not exist, Fleischer proffers that, "the ISP can only identify the account holder, not the person who was actually using the computer at any given time . . . . That means that if there are multiple people, like a family, logging into the same account, only the account holder's name is associated with the IP Address."[111] Google supported this notion in its response to Representative Barton's questionnaire:

> When an individual is not authenticated, we do not consider an IP address to be personally identifiable because we would need to get specific data from an ISP about which of its customers was using a particular IP address at a particular time on a particular day in order to link it to an individual. Even then, you could not say which member of a household was online at a particular time.[112]

---

[108] *Id.*

[109] Posting of Peter Fleischer to Peter Fleischer: Privacy. . . ? blog, http://peterfleischer.blogspot.com/2008/02/can-website-identify-user-based-on-ip.html (Feb. 15, 2008, 16:49 EST).

[110] *Id.*

[111] *Id.*

[112] Letter from Alan Davidson to Joe Barton, *supra* note 21, at 13. In Google's lawsuit with Viacom in which Viacom moved to compel YouTube and Google to produce certain electronically stored data, such as user's IP address, Google argued that such data should not be disclosed because of the users' privacy concerns. "Plaintiffs would likely be able to determine the viewing and video uploading habits of YouTube's users based on the user's login ID and the user's IP address." Viacom Int'l v. YouTube, No. 07-2103, slip op. at 13 (S.D.N.Y. July 1, 2008), *available at* http://docs.justia.com/cases/federal/district-courts/new-york/nysdce/1:2007cv02103/302164/117/.

Proponents argue that because IPs may be used to infer identity, they should be categorized as PII. Even though IP addresses are not a traditional type of PII, they still have the potential to disclose one's identity.[113] Ari Schwartz, deputy director of the Center for Democracy and Technology ("CDT"), believes that, "[c]ompanies that deal in search results have to understand that they carry very sensitive information, even if it doesn't have what we would traditionally consider to be personally identifiable information involved." [114] Schwartz's comments were made in response to AOL's 2006 public disclosure of the IP addresses of 658,000 users on a research area of its website.[115] In a report released in August 2007 about the privacy policies of search engines, CDT stated that, "depending on the circumstances, these data elements [search query, IP address, and cookies], alone or in combination with other information, have the potential to identify individual users."[116] CDT proved correct when *The New York Times* revealed that it was able to match some of the released AOL search records to the identity of individuals.[117]

Marc Rotenberg of EPIC also believes that identity can be inferred from an IP address; he believes that an IP address can be linked to an individual with little effort, even if a name or address is not associated with the IP number.[118] In a prepared statement before the European Parliament in January 2008, regarding Google's acquisition of DoubleClick, Rotenberg recommended that Google cease its storage of

---

[113] Dawn Kawamoto & Elinor Mills, *AOL Apologizes for Release of User Search Data*, CNET NEWS, Aug. 7, 2006, http://www.news.com/AOL-apologizes-for-release-of-user-search-data/2100-1030_3-6102793.html.

[114] *Id.*

[115] *Id.*

[116] CTR. FOR DEMOCRACY AND TECH., SEARCH PRIVACY PRACTICES: A WORK IN PROGRESS 1 (2007), http://www.cdt.org/privacy/20070808searchprivacy.pdf.

[117] Stefanie Olsen, *Google Draws Privacy Complaint to FTC*, CNET NEWS, Apr. 20, 2007, http://www.news.com/2100-1024_3-6177819.html. Among some of the search terms linked up to one IP address were terms such as "how to tell your family you're a victim of incest," "casey middle school," "surgical help for depression," "can you adopt after a suicide attempt," "Fishman David Dr - 2.6 miles NE - 160 E 34th St, New York, 10016 - (212) 731-5345," "gynecology oncologists in new york city," and "how long will the swelling last after my tummy tuck." Kawamoto & Mills, *supra* note 113.

[118] Olsen, *supra* note 117.

IP addresses because the practice could be used to identify users.[119] Similarly, Germany's data commissioner, Peter Schaar, told the European Parliament that while IPs may not always be linked to a particular individual, he considers these cases exceptions to the general rule that IPs must be regarded as personal data.[120]

Even Peter Fleischer of Google acknowledges that, in some instances, an IP address may be personally identifiable[121]: "[T]here is no black or white answer: sometimes an IP address can be considered as personal data and sometimes not, it depends on the context, and which personal information it reveals."[122] As stated in Section III above, there are indeed ways in which ISP information may be obtained from third parties, despite the prohibition against ISPs sharing this information. For example, one could imagine a scenario in which an ISP and a search engine were part of the same company, and thus, the prohibition against sharing information would not apply. In this scenario, the company could identify the user by "cross-indexing" among its own databases. [123] The United Kingdom's

---

[119] Marc Rotenberg, President, Elec. Privacy Info. Ctr., Address Before the European Parliament and LIBE Comm.: Data Protection and Search Engines on the Internet 7 (Jan. 21, 2008), epic.org/privacy/ftc/google/EPIC_LIBE_Submission.pdf.

[120] Aoife White, *EU Official Says IP Address is Personal*, MSNBC.COM, Jan. 21, 2008, http://www.msnbc.msn.com/id/22770682.

[121] Fleisher suggests certain factors that should be considered in determining whether information is personal data: how that data could be matched with publicly available information; analyzing the statistical chances of identification in doing so; the chances of the information being disclosed and being matched with other data likely held by a third party; the likelihood that "identifying" information may come into their hands in future, perhaps through the launch of a new service that seeks to collect additional data on individuals; the likelihood that data matching leading to identification may be made through the intervention of a law enforcement agency; and whether the organization has made legally binding commitments (either through contract or through their privacy notice) to not make the data identifiable. Posting of Peter Fleischer to Peter Fleischer: Privacy. . . ? blog, http://peterfleischer.blogspot.com/2007/02/are-ip-addresses-personal-data.html (Feb. 5, 2007, 17:18 EST).

[122] *Do Internet Companies Protect Personal Data Well Enough?*, NEW EUROPE, Jan. 26, 2008, www.neurope.eu/articles/82144.php.

[123] In her lone dissenting vote in the FTC's decision to approve Google's acquisition of DoubleClick, FTC Commissioner Pamela Harbour voiced a similar concern: "[p]ost-merger, a user would visit one or more sites displaying DoubleClick ads, and also conduct one or more Google searches, during a time period when the IP address remained the same .... The merged firm would be able to use the common IP address to link the Google and DoubleClick cookies on that machine, and thereby cross-index that user among both databases– without relying on any proprietary customer data. And once the cookies

Information Commissioner[124] supports this moderate stance as well, distinguishing between dynamic and static addresses[125]:

> [I]f it is only the ISP who can link the IP address to an individual it is difficult to see how the [UK's Data Protection] Act can cover collecting dynamic IP addresses without any other identifying or distinguishing information. Some IP addresses are 'static,' and . . . they can be linked to a particular computer which may then be linked to an individual user. Where a link is established and profiles are created based on static IP addresses, the addresses and the profiles would be personal information and covered by the Act.[126]

Saul Hansell of *The New York Times* likens logging IP addresses to taking pictures with a security camera.[127] Just as a security camera videotape cannot itself divulge the names or identities of any of the people on the recording, an IP address cannot identify a user without additional data from ISPs.[128] Hansell acknowledges that, "recording makes it much easier to gather that information and find out who is

---

themselves were linked in the merged firm's dataset, it would not matter if the user's IP address changed in the future." In re Google/DoubleClick, Fed. Trade Comm'n File No. 071-0170, at n.22 (2007) (Harbour, P., dissenting), http://www.ftc.gov/os/caselist/0710170/071220harbour.pdf.

[124] According to its website, the U.K. Information Commissioner's Office is the U.K.'s independent authority set up to promote access to official information and to protect personal information. ICO: Information Commissioner's Office, http://www.ico.gov.uk (last visited Jan. 27, 2009).

[125] INFO. COMM'R OFFICE, DATA PROTECTION GOOD PRACTICE NOTE: COLLECTING PERSONAL INFORMATION USING WEBSITES, http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/collecting_personal_information_from_websites_v1.0.pdf (last visited Jan. 27, 2009).

[126] *Id.* The U.K. Information Commissioner points out that "it is not easy to distinguish between dynamic and static IP addresses, so there is limited scope for using them for personalised profiling."

[127] Saul Hansell, *I.P. Address: Partially Personal Information*, N.Y. TIMES, Feb. 24, 2008, http://bits.blogs.nytimes.com/2008/02/24/ip-address-partially-personal-information.

[128] *Id.*

shopping."[129] He proposes that a new category of information be created, called "partially personal information," which he describes as "bits of data that can be personal under certain circumstances."[130] Peter Fleischer also supports a more nuanced approach to defining PII that would "move from the current legal model (a black/white model–either PII or not) to a newer model, a sort of slope based on a 'privacy risk rating.'"[131] He argues that the E.U. Directive's definition of personal data is too broad, and calls for an approach that categorizes the data based on how practically identifiable the information may be.[132] This privacy risk rating system could be something privacy regimes consider in the future, but for now the status quo system of "PII" or "non-PII" remains.

VII. CONCLUSION

While the Article 29 Data Protection Working Party has determined that IP addresses are personal data and that search engines are processors and controllers of that data, it remains to be seen if the Member States will adopt the Working Party's stance; even if they do, it is unclear how the quality of their searches or advertisements will be affected in these States. Likewise, it is unclear if the Working Party's *Opinion* will affect how search engines operate in the United States. In the meantime, companies like Yahoo, Google, Microsoft, and Ask.com continue to pile up information about their customers. Some types of information may have little or no consequences, while other types may have the potential to identify a user. Some types of information—such as IP addresses—fall into a gray area; some people believe they are personally identifiable, while others disagree. Ultimately, resolving the debate over the

---

[129] *Id.*

[130] *Id.*

[131] Posting of Peter Fleischer to Peter Fleischer: Privacy. . . ? blog, *supra* note 121.

[132] Fleischer states that, "[p]ersonal data is very broadly defined in Article 2 of the Directive . . . . Where this definition is applied unqualified then it may be interpreted in such a way that data will remain 'personal' and subject to the full remit of the law if individuals remain in any way identifiable. We believe that the concept of personal data should rather be defined pragmatically, based upon the likelihood of identification. In our view, it should not be the case that an organisation has to be sure that there is no conceivable method, however unlikely in reality, by which the identity of individuals can be established. This is a highly impractical approach." *Id.*

classification of IPs will depend on how search engines and regulators define terms like "reasonably linked" and "identifiable person." For now, at least, the question remains: Are IP addresses "personally identifiable information"?

APPENDIX: SELECTED DEFINITIONS OF "PERSONAL INFORMATION" IN U.S. LAWS

The Children's Online Privacy Protection Act of 1998
"Personal information" means individually identifiable information about an individual collected online, including– (A) a first and last name; (B) a home or other physical address including street name and name of a city or town; (C) an e-mail address; (D) a telephone number; (E) a Social Security number; (F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or (G) information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph.[133]

Drivers Privacy Protection Act
"Personal Information" means information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the five-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status.[134]

Fair Credit Reporting Act
"Consumer report" means any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under section 604.[135]

Gramm-Leach Bliley Act
"Nonpublic personal information" means personally identifiable financial information– (i) provided by a consumer to a financial

---

[133] 15 U.S.C. § 6501(8) (2006).

[134] 18 U.S.C. § 2725(3) (2006).

[135] 15 U.S.C. § 1681(d)(1) (2006).

institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution.[136]

Health Information Portability and Accountability Act
"Health information" means any information, whether oral or recorded in any form or medium, that– (A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.[137]

Right to Financial Privacy Act
"Financial records" means an original of, a copy of, or information known to have been derived from, any record held by a financial institution pertaining to a customer's relationship with the financial institution.[138]

Video Privacy Protection Act
"Personally identifiable information" includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider.[139]

---

[136] 15 U.S.C. § 6809(4) (2006).

[137] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

[138] 12 U.S.C. § 3401(2) (2006).

[139] 18 U.S.C. § 2710(3) (2006).