DEMYSTIFYING CLICKSTREAM DATA: A EUROPEAN AND U.S. PERSPECTIVE

Daniel B. Garrie[*]
Rebecca Wong[**]

---

[*] Mr. Garrie is a founding and managing member of LegalTech Group. He has been admitted to practice law in both New York and New Jersey. Mr. Garrie graduated from Rutgers University School of Law with a focus in Cyber Law Litigation. He holds an M.A. and B.A. in Computer Science from Brandeis University. He is the recipient of several competitive awards and scholarships, and author of over 20 published law review articles on technology law. Currently, he serves as Editor-in-Chief of the Journal of Legal Technology Risk Management, a world renowned journal examining the complex issues of global regulatory compliance. Mr. Garrie combines both his decade plus work experience in technology with the leading emerging issues in technology law. Over the past decade Mr. Garrie has worked on four continents with large companies and government agencies, including: the Department of Justice, WestpacTrust Bank (Australia/NZ), Bank of Paris (in Argentina), ClickIT Solutions (Siemens spin-off in Argentina), Department of Homeland Security, Sleep Solutions (J&J), Schlumberger, AIG, Brandeis University, Captiva Software (bought by IBM), and Exigen Group (in Australia). Prior to co-founding LegalTech Group, Mr. Garrie founded and sold D&D Network Design, a firm specializing in delivering complex international web enterprise applications focusing on Web Sphere and Microsoft.Net platforms. Today, he also serves as an advisor to several Internet technology startups worldwide.

Daniel B. Garrie would like to thank his mother Erica Garrie and Dean Camille Andrews at Rutgers School of Law for her support and guidance.

[**] Rebecca Wong is Senior Lecturer in Law at Nottingham Law School, Nottingham Trent University with teaching and research interests in Data Protection Laws, Cyberlaw, Intellectual Property, and Tort. She has recently completed her PhD at University of Sheffield in data protection law, examining the adequacy of the European data protection framework principally through the Data Protection Directive 95/46/EC and the Directive on Privacy and Electronic Communications 2002/58/EC within the online environment. Her recent works have included participating in a European Commission project, PRIVIREAL, which examined the implementation of the Data Protection Directive 95/46/EC in relation to medical research and the role of ethics committees co-ordinated by Professor Deryck Beyleveld and David Townend. She is the author of *Privacy: charting its developments and prospects*, a chapter published in the *Human Rights in the Digital Age* (2005) and *Data Protection Online: Alternative approaches to sensitive data* (2007). She is currently editing a special issue on "Identity, Privacy and New Technologies," to be published in *International Journal of Intellectual Property Management*, 2008.

Rebecca Wong would like to dedicate this article to Professor Deryck Beyleveld at Durham University and Professor Roger Brownsword at Kings College, London for their support and guidance throughout, a debt that is long overdue.

Many thanks also to Ryan Lewis for his assistance in penning and editing this article; Mr. Lewis graduated from Brown University with Honors and is currently working in New York City in the field of technology compliant solutions for major corporations. The authors also wish to thank the Emory International Law Review Editorial Board for their editorial assistance. We greatly appreciate their hard work and dedication and have enjoyed working with them during the course of this Article.

INTRODUCTION

There has been much literature written on the subject of clickstream data.[1] However, very little has been discussed over the extent to which clickstream data is considered as "personal data" under European and U.S. law.[2] This Article considers the current European Union (EU) regulations governing clickstream data by examining the European Data Protection Directive 95/46/EC (DPD)[3] and the Directive on Privacy and Electronic Communications 2002/58/EC (DPEC),[4] comparing these laws with the U.S. legal framework. In particular, this Article discusses the broad application of the DPD under Article 4 and the notion of "personal data" as defined under Article 2(a).[5] The implications of the DPD should not be underestimated because the DPD can have overreaching effects by applying to companies or organizations operating outside the European Economic Area ("EEA"), principally through Article 4(1)(c).[6] In addition, this Article surveys the applicable clickstream statutory regulatory frameworks by reviewing Title III of the 1968 Omnibus Crime Control and Safe Streets Act ("Wiretap Act") and its progeny.[7] This Article takes a critical approach to clickstream data by

---

[1] *See, e.g.*, DANIEL J. SOLOVE, THE DIGITAL PERSON 23–24 (2004) (discussing the practice of websites that collect personal information from users, enabling them to target their advertising); Lee Kovarsky, *Tolls on the Information Superhighway: Entitlement Defaults for Clickstream Data*, 89 VA. L. REV. 1037, 1070–1978 (2003) (discussing the lack of statutory remedies to redress the injury caused by companies invading personal privacy); Gavin Skok, *Establishing a Legitimate Expectation of Privacy in Clickstream Data*, 6 MICH. TELECOMM. & TECH. L. REV. 61, 66–67 (2000) (stating that companies compile personal data to obtain information about consumer preferences).

[2] *See* LEE A. BYGRAVE, DATA PROTECTION LAW: APPROACHING ITS RATIONALE, LOGIC AND LIMITS 316–18 (2002) (stating that the EC Directive and other data protection laws do not conclusively define what is considered 'personal data' in clickstream data).

[3] Council Directive 95/46/EC, Protection of Individuals with Regard to the Processing of Personal Data, 1995 O.J. (L 281) 31 (EC) [hereinafter DPD].

[4] Council Directive 2002/58/EC, Directive on Privacy and Electronic Communications, 2002 O.J. (L 201) 37 (EC) [hereinafter DPEC].

[5] Article 2(a) defines personal data as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one 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." DPD, *supra* note 3, art. 2.

[6] *Id.* art. 4(1)(c); *see also* BYGRAVE, *supra* note 2, at 14 (stating that instruments such as the EC Directive are significant because they shape the data protection laws of many different jurisdictions).

[7] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 212 (1968) (codified as amended at 18 U.S.C. §§ 2510-2522 (2006)). The Electronic Communications Privacy Act of 1986 amended Title III to extend its wire tap restrictions over telephone communications to include communications transmitted by electronic data. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

considering the current EU and U.S. regulatory frameworks for clickstream data and by analyzing the extent to which such data is protected.

I. WHAT IS CLICKSTEAM DATA?

The first question is what is clickstream data?[8] Clickstream data is defined as "the generic name given to the information a website can know about a user simply because the user has browsed the site."[9] Clickstream data is compiled from cookie based technology,[10] which websites began using in the mid-1990s.[11] Cookies are information packets transmitted from a server to an end-user's web browser and that are then retransmitted back to the server each time the browser accesses a server's webpage.[12] Cookies store information used for authentication, identification, or registration of an end-user to a web site, thereby enabling the end-user's web browser to maintain a relationship between the server and the end-user.[13] The use of cookie based technology enables companies to deliver user-specific solutions for each machine that accesses their web pages by placing electronic markers on end-user

---

[8] Portions of this section have been substantially reprinted from Daniel B. Garrie, *The Legal Status of* Software, 23 J. MARSHALL J. COMPUTER & INFO. L. 711, 732–35 (2005) [hereinafter Garrie, *Legal Status*] and Daniel B. Garrie, Matthew J. Armstrong & Donald. P. Harris, *Voice Over Internet Protocol and the Wiretap Act: Is Your Conversation Protected?*, 29 SEATTLE U. L. REV. 97, 108–11 (2005) [hereinafter Garrie, *Voice Over*].

[9] Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1085, 1104 (2002). This information includes a user's detailed browsing activity and TCP/IP address, which can be used to discover personal information about the user. *Id.* Once a user has accessed a website that uses cookie technology or an affiliated site, the embedded cookie on the hard drive begins collecting data about the user's web activities. Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1155 (W.D. Wash. 2001). There are three reported cases in which cookie technology was used by a website to mine personal information from the user's machine: *Chance*, 165 F. Supp. 2d at 1155, *In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 502–03 (S.D.N.Y. 2001), and *In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 12 (1st Cir. 2003).

[10] Kovarsky, *supra* note 1, at 1045–46.

[11] *See In re DoubleClick, Inc.*, 154 F. Supp. 2d at 502–03 ("Cookies are computer programs commonly used by Web sites to store useful information . . . .").

[12] *See* Rachel K. Zimmerman, Note, *The Way the "Cookies" Crumble: Internet Privacy and Data Protection in the Twenty-First Century*, 4 N.Y.U. J. LEGIS. & PUBL. POL'Y 439, 440 (2000–2001).

[13] *See generally* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1458–60 (2001); Lawrence Jenab, Comment, *Will the Cookie Crumble?: An Analysis of Internet Privacy Regulatory Schemes Proposed in the 106th Congress*, 49 KAN. L. REV. 641, 667–68 (2001); Zimmerman, *supra* note 12.

machines.[14] Collectively these cookie-driven markers create a trail of information commonly referred to as "clickstream data."[15]

Clickstream data and cookies can be found in most Internet driven commerce contexts, including those involving the employer-employee workplace and the Internet Service Provider (ISP)/online company and its users, particularly in the context of interactive marketing.

In its infancy, clickstream data was used to garner basic information from a web user,[16] such as the type of computer an individual used to access the Internet, the type of Internet browser utilized, or the identification of each site or page visited.[17]

As technology evolved, however, so did the scope of data encompassed by clickstream data.[18] For instance, today, when an individual discloses certain information during a visit to a website via his or her Personal Digital Assistant, cell phone, Blackberry, laptop computer, iPod, or desktop computer, it is possible that the website will be collecting clickstream data of a much more personal nature.[19] Clickstream data is used in part because web server technologies cannot store, sort, and render to a user the vast amounts of data required to deliver the respective web solutions to each individual user to a site or to authenticate a user.[20] Thus, such websites can off-load information to the

---

[14] *See* Jerry Berman & Deirdre Mulligan, *Privacy in the Digital Age: Work in Progress*, 23 NOVA L. REV. 551, 554 (1999).

[15] Once a user has accessed a web site that uses cookie technology or an affiliated site, the embedded cookie on the hard drive begins collecting data about the user's web activities.

[16] *See* Berman & Mulligan, *supra* note 14, at 559 (noting that cookies were designed for the benign purpose of enabling websites to recognize repeat visitors).

[17] *See* Karen Dearne, *You are Being Monitored Online*, THE AUSTRALIAN, Sept. 24, 2002, at 31; Fusun Feride Gonul, *Stereotyping Bites the Dust; Marketers No Longer Focusing On Demographic Profiling*, PITT. POST-GAZETTE (Pa.), Feb. 26, 2002, at B3.

[18] *See* Lin, *supra* note 9, at 1104–05 (defining clickstream data as a trail of information that a user leaves behind while browsing on the Web); *see generally* Jane Kaufman Winn & James R. Wrathall, *Who Owns the Consumer? The Emerging Law of Commercial Transactions in Electronic Customer Data*, 56 BUS. LAW. 213, 234–35 (2000) (stating that the use of cookies is no longer limited to tracking movements on a single website, but has expanded to tracking site to site movement); Herbert A. Edelstein, *Pan for Gold in the Clickstream*, INFORMATIONWEEK, Mar. 12, 2001, at 77 (stating that by analyzing the tracks people make through a company's website, the company is able to retrieve information about their customers' purchasing habits).

[19] *See In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 15 (1st Cir. 2003) (information collected by defendant included email addresses, insurance statuses, education levels, medical conditions, and other sensitive information stored by computers).

[20] *See generally* R. A. MOELLER, DISTRIBUTED DATA WAREHOUSING USING WEB TECHNOLOGY: HOW TO BUILD A MORE COST-EFFECTIVE AND FLEXIBLE WAREHOUSE (2001).

user's device where it is stored in text files called "cookies."[21] These cookies provide the website a mechanism that is able to collect or store data on the user's machine,[22] thereby enabling the web site to record, track, monitor, and deliver dynamic content reflective of the data points stored on their machine.[23]

The data mining industry and a majority of web portals and Internet companies would be severely limited, if not rendered useless, in the absence of clickstream data.[24] Internet companies currently rely heavily on tracking clickstream data to profile user preferences in order to deliver customized services and advertisements to Internet users.[25] Although it is possible for authentication processes to occur in a different manner, by requiring the users to affirmatively consent to monitoring of clickstream data, it is highly unlikely that fully informed end-users[26] would interact with sites that track, monitor, and traffic in their personally identifiable information.[27]

A. Employer/Employee Workplace

1. Europe

Software exists such that employers may monitor the web pages visited and Internet transactions executed by their employees.[28] Although the employer has unchecked monitoring privileges in the United States, any covert

---

[21] *See* MICHAEL J. A. BERRY & GORDON LINOFF, MASTERING DATA MINING: THE ART AND SCIENCE OF CUSTOMER RELATIONSHIP MANAGEMENT 479–80 (2000); Colin Shearer, *The CRISP-DM Model: The New Blueprint for Data Mining*, 5 J. DATA WAREHOUSING 4, 13–22 (2000).

[22] Once a user has accessed a web site that uses cookie technology or an affiliated site, the embedded cookie on the hard drive begins collecting data about the user's web activities. *See* Berman & Mulligan, *supra* note 14, at 559.

[23] Jenab, *supra* note 13, at 645.

[24] Elimination of clickstream data or cookies would impact such websites as: www.yahoo.com; www.google.com; www.wamu.com; www.schwab.com; www.ibm.com. Adjoining these web sites are a slew of Internet and web applications that utilize cookies and clickstream data for authentication. Elimination would impact not only businesses but also a large number of government enabled web applications. *See* The Office of the Privacy Commissioner, Guidelines for Federal and ACT Government Websites, http://www.privacy.gov.au/internet/web/ (last visited Oct. 28, 2006) (providing guidance for the many government sites that use cookies and clickstream data technology).

[25] *See In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 503–07 (S.D.N.Y. 2001); *see generally* BERRY & LINOFF, *supra* note 15; Zimmerman, *supra* note 12.

[26] *See generally* Alan F. Blakley, *Privacy: The Delicate Entanglement of Self and Other*, 3 RUTGERS J.L. & URB. POL'Y 172, 172–79 (2006).

[27] Edelstein, *supra* note 18, at 85.

[28] *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 18–19 (1999); *see generally* Julie E. Cohen, *Privacy, Ideology and Technology: A Response to Jeffrey Rosen*, 89 GEO. L.J. 2029 (2001) (discussing employer-employee monitoring in cyberspace).

monitoring by an employer would potentially violate the national data protection laws in Europe, unless employees have consented to such use.[29] In the context of European data protection law, it is arguable that employees consent reluctantly to their employer monitoring their online behavior in the economic interest of the company. As Lee Kovarsky has stated:

> That employers may monitor email and web surfing to promote productivity and protect against industrial espionage has become more of a fact of life than a controversy and employers would likely contract around any default rule to the contrary.[30]

Taking an alternative view on employee monitoring, the Article 29 Working Party, an independent advisory body tasked to provide opinions on the DPD and the DPEC, has issued some guidelines on the surveillance of electronic communications in the workplace.[31] These guidelines aim to "contribute to the uniform application of the national measures adopted under the [DPD]" in surveillance and monitoring of electronic communications in the workplace.[32] The Working Party has taken the view that *prevention* should be more important than *detection* and that the interest of the employer is better served in preventing Internet misuse, rather than detecting such misuse.[33]

These guidelines have been found to emphasize the following principles when monitoring e-mail and Internet use of employees within the borders of the EU:

- *Principle of necessity*—the monitoring in question must be necessary for a specified purpose and should not be used if there are any less intrusive methods.[34]
- *Principle of finality*—data must be collected for a specified, explicit, and legitimate purpose and not further processed in a way incompatible with those purposes.

---

[29] The Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Working Document on the Surveillance of Electronic Communications in the Workplace*, 26, 5401/01/EN/Final, WP 55 (May 29, 2002) [hereinafter *Surveillance of Electronic Communications*], *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp55_en.pdf; *see also* Donald P. Harris, Daniel B. Garrie & Matthew J. Armstrong, *Sexual Harassment: Limiting the Affirmative Defense in the Digital Workplace*, 39 U. MICH. J.L. REFORM 73, 83–87 (2005).

[30] Kovarsky, *supra* note 1, at 1043.

[31] *See generally Surveillance of Electronic Communications*, *supra* note 29, at 26.

[32] *Id.*

[33] *Id.* at 4.

[34] *Id.* at 13.

- *Principle of transparency*—the employer must be clear and open about his activities. Unless covert monitoring falls within the exemptions laid down under Article 13[35] of the DPD, such monitoring should not be permitted. This principle may also include the obligation to notify the relevant data protection authorities before personal data is processed.
- *Obligation to provide information about the data subject*—in particular, workers should be provided with a readily accessible, clear, and accurate statement of the company's policy on e-mail and Internet monitoring. Data subjects also have the right to access the personal data processed by his or her employer.
- *Principle of legitimacy*—in accordance with Article 7 of the DPD, or data protection laws transposing this provision, processing of personal data can only take place if it has a legitimate purpose.
- *Principle of proportionality*—personal data must be adequate, relevant, and not excessive with regard to achieving the purpose specified. In other words, the monitoring must be proportional to the risks entailed by the employer.
- *Accuracy and retention of data*—data stored by an employer consisting of data from or related to a worker's e-mail account or the worker's use of the Internet must be accurate and kept up to date and not kept for longer than necessary.
- *Security*—in accordance with Article 17 of DPD, employers should ensure that appropriate technical and organizational measures are in place to ensure that any personal data held by the employer is secure and safe from outside intrusion.[36]

Whilst these principles are helpful in guiding the employers over the general application of e-mail and Internet monitoring, employers and employees should nevertheless be educated about the collection of clickstream data and the ways in which it is used.

2. *U.S. Law*

The United States' courts have recognized an employer's right to monitor employees' e-mail messages and to use digital technologies to protect trade

---

[35] Exemptions provided under Article 13 of the DPD included the following areas: national security; defence; public security; the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; and the protection of the data subjects or of the rights and freedoms of others. *Id.* at 14 n.15.

[36] *Id.* at 13–18.

secrets.[37] The U.S. courts have found employees do not have an objectively reasonable expectation of privacy when their employer has an e-mail policy informing them that their e-mail or Internet use may be monitored.[38] For instance, the Fourth Circuit in *United States v. Simons* recognized that the employee has no expectation of privacy in clickstream data.[39] Essentially, U.S. courts have reasoned employers have the right to invade employees' digital work spaces because employers have legitimate interests in all communications transmitted on their digital networks.[40]

In monitoring employees, the vast majority of large employers use digital tracking technology.[41] Recently, the Washington Internet Daily released a survey finding that eighty percent of major U.S. companies record and review their employees' electronic communications or browser use.[42] Sixty-seven percent of employers have disciplined at least one employee for improper or excessive use of e-mail or Internet access; thirty-one percent have fired employees for such conduct.[43] A recent survey found that more than three-quarters of major U.S. corporations monitor employee activities, including telephone calls, e-mail, Internet communications, and computer files.[44] In addition to the employer's ability to monitor employee digital transmissions, employers may possess a high degree of control over employee computer desktops.[45] Employer control helps employee productivity by ensuring that a uniform technical environment exists.[46]

---

[37] *See* Blakey v. Cont'l Airlines, Inc., 751 A.2d 538, 551–52 (N.J. 2000); Jay M. Zitter, Annotation, *Liability of Internet Service Provider for Internet or E-mail Defamation*, 84 A.L.R. 169 (2000).

[38] *See* Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 409 (2d Cir. 2004); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002); Nexans Wires S.A. v. Sark-USA, Inc., 319 F. Supp. 2d 468, 474 (S.D.N.Y. 2004).

[39] United States v. Simons, 206 F.3d 392 (4th Cir. 2000); *see also* Skok, *supra* note 1, at 80–81.

[40] *See* Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002) (holding that the abuse of access to workplace computers is so common that "reserving a right of inspection is so far from being unreasonable that the failure to do so might well be thought irresponsible").

[41] *Employers Fighting Net Abuse Must Mind Privacy*, WASHINGTON INTERNET DAILY, Apr. 24, 2002, http://www.wrf.com/media_news.cfm?sp=news&tp=&industry_id=0&practice_ID=0&ID=2037.

[42] *Id.*

[43] *Id.*

[44] AM. MGMT. ASS'N, 2001 AMA SURVEY: WORKPLACE MONITORING & SURVEILLANCE: SUMMARY OF KEY FINDINGS (2001), *available at* http://www.amanet.org/research/pdfs/ems_short2001.pdf.

[45] *See generally* Michelle Delio, *New Tools a Spying Boss Will Love*, WIRED NEWS, Nov. 13, 2002, http://www.wired.com/news/privacy/0,1848,56324,00.html (explaining employer techniques to minimize employee misuse of technology).

[46] *See generally id.*

Because of this judicially recognized expectation of diminished privacy in the workplace,[47] employees are only entitled to bring suit when an intrusion infringes upon intensely private matters or when the employer has failed to inform the employee of the monitoring.[48] The combined actions of the U.S. Congress and the courts have effectively expanded an employer's ability to monitor employee electronic communications without violating federal privacy laws.[49]

B. ISP/Online Company and the User

1. Europe

The responsibilities of the ISP's and online companies to Internet users can be examined by differentiating between the ISP and the online advertising company. In both contexts, the collection of the user's personal information should be in accordance with the data protection principles as laid down under Article 6 of the DPD or its corresponding laws on data protection.[50] Article 6 of the DPD provides that Member States should ensure that personal data are:

> (a) processed fairly and lawfully;
> (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

---

[47] *See generally* Blakely, *supra* note 26, at 179 (providing evidence of the foundation of this view, which is rooted in the ancient Greek belief that privacy coexists with the public realm).

[48] *See, e.g.*, *Med. Lab. Mgmt. Consultants v. Am. Broad. Cos., Inc.*, 30 F. Supp. 2d 1182, 1188 (D. Ariz. 1998); *Doe v. Kohn Nast & Graf, P.C.*, 862 F. Supp. 1310, 1326 (E.D. Pa. 1994) (finding employer may have intruded on an employee's privacy by reading personal medical documents on employee's desk).

[49] *See, e.g.*, *Theofel v. Farey-Jones*, 359 F.3d 1066, 1075 (9th Cir. 2004) (finding that email messages stored on ISP servers fall within the definition of "electronic storage" under the Stored Communications Act); *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114–15 (3d Cir. 2003) (finding that the employer's search of an email system was permitted); *United States v. Angevine,* 281 F.3d 1130, 1134–35 (10th Cir. 2002) (holding that the professor, who had entered a conditional plea for downloading child pornography to his workplace computer, had no expectation of privacy in his use of his public employer's computer because the university's usage and monitoring policy was displayed upon login); *United States v. Bunnell*, No. CRIM.02-13-B-S, 2002 WL 981457, at *2 (D. Me. May 10, 2002) (stating a public university "student has no generic expectation of privacy for shared usage on the university's computers" (citing United States v. Butler, 151 F. Supp. 2d 82, 84 (D. Me. 2001))).

[50] *See also* European Commission. Status of implementation of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data, *available at* http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm (last visited Feb. 9, 2007).

> (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.[51]

Gavin Skok aptly described the differences between an online advertiser and the ISP as follows:

> Some online advertisers have developed "networks" of hundreds of unrelated Web sites which use individual identifying codes to identify and track Web users' clickstreams as they travel among the sites on the network. The data compiled by these businesses is then "mined" for hints about consumer preferences. . . . In contrast, ISPs can precisely monitor and record an entire clickstream since all of the user's [sic] online commands are sent through the ISP.[52]

The DPD considers an ISP to be a data controller because an ISP has access to the user's Internet provider (IP) address and clickstream data.[53] However, even when an IP address and clickstream data are combined with other information that a user has voluntarily provided, such as a postal address, ISPs generally must still adhere to the DPD.[54]

An ISP may possibly collect an individual's personal data in its role as a third party facilitator.[55] Under those circumstances, an ISP would be regarded as a data processor under Article 2(e) of the DPD,[56] unless the ISP "alone or jointly with others determines the purposes and means of the processing," in which case the ISP would be regarded as a data controller under Article 2(d) of the DPD.[57] This distinction is important because the DPD places significant

---

[51] *Id.*
[52] Skok, *supra* note 1, at 66–67.
[53] *See* DPD, *supra* note 3, art. 2.
[54] *See id.* art. 3.
[55] *See id.* art. 2(e).
[56] *See id.*
[57] *See id.* art. 2(d).

obligations on data controllers who process personal data.[58] For example, data controllers must comply with the data protection principles under Article 6 of the DPD and compensate the data subject for damage caused by the unlawful processing of personal data under Article 23 of the DPD.[59] To summarize, online advertisers and ISPs that collect clickstream data qualify as "data controllers" under Article 2(d) of the DPD because they are collecting an individual's personal data and therefore must comply with the relevant data protection laws that apply.[60]

2. *U.S. Law*

To some degree, U.S. law parallels its European counterpart by distinguishing ISPs from online advertising companies.[61] However, it differs notably because unlike the DPD, the U.S. regulatory frameworks do not define personal data.[62] As such, the sub-set of personal data is unprotected as well.[63] U.S. law is further complicated because the regulatory framework language[64] does not differentiate between written and oral digital communications.[65] Under the Electronic Communication Privacy Act (ECPA)[66] a government official that seeks to intercept or obtain electronic communications, such as ISP logs, must obtain judicial authorization by way of a "Title III" order from a federal judge.[67] Although the ECPA has been amended by the U.S.A. Patriot Act, the concept requiring the government to make some showing to a federal judge is true in most instances.[68] In summary, the United States lacks explicit comprehensive digital privacy legislation. Furthermore, the definition of

---

58 *See generally id.* arts. 6, 23.

59 *See generally id.*

60 The subject of clickstream data as "personal data" is discussed further in Part III.

61 *See* Garrie, *Voice Over*, *supra* note 8, at 115.

62 *See generally id.*

63 *See generally id.*

64 *See generally* David Bender & Larry Ponemon, *Binding Corporate Rules for Cross-Border Data Transfer*, 3 RUTGERS J.L. & URB. POL'Y 154, 155–59 (2006).

65 *See generally* Garrie, *Voice Over*, *supra* note 8.

66 *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified in 18 U.S.C. §§ 2510-2522 (2000)).

67 *Id.* § 2516.

68 The scope and impact of the U.S.A. Patriot Act is beyond the scope of this article. For further discussion of the U.S.A. Patriot Act, see John P. Elwood, *Prosecuting the War on Terrorism: The Government's Position on Attorney-Client Monitoring, Detainees, and Military Tribunals*, 17 CRIM. JUST. 30, 51 (2002).

personal data is discussed, applied, and defined only in select areas, such as medical privacy.[69]

In the context of clickstream data, the degree of liability for a specific ISP hinges on the role the ISP is playing with respect to the clickstream data collection. If the ISP's role is that of a third party, the ISP is immune from liability for its role in collecting the clickstream data and for most third party acts because of section 230 of the Communication Decency Act (CDA).[70] The CDA provides that ISPs are not publishers or speakers of information provided by a third party entity, a stipulation that effectively grants immunity to the ISP.[71] Therefore, in the context of clickstream data, the CDA effectively immunizes the ISP from liability, so long as it is a third party performing the data collection.[72] In cases in which an ISP itself is collecting clickstream data of end-users, the ISP may be found liable depending on the manner and type of consent that it acquired of the end-user.[73]

II. EUROPEAN LEGAL FRAMEWORK ON THE PROTECTION OF CLICKSTREAM DATA

A. Data Protection Directive 95/46/EC

The DPD was passed in 1995 with the aim of harmonizing the data protection laws within the EU.[74] An EU directive is binding on the Member State to which is it is addressed; however, the Member States decide on the form and methods in which to transpose the directive. To date, all the Member States, including the accession states that have joined the EU in 2004, have

---

[69] *See, e.g.*, Med. Lab. Mgmt. Consultants v. Am. Broad. Cos., Inc., 30 F. Supp. 2d 1182, 1188 (D. Ariz. 1998); Doe v. Kohn Nast & Graf, P.C., 862 F. Supp. 1310, 1326 (E.D. Pa. 1994) (finding employer may have intruded on an employee's privacy by reading personal medical documents on employee's desk).

[70] 47 U.S.C. § 230 (2006).

[71] *See id.* § 230(c)(1).

[72] *See id.*

[73] *See* Alan F. Blakley, Daniel B. Garrie & Mathew J. Armstrong, *Coddling Spies: Why the Law Doesn't Adequately Address Computer Spyware*, 2005 DUKE L. & TECH. REV. 25, 31–32. For a discussion of how the U.S. courts have interpreted the permissible range of collection of clickstream data by corporate entities, see Part IV.

[74] *See generally* DPD, *supra* note 3, pmbl. Two main international developments influenced the DPD. These were the OECD Guidelines in 1980 and the Council of Europe Convention in 1981, which developed guidelines involving the processing of personal data. Sweden was the first country to introduce data protection laws in the 1970s, but the harmonization of data protection laws within the EU did not occur until 1995. For further reading see ROSEMARY JAY & ANGUS HAMILTON, DATA PROTECTION: LAW AND PRACTICE 4–6 (1999), and CHRISTOPHER KUNER, EUROPEAN DATA PRIVACY LAW AND ONLINE BUSINESS 85–87 (2003).

enacted data protection laws to transpose the DPD.[75] The DPEC supplements the DPD; the former applies to the processing of personal data in the electronic communications sector.[76] The DPD refers to three main actors. One is the "data subject" whose data is being collected by a "data controller."[77] A data controller is broadly defined under Article 2(d) DPD 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, the controller or the specific criteria for his nomination may be designated by national or Community law.[78]

The DPD also refers to a "data processor" as one who processes personal data on behalf of the data controller.[79] The data processor's role is limited by the data controller.[80] A data processor is not limited to a person; the term may apply to a legal person, public authority, agency, or any other body which processes personal data as defined within Article 2(e) DPD.[81] For example, company A compiles an online survey of Internet users for company B. Under these circumstances, company A would be acting on behalf of company B.

The following sections consider the application of the DPD and whether clickstream data constitutes "personal data" within the DPD. The relevant provisions are Article 4(1)(c) and Article 2(b) of the DPD, which provide for the application of the DPD and the notion of personal data, respectively.

1. Application

The application of the DPD is contained within Article 4, which is comprised of three parts.[82] Article 4(1)(c) is most relevant here, providing that:

> The controller is not established on Community territory and, for purposes of processing personal data *makes use of equipment*,

---

[75] PRIVIREAL, Data Protection-Country Laws, http://www.privireal.org/content/dp/countries.php (last visited Oct. 19, 2006).

[76] *See generally* DPEC, *supra* note 4.

[77] DPD, *supra* note 3, art. 2.

[78] *Id.*

[79] *Id.*

[80] *See id.*

[81] *Id.*

[82] *Id.* art. 4.

> automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.[83]

The Article 29 Working Party has taken the view that spyware and cookies may constitute "equipment" within the terms of Article 4(1)(c).[84] The words "make use of" are to be construed as "to determine," whereby the data controller determines how the equipment is used.[85] Therefore, it is possible that a non-EEA data controller could fall within the scope of the DPD if it uses software within a Member State to record clicktrails of users.[86] For example, a U.S. based company could be subject to the DPD if it uses monitoring software in France to record the websites visited by French citizens. How this provision is enforced against non-EEA data controllers is another matter, but Article 4(1)(c) can nevertheless reach beyond the EEA and apply to non-EEA data controllers.[87] Companies outside of the EEA using "equipment" as defined within Article 4(1)(c) of the DPD should therefore be cautious about the types of personal information they collect to ensure that they operate within the DPD, even if they are not established in any of the EU Member States.[88]

Another point to add is that clickstream data is most likely to be used by data mining industries and Internet companies.[89] If clickstream data is being used to deliver customized services and advertisements to Internet users, then

---

[83] *Id*. (emphasis added).

[84] *See generally* DOUWE KORFF, EC STUDY ON IMPLEMENTATION OF DATA PROTECTION DIRECTIVE: COMPARATIVE SUMMARY OF NATIONAL LAWS 43–51 (2002) (explaining the limits of "equipment" in Article 4(1)(c)).

[85] KUNER, *supra* note 74, at 98; *see also* Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Working Document on Determining the International Application of EU Data Protection Law to Personal Data Processing on the Internet by Non-EU Based Web Sites*, 9–10, 5035/01/EN/Final, WP 56 (May 30, 2002) [hereinafter Art. 29 Working Party: Internet], *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_en.pdf (explaining the meaning and giving examples of "making use").

[86] *See also* Working Party on the Protection of Individuals With Regard to the Processing of Personal Data, Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware, 5093/98/EN/final, WP 17 (Feb. 23, 1999) [hereinafter Recommendation 1/99], *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp17en.pdf. "Clicktrails consist of information about an individual's behaviour, identiy [sic], pathway or choices expressed while visiting a web site. They contain the links that a user has followed and are logged in the web server" *Id*. at 4; *see generally* KORFF, *supra* note 84.

[87] *See generally* KUNER, *supra* note 74, at 97.

[88] *See* DPD, *supra* note 3, art. 4(c).

[89] *See generally* JIAWEI HAN & MICHELINE KAMBER, DATA MINING: CONCEPTS AND TECHNIQUES 473–75 (2001); Garrie, *Legal Status*, *supra* note 8; Balaji Rajagopalan & Ravi Krovi, *Benchmarking Data Mining Algorithms*, 13 J. DATABASE MGMT. 25 (2002) (finding that the amount of data collected by business is increasing).

the collection of such personal data would bring any company that is established in one or more of the Member States of the EU within the scope of the DPD.[90] Even if the company is not established within the EU, Article 4(1)(c) may still apply to companies outside the EEA that collect the clickstream data of their users.[91] The purpose behind Article 4(1)(c) is to prevent data controllers from circumventing their responsibilities under the DPD by operating outside the EEA while using equipment within a Member State.[92] For example, if company X is based in New York and has software in France that collects the clickstream data of its users, company X is making use of equipment[93] within Article 4(1)(c) of the DPD. Therefore, company X would be required to comply with the French data protection laws that correspond to the DPD.

In short, the Article 29 Working Party does not rigidly interpret "equipment," extending the definition to cookies, javascripts, and spyware.[94]

2. *Personal Data of an Individual*

The definition under Article 2(a) of the DPD broadly covers "any information relating to *an identified* or *identifiable natural person* ('data subject'); an identifiable person is one 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."[95]

---

[90] DPD, *supra* note 3, art. 4.

[91] *Id.*

[92] *See generally* KUNER, *supra* note 74, at 95–104 (giving an overview of the background of Article 4(1)(c) of the DPD).

[93] For a detailed analysis of the subject of "equipment," see *id.* at 94–105.

[94] *See also* European Commission. Status of implementation of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data, *available at* http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm (last visited Feb. 9, 2007).

[95] DPD, *supra* note 3, art. 2 (emphasis added). Recital 26 of the DPD adopts a broad criterion for identifiability, providing that "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." *Id.* pmbl., para. 26. Recommendation R(89) 2 on the Protection of Personal Data Used for Employment Purposes also provides that "[a]n individual shall not be regarded as 'identifiable' if the identification requires an unreasonable amount of time, cost and manpower." Council of Europe, Committee of Ministers, On the Protection of Personal Data Used for Employment Purposes, § 1.3, Recommendation No. R (89) 2 (Jan. 18, 1989), *available at* http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/international_legal_instruments/Rec(89)2_EN.pdf. For an in-depth analysis of the notions of "identification" and "identifiability," see BYGRAVE, *supra* note 2, at 42–50.

The question about whether clickstream data is "personal data" within the meaning of Article 2(a) DPD is important for various reasons. First, if clickstream data is "personal data," then the DPD would obviously apply.[96] This scenario would require any company established within a Member State of the EU to comply with the relevant national data protection laws.[97] However, the question is also important because of its application to non-EEA data controllers.[98] The collection of clickstream data is not restricted within EU borders and it is possible that non-EEA data controllers could again be brought within the scope of the DPD.

As elucidated above, clickstream data can be extracted from personal information such as static IP addresses, cookies, and webpages viewed by individuals.[99] Already, some data protection authorities in Germany[100] and Sweden[101] have taken the view that static IP addresses constitute personal data within their country's data protection laws. The question that arises is what are the implications of such a view for companies whether based within or outside the EU?[102] For companies based within the EU, the relevant EU Member State data protection law applies, depending on where the company is established.[103] For example, a company based in the United Kingdom would be required to comply with the UK Data Protection Act of 1998.[104] With regard to a company based outside the EU, one must determine whether the company uses "equipment" within the meaning of Article 4(1)(c) of the DPD to collect IP addresses of users in the EU.[105] Any non-EEA organization or company that makes use of software within a EU Member State to collect IP addresses of European users would be required to adhere to the relevant Member State data

---

96 DPD, *supra* note 3, art. 2.

97 *Id.* art. 4.

98 *See* KUNER, *supra* note 74, at 94.

99 *See infra* Part II.

100 *See* Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], Sept. 14, 1994, BGB1. I at S.2325, § 3, (F.R.G.), *translation available at* http://www.bfdi.bund.de/cln_029/nn_535764/EN/DataProtectionActs/DataProtectionActs__node.html__nnn=true. The Act defines "personal data" as "any information concerning the personal or material circumstances of an identified or identifiable individual." *Id.* The Federal Data Protection Commissioner shares the same view as the Article 29 Working Party that IP addresses are personal data. Email Interview with Ms Jennen, Federal Data Protection Commissioners (May 2, 2005).

101 *See* 3 § Personuppgiftslagen (Svenska författningssamling [SFS] 1998:204) (Swed.), *translation available at* http://www.datainspektionen.se/pdf/ovright/pul-end.pdf. The Act defines "personal data" as "all kinds of information that directly or indirectly may be referable to a natural person who is alive." *Id.*

102 For an in-depth discussion of Article 4(1) of the DPD, see KUNER, *supra* note 74, at 94–105.

103 *See id.*

104 *See* Data Protection Act, 1998, c. 29, § 5 (U.K.).

105 DPD, *supra* note 3, art. 4.

protection laws.[106] For example, if a company based in India uses software in France to collect IP addresses of European users, then the French data protection laws would apply. In short, Article 4(1)(c) of the DPD applies to any company outside the EU that makes use of the equipment within a Member State.[107]

The next question is how one determines whether clickstream data is personal data. Article 2(a) of the DPD provides some guidance.[108] The key is whether clickstream data *relates* to an identified or identifiable individual. If clickstream data cannot *relate* to an identified or identifiable person, then the data arguably falls outside the scope of the DPD.[109] However, if clickstream data pertains to or facilitates the identification of a *specific individual*, then the DPD would apply.[110] This interpretation would require the organization, as the data controller, to comply with the data protection principles as laid down under Article 6(1) or its corresponding provision and the laws of the relevant Member State.[111]

The preamble to the DPD provides some assistance on the interpretation of personal data.[112] The relevant provision is Recital 26, which provides that:

> Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, 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*; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable . . . .[113]

The DPD does not apply to data that is in anonymous form because no single individual can be identified.[114] Data in anonymous form prevents anyone from ascertaining that the data in question relates to an identified or identifiable individual.[115]

---

106 *See* KUNER, *supra* note 74, at 94–105.

107 *See* DPD, *supra* note 3, art. 4.

108 *Id.* art. 2.

109 *Id.*

110 *See id.*

111 *Id.* art. 6.

112 *Id.* pmbl., para. 26.

113 *Id.* (emphasis added).

114 *See* Privacy in Research Ethics & Law, Recommendations Around Anonymisation and the Definition of Personal Data, http://www.privireal.org/content/recommendations/#Recc (last visited on Oct. 19, 2006).

115 *See id.* (providing an in-depth analysis of anonymisation).

The discussion about clickstream data as personal data is not entirely conclusive. On the one hand, the Article 29 Working Party takes the view that clickstream data qualifies as personal data under the DPD in most instances.[116] For example, the collection of a user's IP addresses and webpages visited qualifies as collecting personal information relating to an individual. As early as 2000, the Article 29 Working Party identified that there was monitoring software available to ISPs that could be used to generate far more information about traffic patterns and content preferences.[117] These include software such as Alexa, which is added to a browser and used to accompany the user while surfing.[118] The information collected is then used to form a large database, which in turn measures Internet usage.[119]

Reidenberg and Schwartz, however, take the view that "[for] on-line services, the determination of whether particular information relates to an 'identifiable person' is unlikely to be straightforward."[120] While there may be difficulties in determining whether clickstream data correlates with a specific individual, the technologies have become so sophisticated that it is possible to extract personal information from clickstream data and identify specific individuals from this process.[121] The next question is whether the DPD protects clickstream data belonging to a group of individuals.

3. Personal Data Belonging to a Group of Individuals

As the DPD is person-specific, it is unlikely that clickstream data belonging to a group of individuals will be protected.[122] For example, if a computer was registered against a number of individuals through an IP address, then it is not personal data within the meaning of Article 2(a) DPD because a single individual cannot be identified from such use.[123] As Lee

---

116 *See generally* Recommendation 1/99, *supra* note 86, at 4 (explaining that cookies and javascript are personal data under the DPD).

117 *See* Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Working Document: Privacy on the Internet—An Integrated EU Approach to On-Line Data Protection*, 46, 5063/00/EN/Final, WP 37 (Nov. 21, 2000), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf.

118 *Id.*

119 *Id.*

120 JOEL R. REIDENBERG & PAUL M. SCHWARTZ, DATA PROTECTION LAW AND ONLINE SERVICES: REGULATORY RESPONSES 23 (1998), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/regul_en.pdf.

121 *See* Garrie, *Legal Status*, *supra* note 8, at 727.

122 *See* BYGRAVE, *supra* note 2, at 317.

123 *See* DPD *supra* note 3, art. 2.

Bygrave states: "The chance of an IP address (and other clickstream data registered against that address) constituting personal data will be diminished if a multiplicity of persons are *registered* against the address."[124]

Discussion over the extension of the DPD to legal entities is well documented.[125] While a number of countries—Austria, Denmark, Norway, and, to a limited extent, Italy—have extended their own data protection laws to legal entities, the DPD does not protect clickstream data belonging to legal entities any more than it protects data belonging to a group of individuals.[126]

4. Clickstream Data as Sensitive Data

Assuming clickstream data is construed as "personal data," the next question is whether clickstream data can ever be sensitive data. Article 8(1) of the DPD categorizes sensitive data as "personal data *revealing* racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."[127] Assuming that the clickstream data is person specific (i.e. relating to an identifiable individual), data revealing an individual's ethnic origin or religious opinion would qualify as sensitive data.[128] However, there is one flaw with this argument. It is not always possible to draw an inference of an individual's sensitive data based on the fact that he or she has visited a particular website. For example, if a user visited a Christian website, it is not necessarily true that the user was doing so for his or her religious beliefs rather than for research purposes. Certainly, repeated visits to a particular website or websites of a similar nature may indicate that the user holds particular religious beliefs. But it does not always follow that a website will necessarily correlate with a user's sensitive data as defined under Article 8(1).

The DPD does not draw a distinction in ascertaining the user's intention when he or she visits a website.[129] The current categorization of sensitive data

---

[124] BYGRAVE, *supra* note 2, at 318.

[125] For a detailed analysis into legal entities, see BYGRAVE, *supra* note 2, at 173–298 (analyzing data protection for legal entities), and DOUWE KORFF, STUDY ON THE PROTECTION OF THE RIGHTS AND INTEREST OF LEGAL PERSONS WITH REGARD TO THE PROCESSING OF PERSONAL DATA RELATING TO SUCH PERSONS 22–41 (1998) (outlining the treatment of legal entities in the Member States).

[126] *See id.*

[127] DPD, *supra* note 3, art. 8(1) (emphasis added).

[128] *See id.*

[129] *See* Rebecca Wong, *Data Protection Online: Alternative Approaches to Sensitive Data?*, 2(1) J. INT'L COM. L. & TECH. 9–16, *available at* http://www.jiclt.com/index.php/JICLT; *see also* Consultative Committee for the Protection of Individuals with Regard to the Automatic Processing of Personal Data, Report for the

is not adequate as it is based on the actual nature of the data.[130] More specifically, the publication of any personal data on the Internet may, under particular contexts, constitute the processing of sensitive data.[131] For example, a photograph showing the ethnic origin of the individual would be regarded as sensitive data irrespective of the context or purpose in which the photograph was published.[132]

From a practical perspective, it would be difficult to correlate a user's visit on a website with any of the data listed under Article 8(1) DPD.[133] However, the key to understanding this provision is the word "revealing" under Article 8(1). If the European Court of Justice broadly interpreted "sensitive data" so that reference to an individual's foot injury on a webpage would constitute the processing of sensitive data (as in *Lindqvist*),[134] then it is possible to contend that an individual's clickstream data could also be defined as sensitive data within Article 8(1) DPD. Even if the correlation between the user and his or her clickstream data revealing sensitive data is weak, the DPD may nevertheless still apply.[135] In other words, there is still the possibility that clickstream data of a single individual would qualify under Article 8(1) of the DPD as "sensitive data" notwithstanding the difficulties highlighted above.

III. DIRECTIVE ON PRIVACY AND ELECTRONIC COMMUNICATIONS 2002/58/EC

The next issue is whether the Directive on Privacy and Electronic Communications 2002/58/EC covers clickstream data. The DPEC applies to the processing of personal data in the electronic communications sector and complements the DPD. Although it updates the Telecommunications Directive 97/66/EC in dealing with various issues ranging from an opt-in consent of

---

Committee of Ministers, app. 4, T-PD (2004) RAP 21 (April 5, 2005), *available at* http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/events/ t-pd_and_t-pd-bur_meetings/T-PD%20_2005_%20RAP%2021%20E.pdf (referring to the current enumeration of sensitive data under Article 8(1) DPD and making a number of recommendations).

130 *See* Wong, *supra* note 129.

131 *See* BYGRAVE, *supra* note 2, at 69 (commenting on the context approach and sensitive data); *see generally* Spiros Simitis, Revisiting Sensitive Data, http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/reports_and_studies_by_experts/Z-Report_Simitis_1999.asp (last visited Oct. 19, 2006) (discussing the context oriented approach to personal data as sensitive data).

132 The arguments on the current approach to sensitive data have been covered elsewhere.

133 *See* DPD, *supra* note 3, art. 8.

134 Case C-101/01, Lindqvist v. Åklagarkammaren i Jönköping, 2002 E.C.R. I-12791, 1 C.M.L.R. 20 (2002).

135 *See* DPD, *supra* note 3, art. 8.

unsolicited commercial communication to location data,[136] the DPEC does not have a specific section dealing with clickstream data.[137] It only considers specific devices such as cookies and spyware that intrude upon a user's personal privacy.[138] The relevant section is Article 5(3) of the DPEC, which provides:

> Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, *inter alia* about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.[139]

In short, users and subscribers should be provided with clear and comprehensive information about the use of such devices and have the right to object to such processing.[140] This provision is a watered-down version from the original proposals to the DPEC that required an opt-in consent from users before such devices could be installed. Article 5(3) should be considered in light of Recital 24 of the preamble of the DPEC, which states:

> Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned.[141]

---

136 DPEC, *supra* note 4, pmbl., para. 4.
137 *See generally id.*
138 *See id.* pmbl., para. 25.
139 *Id.* art. 5.
140 *See id.*
141 *Id.* pmbl., para. 24.

The main criticism is that under the DPEC there is no express reference to clickstream data.[142] Article 5(3) is "device specific" by focusing on specific items that could be installed without a user's knowledge.[143] In the absence of a definition, a purposive interpretation should be adopted by looking at whether the devices in question intrude upon the privacy of the users.[144] Clickstream data would be covered under the general DPD, but not so under the DPEC. Given that the DPEC is intended to apply to the processing of personal data in electronic communications,[145] one can argue that there should be a specific section that expressly deals with clickstream data, rather than merely an update of the Telecommunications Directive 2002/58/EC. Further discussion about DPEC and clickstream data is needed with data protection authorities and the Article 29 Working Party.

IV. U.S. LEGAL TREATMENT OF CLICKSTREAM DATA

Unlike its European counterpart, the U.S. legal framework does not have to contend with a series of legal frameworks that specify the types of data. While the U.S. courts have guidelines, it is determined on a case-by-case basis. Therefore, a great deal of the U.S. clickstream debate has been interpreted by the U.S. courts.[146]

A. Treatment of Clickstream Data by U.S. Courts

Unlike the European courts, the U.S. courts to date have not differentiated clickstream data further than by recognizing it as an exception to the Wiretap Act. U.S. courts have achieved this differentiation by imputing that a visitor's utilization of a web-portal constitutes consent to interception and manipulation of the user's data, including but not limited to the data exchanged with that web-portal.[147] The courts have found that this data can then be monitored and

---

142 *See generally id.*

143 *See id.* art. 5(3).

144 *Compare* DPD, *supra* note 3, *with* DPEC, *supra* note 4.

145 DPEC, *supra* note 4, art. 1.

146 *See, e.g.*, *In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 12 (1st Cir. 2003); *In re* Toys R Us, Inc., Privacy Litig., 2001 U.S. Dist. Lexis 16947 at *1 (N.D. Cal. Oct. 9, 2001); Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1155–57 (W.D. Wash. 2001); *In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 503–07 (S.D.N.Y. 2001). Portions of Part IV have been substantially reprinted from Garrie, *Voice Over*, *supra* note 8, at 117–20.

147 *See In re DoubleClick*, 154 F. Supp. 2d at 511 ("Although the users' requests for data come through clicks, not keystrokes, they nonetheless are voluntary and purposeful. Therefore, because plaintiffs' GET,

recorded by prying eyes and mined for information that can be used internally to construct a web user profile, recreate his or her online experience, sold to interested third-parties, or given to unknown third-parties for other unspecified reasons such as security.[148]

While the U.S. courts have dealt with clickstream data in *Chance*,[149] *Pharmatrak*,[150] *Toys R Us*,[151] and *DoubleClick*,[152] in which plaintiffs all alleged violations of the Wiretap Act through the use of cookie technology to intercept clickstream data,[153] the outcome of each of these cases rested upon the Wiretap Act, and examinations of reasonable expectations of privacy under *Katz*'s two-part test were cursory at best.[154] Recently, however, the First Circuit Court of Appeals in *Pharmatrak*[155] limited the effects of this judicial exception by stipulating that a user's consent can be inferred only when there is actual notice and when one party actually consents to the interception.[156] While it is unlikely that this holding has benefited users, no empirical data exists on what influence any of the aforesaid holdings have had on the development of web-site monitoring technologies.

POST and GIF submissions to DoubleClick-affiliated Web sites are all 'intended for' those Web sites, the Web sites' authorization is sufficient to except DoubleClick's access under § 2701(c)(2).").

148 *See* Usama M. Fayyad, Gregory Piatetsky-Shapiro & Padhraic Smyth, *From Knowledge Discovery to Data Mining: An Overview*, *in* ADVANCES IN KNOWLEDGE DISCOVERY AND DATA MINING 6–11 (1996); Tal Z. Zarsky, *"Mine Your Own Business!": Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion*, 5 YALE J.L. & TECH. 1, 4, 11 (2002–2003).

149 *See Chance*, 165 F. Supp. 2d at 1156–57.

150 *See In re Pharmatrak,* 329 F.3d at 16. The Electronic Communications Privacy Act provides for a private right of action against one who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a) (2006).

151 *See In re Toys R Us, Inc.*, 2001 U.S. Dist. Lexis 16947 at *1.

152 *See In re DoubleClick*, 154 F. Supp. 2d at 503–04.

153 *See generally* Daniel B. Garrie, Mathew J. Armstrong & Alan F. Blakley, *Voice Over Internet Protocol: Reality v. Legal Fiction*, 52 FED. LAW. 34, 34 (2005) (describing clickstream data and cookie technology).

154 The Supreme Court has historically applied a two-part test to determine whether the Fourth Amendment protects an asserted privacy interest. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J. concurring) (announcing a test to determine expectations of privacy). First, the individual must exhibit a subjective expectation of privacy. *Id.* Second, the expectation must be "one that society is prepared to recognize as 'reasonable.'" *Id.*; *see also* United States v. Thomas, 729 F.2d 120, 122–23 (2d Cir. 1984) (applying two-part test).

155 *See In re Pharmatrak*, 329 F.3d at 19–22.

156 *Id.* at 20 ("Without actual notice, consent can only be implied when the surrounding circumstances *convincingly* show that the party knew about and consented to the interception." (quoting Berry v. Funk, 146 F.3d 1003, 1011 (D.C. Cir.1998))). Moreover, "knowledge of the capability of monitoring alone cannot be considered implied consent." *Id.* (quoting Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983)).

1. Wiretap Act and Broad Judicial Interpretation of the Consent Exception.

In dealing with clickstream data[157] and cookie-related technology,[158] a Second Circuit district court in *DoubleClick*[159] construed the Wiretap Act's consent exception broadly,[160] requiring only implied consent, whereas the First Circuit Court of Appeals in *Pharmatrak*[161] narrowly construed the exception, requiring actual consent.[162] In both of these cases, the court heard Wiretap Act claims alleging unauthorized third party access to communications.[163] In these cases, end-users conveyed digital information to second-party entities that then used the information to construct user profiles in a process referred to as data mining.[164]

The implications of the distinction between implied and actual consent are important because the former interpretation of consent favors industry while the latter interpretation favors the user. The users' interests appear to be marginalized in *DoubleClick*.[165] Although the court may not have found a violation of the users' privacy rights in *DoubleClick*,[166] a violation of privacy rights did arguably occur because the users did not truly consent to their clickstream data being extracted from their machines. The court's holding demonstrates that the threshold for establishing implied consent is significantly lower than that of showing actual consent for the user.

The *DoubleClick* court permitted web businesses to intercept clickstream data utilizing cookie technology,[167] thereby extracting personal information from users' machines.[168] The defendant web business placed cookies on end-users' computers, which then transmitted personal information back to the

---

157 *See In re DoubleClick*, 154 F. Supp. 2d at 501–02.

158 For a more in-depth analysis, see Garrie, *Voice Over*, *supra* note 8, at 117–20.

159 *See In re DoubleClick*, 154 F. Supp. 2d. at 501–02 (discussing cookies and the collection of data, where the plaintiffs again did not prevail).

160 *See id.*

161 *See In re Pharmatrak*, 329 F.3d at 19.

162 *See id*. at 19–22.

163 *See In re Pharmatrak*, 329 F.3d at 12; *In re* Toys R Us, Inc., Privacy Litig., 2001 U.S. Dist. Lexis 16947 at *1 (N.D. Cal. Oct. 9, 2001); Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1155 (W.D. Wash. 2001); *In re DoubleClick*, 154 F. Supp. 2d at 507.

164 *In re Pharmatrak*, 329 F.3d at 12; *In re DoubleClick*, 154 F.Supp. 2d at 503, 505; *see generally* Joseph S. Fulda, *Data Mining and Privacy*, 11 ALB. L.J. SCI. & TECH. 105 (2000) (describing data mining).

165 *See In re DoubleClick*, 154 F. Supp. 2d at 510.

166 *See id.* at 514, 519.

167 *See id.* at 503–04.

168 *See id*. at 505 n.14.

website's owner or to a third-party data mining company.[169] Rather than find that there had been a violation of the users' privacy rights,[170] the court found that the web business's unilateral consent was sufficient to authorize third-party usurpation of the users' personal information using cookie technology.[171] The court held that the third-party data mining companies did not violate the Wiretap Act under 18 U.S.C. § 2511(2)(d) because the users had given implied consent and because their actions were not conducted for tortious or illegal purposes.[172]

2. *Wiretap Act and Judicial Interpretation Distinguishing Inferred Consent from General Consent.*

By contrast, the court in *Pharmatrak*[173] challenged the sweeping implications of the implied consent argument established in *DoubleClick*[174] by requiring that the party both know about and consent to the interceptions before consent can be inferred.[175] The court in *Pharmatrak* found in favor of the Internet users, holding that neither party to the communication consented to the web-monitoring company's interception of personally identifiable information.[176] The court reasoned that "without actual notice, consent can only be implied when the surrounding circumstances *convincingly* show that the party knew about and consented to the interception."[177] Because the parties had an explicit contract limiting the permissible scope of the interception to non-personally identifiable data,[178] the court refused to find implied consent between the parties to collect personally-identifiable information that clearly

---

169 *See id.* at 502–03.

170 *See id.* at 514–15.

171 *See id.* at 518–20.

172 *See id.*

173 *See In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 19–22 (1st Cir. 2003).

174 *See In re DoubleClick*, 154 F. Supp. 2d at 518–20 (holding that no unlawful interception of communications had occurred because the consent of the Web portal entity, as a party to the communication under § 2511(2)(d) of the Wire Tap Act, was sufficient in itself to authorize the third-party to usurp the users' information).

175 *See In re Pharmatrak*, 329 F.3d at 20 (stating that "without actual notice, consent can only be implied when the surrounding circumstances *convincingly* show that the party knew about and consented to the interception" (quoting Berry v. Funk, 146 F.3d 1003, 1011 (D.C. Cir. 1998))). Moreover, "knowledge of the capability of monitoring alone cannot be considered implied consent." *Id.* (quoting Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983)).

176 *See id.* at 19–22.

177 *See id.* at 20.

178 *See id.* at 15.

exceeded the bounds of the express contract.[179] The *Pharmatrak*[180] requirement of actual consent represents a stricter stance on inferring consent than was taken in *DoubleClick*.[181] However, even under this construction, end-users never input all of the written information transmitted by cookie via clickstream technology over the Internet; thus, the courts have imputed consent by reasoning that end-users and their computers are the same entity.

By limiting the court's ability to infer consent to situations in which actual consent has been obtained,[182] the *Pharmatrak* holding took a major step towards eliminating the judicially created pseudo-exception for clickstream data under the Wiretap Act.[183]

B. Conclusion Concerning U.S. Law

Clickstream data still presents novel challenges to the U.S. legal system and the law surrounding clickstream data is likely to evolve. Although the U.S. courts have addressed specific situations of consent and privacy of the user, the digital privacy landscape remains convoluted and complex.[184] Moreover, the state of the law today seems to fall notably short of protecting the consumer. However, if the trend established in *Pharmatrak* continues, courts may eliminate the clickstream data exception on their own by requiring either explicit or implicit actual consent for all third-party clickstream data interceptions under the Wiretap Act, including those data sent by end-users' machines without any end-user input. Although European law is not perfect, it provides some specificity as to acceptable and unacceptable collection of clickstream data, thereby providing more effective and stronger consumer protections than those provided by the U.S. legal structure.

CONCLUSION

The purpose of this Article is two-fold. First, it is to raise the level of discussion amongst data protection authorities, legislators, and internet

---

[179] *Id.* at 20–21. Nevertheless, Pharmatrak collected personal information on a subset of users and distributed 18.7 million cookies via the Netcompare technology framework. *Id.* at 15.

[180] *See id.* at 20–21.

[181] *See In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 510–11 (S.D.N.Y. 2001).

[182] *See In re Pharmatrak*, 329 F.3d at 19 (stating that "consent may be explicit or implied, but it must be actual consent rather than constructive consent").

[183] *Id.*

[184] Perhaps the Supreme Court will impute via the U.S. Constitution a digital privacy right. Until either the Supreme Court or the Legislature acts, the issues of digital privacy will be unanswered.

companies about the overall regulation of clickstream data within Europe and the United States. Second, the Article draws on specific problems relating to the scope of clickstream data as covered under the European Data Protection framework and the U.S. legal framework. The Data Protection Framework is a starting point, but the regulation and application is not restricted within Europe.

In the United States, such protections are in their infancy because the U.S. legislature has failed to create any substantive uniform protection for a global data protection framework. Of course, in the Untied States, independent states create data protection laws, but these laws have not been treated by the state courts. As demonstrated by the cases *DoubleClick* and *Pharmatrak*, federal judicial interpretations of consent to clickstream data are inconsistent. Furthermore, users' interests were marginalized in *DoubleClick*. In contrast, the decision in *Pharmatrak* is a step towards the right direction in recognizing the rights of Internet users.

Given the potential ways in which clickstream data can be used, be it in the United States or Europe, companies should be aware of the DPD, while users and consumers should be made more aware of clickstream data and how it is used. Additionally, DPEC is not without its shortcomings and certainly more needs to be done to raise the issue at a European level with both the Article 29 Working Party and data protection authorities.