KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

Comments of the Center for Democracy & Technology
to the European Commission

in the matter of the

Consultation on the Legal Framework
for the Fundamental Right to Protection of Personal Data

Submitted December 31, 2009

The Center for Democracy & Technology (CDT) is pleased to offer this contribution to the Commission's consultation. We hope that these comments, which draw upon CDT's research and advocacy, will assist the Commission in addressing the challenges posed by new technologies and business practices and by the reality of global data flows.

In these comments, CDT focuses on five technological trends that pose special challenges to data protection today: cloud computing, behavioral advertising, deep packet inspection, location awareness, and re-identification of seemingly anonymous data.

About CDT

CDT is a non-profit, non-governmental public interest organization headquartered in Washington, DC. Our mission is to keep the Internet open, innovative and free. We accomplish our mission through technical, policy and legal analysis, consultation with industry, academia and other stakeholders, and advocacy. Since our establishment in 1994, CDT has helped to shape public policy on a wide range of Internet issues, including consumer privacy. For example, CDT created the Anti-Spyware Coalition, which has helped to build consensus definitions and best practices for anti-spyware researchers. We also have a special project on health privacy. CDT advocates in the United States for adoption of a comprehensive federal consumer privacy law based on a full set of Fair Information Practices (FIPs), combined with robust industry practices and privacy by design, also reflecting the FIPs.[1] CDT coordinates the Internet Privacy Working Group, a forum for consumer advocates and Internet companies, where stakeholders can engage in dialogue and seek consensus on consumer privacy issues. We have worked with industry on privacy best practices (for example on the use of RFID), and we offer consumers a wide range of resources. CDT staff present frequently before governmental and technical standards bodies around the world.

---

[1] CDT recently filed with the US Federal Trade Commission detailed comments laying out our vision for comprehensive consumer privacy protection: "Refocusing the FTC's Role in Privacy Protection; Comments of the Center for Democracy & Technology in regards to the FTC Consumer Privacy Roundtable," November 6, 2009, http://www.cdt.org/privacy/20091105_ftc_priv_comments.pdf.

1. New challenges for personal data protection, in particular in the light of new technologies and globalization

The European Union's Data Protection Directive (the Directive) has been the most prominent data protection law in the world for the past fifteen years. In addition, the European Commission (the Commission) and its institutions have set an example for the rest of the world through their constant efforts to improve consumer privacy in response to changes in technology and business practices. However, although the Directive is a comprehensive, flexible, and technology-neutral framework, there are several technological advances that pose special challenges to consumer privacy, especially as the digital world becomes even more borderless than before. We focus here on five such developments: cloud computing, behavioral advertising, deep packet inspection, location awareness, and the issues surrounding re-identification of data previously thought to be anonymized or de-identified.

a. Data storage in "the cloud"

As online storage has become both ubiquitous and inexpensive, consumers and businesses are storing or processing personal data on remote servers (in "the cloud") rather than on local machines. Because the data can be accessed from different locations and different devices at any time, cloud computing is well-suited both to individuals wishing to store, process and share information and to the collaborative work styles and distributed, disaggregated structures that characterize modern commerce. It can provide significant benefits in terms of flexibility, cost, and security. However, placing personal data in the cloud can also pose risks to privacy as data crosses borders, often without the knowledge or understanding of the consumer, to countries with inadequate levels of data protection. Though the Directive limits the transfer of personal data into such countries, limiting cross border data flows is becoming increasingly difficult and impractical.

The Commission has already recognized both the potential benefits and the challenges of cloud computing. Commissioner Viviane Reding has suggested promoting the cloud to small and medium-sized enterprises to help them leverage ICT at a lower cost.[2] She further called for the development of a "European Cloud" as a way to obtain the benefits of third party storage and software as a service without running afoul of the Directive.[3] However, cloud computing may be most efficient when data can be stored and served from anywhere in the world, depending on load, cost and other factors.

Consumers cannot be expected to understand or provide meaningful consent for each of the complex transactions involved in cloud computing. Data protection law must take account of this paradigm. Companies must be encouraged to assume the burden for

[2] Viviane Reding, "Europe's Fast Track to Economic Recovery," The Ludwig Erhard Lecture 2009 Lisbon Council, July 9, 2009, http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/09/336&format=HTML&aged=0&language=EN&guiLanguage=en.

[3] *Id.*

protecting data and must be made accountable for that protection and for appropriate use of data as well as for its misuse, beyond the legal requirements of any one country.[4]

b. Behavioral advertising

Behavioral advertising is a method of marketing whereby advertisers "track, collect and aggregate information about consumers' Web browsing activities and compile individual profiles that are used to match advertisements to consumers' interests."[5] While advertising is the legitimate foundation for much of the free content and services available on the Internet, the collection and use of large amounts of data to create detailed profiles of interests or preferences has clear privacy implications.

In recent years, companies, policymakers, regulators and consumer advocates in the US have grappled with the implications of online behavioral profiling. CDT has been at the center of this debate, convening stakeholders for consultation and consensus-building, developing resources for consumers, and testifying before Congress and the Federal Trade Commission (FTC).

CDT recently released a paper that analyzes the self-regulatory frameworks developed by the online advertising industry in the US.[6] We concluded that self-regulation, while necessary, is not sufficient to protect consumers and that fully protecting consumer privacy interests in the US will require Congress to pass general consumer privacy legislation that encompasses both online and offline practices and that gives the FTC broader rulemaking authority over consumer privacy in general and behavioral advertising practices more specifically. Importantly, we urged that FTC rulemaking and self-regulatory guidelines should reflect the full set of Fair Information Practice principles (FIPs), which focus on minimizing data use, sharing and retention as well as on data collection. Over the years, regulators and self-regulatory bodies in the US have narrowly focused their attention almost exclusively on notice and consent, an approach that places too much burden on consumers and establishes too few substantive obligations on data controllers. Our commentss to the FTC provide more detail on CDT's recommendations for comprehensive privacy protection.

Other CDT resources on behavioral advertising that may be of interest to the Commission include:

- "Privacy Implications of Online Advertising," Testimony of Leslie Harris, President & CEO, Center for Democracy & Technology, before the Senate Commerce,

[4] One proposal on accountability was issued by companies and experts meeting as the "Galway Project." "Data Protection Accountability: The Essential Elements," October 2009, http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf.

[5] Center for Democracy & Technology, "Online Behavioral Advertising: Industry's Current Self-Regulatory Framework is Necessary, but Still Insufficient On its Own to Protect Consumers," p. 3, December 2009, http://www.cdt.org/files/pdfs/CDT%20Online%20Behavioral%20Advertising%20Report.pdf.

[6] *See id.* at p. 7.

Science & Transportation Committee (July 9, 2008)
http://old.cdt.org/testimony/20080709harris.pdf

- "Threshold Analysis for Online Advertising Practices" (January 28, 2009)
http://www.cdt.org/privacy/20090128threshold.pdf

- "Privacy Principles for the Development of User Controls for Behavioral Targeting" (March 4, 2008)
http://www.cdt.org/privacy/pet/Privacy_Controls_IPWG.pdf

- CDT's Guide to Behavioral Advertising
http://www.cdt.org/privacy/targeting

c. Deep packet inspection

Deep packet inspection (DPI) involves the examination of the contents of Internet communications. The name is a reference to the packetized nature of Internet communications: email, Web browsing and other digital communications are broken up into small packets, consisting of routing information (the "header") and some part of the content of the communication (the packet "payload"). Normally, the devices in the middle of the Internet responsible for routing data inspect packet headers to decide where each packet should go next. This is called "shallow packet inspection" because the analysis is limited to the header information. This shallow sort of inspection does not reveal the actual content of the Web browsing session, email, or VoIP call that a particular packet may contain, just as looking at an address on an envelope reveals nothing about the content of the letter inside. Deep packet inspection, in contrast, is the equivalent of postal employees opening envelopes and reading the letters inside to look for certain details. To do DPI, network devices examine the payload of a packet – the actual data the packet carries – in addition to the packet header.[7] Some companies have explored using DPI in aid of behavioral advertising; in this model, the ISP may copy substantially all of a consumer's data stream and share it with a third party advertising company.

In Congressional testimony last year, CDT described the privacy concerns posed by DPI:

> In part because the Internet was developed around the end-to-end principle, consumers have come to expect that their Internet communications pass through the network without being snooped on the way. DPI dramatically alters this landscape by providing an ISP or its partners with the ability to inspect consumer communications en route.

[7] For a full description of DPI, *see* Statement of Leslie Harris, President and CEO, Center for Democracy & Technology, before the House Committee on Energy and Commerce, Subcommittee on Communications, Technology, and the Internet, "The Privacy Implications of Deep Packet Inspection" (Harris Testimony), pp. 4-5, April 23, 2009, http://www.cdt.org/privacy/20090423_dpi_testimony.pdf.

> Thus, deploying a DPI system likely defies the expectations consumers have built up over time. Absent unmistakable notice, consumers simply do not expect their ISP or its partners to be looking into the content of their Internet communications.[8]

Last year, it emerged in both the UK and the US that ISPs were experimenting with DPI for behavioral advertising purposes. The US Congress held hearings, and the European Commission instituted an action against the UK in connection with DPI.[9] CDT issued a memo noting that DPI might violate US federal wiretapping laws if not conducted with prior, explicit consent of users;[10] experts in the UK offered a similar opinion.[11] The fact that the legality of using DPI for behavioral advertising was unclear under the Directive, such that the UK was apparently prepared to let it be implemented, highlights the need for the Commission and other European institutions to regularly update their interpretation of the Directive in response to specific new practices.

Although recent controversy over DPI has centered on its use for behavioral profiling, the technique has many other uses, some of them clearly legitimate, such as cyber-security and network management. However, even such legitimate uses have serious privacy implications. Accordingly, CDT has urged policymakers to "carefully weigh any expected benefits of a proposed use of DPI against the substantial privacy and other risks outlined above" and "consider whether there may be alternative methods for achieving their goals, with a strong preference for means that do not require sweeping inspection of Internet communications at the ISP level."[12] Because there are often other alternatives to using DPI in many instances, CDT "believes strongly that this analysis will rarely favor the use of DPI on a broad scale."[13]

CDT recommended in April that a US Congressional Subcommittee seek additional information directly from ISPs and their partners about how they are using DPI. Specifically, we urged Congress to obtain from industry answers to these questions: For what purposes are ISPs currently using DPI? Are additional uses anticipated? What

---

[8] *Id.* at p. 6.

[9] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/1626.

[10] "An Overview of the Federal Wiretap Act, Electronic Communications Privacy Act, and State Two-Party Consent Laws of Relevance to the NebuAd System and Other Uses of Internet Traffic Content from ISPs for Behavioral Advertising," Appendix A to Statement of Alissa Cooper, Chief Computer Scientist, Center for Democracy & Technology, before the House Committee on Energy and Commerce, Subcommittee on Telecommunications and the Internet, "What Your Broadband Provider Knows About Your Web Use: Deep Packet Inspection and Communications Laws and Policies," July 17, 2008, http://www.cdt.org/files/pdfs/20080717cooper.pdf.

[11] Nicholas Bohm, Foundation for Information Policy Research, "The Phorm 'Webwise' System – a Legal Analysis," April 23, 2008, http://www.fipr.org/080423phormlegal.pdf.

[12] Harris Testimony, *supra* n. 7, p. 10.

[13] *Id.* at p. 11.

information are ISPs collecting or examining, and how long is that information retained? Are ISPs using DPI on a continuous basis or only intermittently, such as in response to security incidents or to sample traffic for aggregate usage analysis? Are third parties paying ISPs to use DPI to identify or manipulate or divert certain content? If so, for what purposes? In what circumstance – if any – have ISPs obtained the consent of their customers to conduct DPI? How has consent been obtained? In what circumstances do ISPs believe consent is not required?[14]

European regulators should conduct a similar inquiry, closely examining whether and how DPI is being used by ISPs and other network operators in Europe, in order to clarify how the Directive applies and to determine whether further regulation is needed. The Commission should also determine how, if at all, the new Telecoms Package will affect the use of DPI by ISPs. Based upon such inquiries, the Commission might develop legislation to limit the use of DPI and provide safeguards for its deployment in those cases where it is deemed appropriate.

Key CDT resources on DPI include:

"The Privacy Implications of Deep Packet Inspection," Testimony of Leslie Harris, President and CEO, Center for Democracy & Technology, before the House Committee on Energy and Commerce (April 23, 2009)
http://www.cdt.org/privacy/20090423_dpi_testimony.pdf

d. Location information

Increasingly, mobile phones and other Internet-connected devices are "location-enabled:" they are able to detect, store, and broadcast their physical location. Such devices support a wide array of location-based services and applications, such as maps and restaurant finders. As the accuracy of location data improves and as more location-based applications are developed, location will likely come to pervade the online experience.

While the increasing availability of location information paves the way for exciting new applications and services, it also raises several different kinds of privacy concerns. Because individuals carry their mobile devices with them, location data may be collected everywhere and at any time, often without user interaction. It can reveal not only where a person is but also what she is doing. For example, an individual's mobile phone can reveal the fact that she was at a particular medical clinic at a particular time. Location information can also be personally identifiable, even when the device that generates it is not. For many people, there is one location where they spend their daytime hours (at work) and one location where they spend their nighttime hours (at home). After a period of collecting those two data points, it becomes fairly easy to identify the person.

The Article 29 Working Party (WP) addressed location in its opinion of November 2005. The WP said that location data is covered by both the 1995 Directive and the 2002 E-Commerce Directive, requiring consent and giving subjects the rights of access and to

[14] *Id.* at pp. 3-4.

withdraw consent, among others.[15] Because of the sensitivity of the information collected, we agree that meaningful opt-in consent must be required for collection of location data.[16] However, consent does not by itself offer adequate privacy protection in an age where location enabled devices are becoming ubiquitous and data is frequently required to utilize very beneficial services.

Location information is an area in which technical standards can help implement legal rules. We want to bring to the attention of the Commission the activity of the Geographic Location/Privacy Working Group[17] of the Internet Engineering Task Force. This body has created Geopriv, a technical standard for defining and capturing a user's privacy preferences for their location information, and for binding those preferences to the actual location information itself. CDT played a key role in the development of the standard. While GeoPriv cannot guarantee that those rules will be honored in any given situation, it can be a critical element of a larger privacy framework (such as that created by EU law) that provides such guarantees. For example, if the law decrees that no location information can be distributed without the express permission of the person being tracked, GeoPriv could provide the means to grant or not grant such permission. This model, or one like it, could help developers build location-based systems and services that not only comport with the law but also make it easier for consumers to exercise control over their data. We emphasize, however, that even if GeoPriv standards become commonplace, governments will still need to mandate a comprehensive set of Fair Information Practices specific to location information in order for location privacy to be adequately protected.

Key CDT resources on location:

Alissa Cooper and John Morris, "Binding Privacy Rules to Location on the Web" (April 4, 2009) http://www.cdt.org/privacy/LocWebFinal.pdf

CDT Policy Post, "The Dawn of the Location-Enabled Web" (July 6, 2009) http://www.cdt.org/policy/dawn-location-enabled-web

---

[15] *See* Article 29 Working Party, "Opinion on the use of location data with a view to providing value-added services," 2130/05/EN WP115, November 2005, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf.

[16] Meaningful user controls would let individual users decide on their own terms how their location information will be used. Individuals should be able to decide with whom they share their location, what that information is used for, whether or not it gets disseminated further, and how long it's retained. Location-enabled technologies, including Web browsers, should be designed with these controls built in from the beginning, to allow individuals to manage their location data as it is collected. *See* CDT Policy Post, "The Dawn of the Location Enabled Web," July 6, 2009, http://www.cdt.org/policy/dawn-location-enabled-web.

[17] http://www.ietf.org/dyn/wg/charter/geopriv-charter.html.

John Morris and Jon Peterson, "Who's Watching You Now?" (January/February 2007) http://old.cdt.org/publications/20070100ieee.pdf (describing the GeoPriv standard for controlling disclosure of location information)

e. Re-identification of "anonymized" data

The Directive, like other privacy laws, applies to "personal data" and assumes that data otherwise pertaining to an individual can be stripped of identifying information as to render it, in effect, harmless to privacy interests. Article 2(a) defines personal data as "any information relating to an identified or identifiable natural 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." Article 6(e) requires that personal data must be "kept in a form which permits identification of data subject for no longer than necessary for the purposes for which the data were collected or for which they are further processed." Therefore, to allow data controllers to retain data for longer periods of time, or to take their data out of the ambit of the Directive altogether, the Directive relies, in part, on the ability of data controllers to "anonymize" or "de-identify" personal data.[18]

However, the question of whether de-identified personal data really stays anonymous is of increasing concern.[19] Researchers have identified ways in which data that would have been considered anonymous or de-identified under older standards is capable of being re-identified and tied back to the original data subject.[20]

This may pose special challenges under the Directive. Recital 26 of the Directive correctly notes that "[a]ccount 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."[21] Moreover, if data is re-identified in

---

[18] *See* Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," p. 31, Ver 0.99 SSRN: August 14, 2009. The Article 29 Working Party considered the problem in its "Opinion 4/2007 on the concept of personal data" (Opinion 4/2007), 01248/07/EN WP 136, p. 24, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

[19] *See* Michael Barbar and Tom Zeller Jr., "A Face Is Exposed for AOL Searcher No. 4417749," New York Times, August 9, 2006, *http://www.nytimes.com/2006/08/09/technology/09aol.html?_r=1&sq=aol%20data&st=Search&adxnnl=1&scp=2&adxnnlx=1262034171-J0pzIkEl93sbpKmhZ7NiCA, and* Erica Newland, "Netflix Needs to Put 'Privacy Risks' in Their Queue," September 30, 2009, http://www.cdt.org/blogs/erica-newland/netflix-needs-put-privacy-risks-their-queue.

[20] Center for Democracy & Technology, "Encouraging the Use of, and Rethinking Protections for De-Identified (and 'Anonymized') Health Data" (De-identification Paper), p. 8, June 2009, http://www.cdt.org/files/pdfs/20090625_deidentify.pdf. *See also* Ohm, supra n. 18, pp. 15-25.

[21] Opinion 4/2007, *supra* n. 18, at p. 24, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

Europe, it falls within the ambit of the Directive. However, the Directive does not clearly address what happens when data believed to be un-identifiable is sent to a third country and is then re-identified. Under the current rules, it might be possible for a data controller to de-identify data, taking that data out of the ambit of the Directive and allowing its movement to a third country. Then, the recipient in the third country might have the ability, through aggregation or statistical analysis, to re-identify the data. Unfortunately for European data subjects, it is possible under current law that the original controller will have complied with the Directive and the third country recipient would not be covered by the Directive, leaving little recourse in case of misuse.

In the US, the FTC has indicated that it will no longer draw a bright line between personally identifiable information ("PII") and non-PII for the purposes of behavioral advertising. The FTC staff recently stated that "the traditional notion of what constitutes PII versus non-PII is becoming less and less meaningful and should not, by itself, determine the protections provided for consumer data . . . [B]oth PII and non-PII raise privacy issues."[22]

The issue of de-identification has arisen in the context of health data, where it has been especially challenging to strip health data of personal identifiers in order to eliminate or reduce privacy concerns while still retaining information that can be used for research, public health and other purposes. CDT recently published a paper on de-identification of health data.[23] The paper identified three problems. First, not all uses of health data require identical levels of de-identification. Second, when the laws only recognize a distinction between fully identified data and fully de-identified data and the use of fully identified data is too broadly permitted there is little incentive for data controllers to use data that is less than fully identifiable. Third, changes in society and technology have made re-identification of health information easier and cheaper than ever before.

Key CDT resource on re-identification:

> "Encouraging the Use of, and Rethinking Protections for, De-Identified (and 'Anonymized') Health Data" (June 2009)
> http://www.cdt.org/files/pdfs/20090625_deidentify.pdf

2. Does the current legal framework meet these challenges?

For fifteen years, the Data Protection Directive has been a model for comprehensively protecting the personal data of consumers. While new technologies and the reality of globalization challenge the Directive, weakening the framework to make it more "flexible" is not the answer. At the same time, and in light of the new technologies discussed above, it is clear that there is a need for clarification and improvement.

---

[22] Federal Trade Commission Staff Report, "Self-Regulatory Principles For Online Behavioral Advertising: Behavioral Advertising Tracking, Targeting & Technology," February 2009, http://www.ftc.gov/opa/2009/02/behavad.shtm.

[23] De-identification Paper, supra n. 20, http://www.cdt.org/files/pdfs/20090625_deidentify.pdf.

CDT believes that a comprehensive set of FIPs offers the best framework for protecting personal data in the information age. The FIPs appear, with some variation, in many international data protection frameworks including not only the Directive but also the OECD guidelines of 1980 and the Council of Europe convention.[24] The FIPs are also generally accepted in the US. Even though they are not written into US law as comprehensively as they are in Europe, elements of the FIPs are found in the US "sectoral" privacy laws. Moreover, most recently, the FIPs were endorsed by the US Department of Homeland Security (DHS) as providing the best framework for analyzing the privacy of government information systems, even in the area of homeland security.[25]

In the US, the FTC is now conducting a reexamination of its privacy framework. In comments filed in November, CDT called upon the FTC to move beyond a privacy framework based on notice and consent and instead to adopt the full FIPs.[26] CDT strongly believes that the concept of FIPs has remained relevant for the digital age despite the dramatic advancements in information technology that have occurred since these principles were first developed. But the principles must be reemphasized and refocused to be relevant and effective in the 21st century. A robust set of modernized principles that would serve as the foundation for any self-regulation or legislation should contain the following:

- Transparency
- Individual participation
- Purpose specification
- Data minimization
- Use limitation
- Data quality and integrity
- Security
- Accountability and auditing[27]

The Directive generally embodies these principles and any revision should take care not

---

[24] The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html; The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981), http://conventions.coe.int/Treaty/EN/Treaties/HTML/108.htm.

[25] The DHS FIPs (2008), http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[26] "Refocusing the FTC's Role in Privacy Protection; Comments of the Center for Democracy & Technology in regards to the FTC Consumer Privacy Roundtable" (FTC Comments), p. 5, November 6, 2009, http://www.cdt.org/privacy/20091105_ftc_priv_comments.pdf.

[27] *Id.* *See* also "CDT Recommendations for Improving Consumer Privacy Protections," December 9, 2009, http://www.cdt.org/policy/online-behavioral-advertising-industry%E2%80%99s-current-self-regulatory-framework-necessary-still-in#3.

to weaken them. The privacy challenges posed by the vast array of 21st-century technologies and business practices require a greater emphasis on the broader set of substantive protections. The Commission has been a strong voice in favor of all of the Fair Information Practices and a clear statement of modern FIPs would be important.

3. What future action would be needed to address the identified challenges?

The challenges facing privacy can be addressed without any major revision to the Directive. Whatever the Commission does, CDT encourages all data protection regimes to implement the complete set of FIPs. In our comments to the FTC, CDT stated that the full set of FIPs "provides a generally accepted conceptual framework for privacy that will endure amidst new technology and business practices…. We strongly believe that a renewed focus on comprehensively applying these principles will significantly help to protect consumer privacy in the 21st century."[28] The Commission should continue to clarify and interpret the Directive to make clear how it applies to new technologies.

For further information, contact:

Leslie Harris
President and CEO
lharris@cdt.org

[28] FTC Comments, *supra* n. 26, at p. 6.