2. ***Does ECPA Prohibit Cookies?*** When a person interacts with a website, the site can record certain information about the person, such as what parts of the website the user visited, what the user clicked on, and how long the user spent reading different parts of the website. This information is called "clickstream data."

Websites use "cookies" to identify particular users.[55] A cookie is a small text file that is downloaded into the user's computer when a user accesses a web page. The text in a cookie, which is often encoded, usually includes an identification number and several other data elements, such as the website and the expiration date. The cookie lets a website know that a particular user has returned. The website can then access any information it collected about that individual on her previous visits to the website. Cookies can also be used to track users as they visit multiple websites.

In *In re Doubleclick Inc. Privacy Litigation*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001), a group of plaintiffs challenged DoubleClick's use of cookies under the Stored Communications Act (SCA) and Wiretap Act. In 2001, DoubleClick was the leading company providing online advertising. DoubleClick helps advertisers distribute advertisements to websites based on

---

[55] For a discussion of the *DoubleClick* case, see Tal Zarsky, *Cookie Viewers and the Undermining of Data-Mining: A Critical Review of the DoubleClick Settlement*, 2002 Stan. Tech. L. Rev. 1.

information about specific web surfers. When a person visits a DoubleClick-affiliated website, DoubleClick places a cookie on that person's computer. As the person visits other sites that use DoubleClick, it builds a profile of that person's web surfing activity. DoubleClick then can target ads to specific people based on their profile. For example, suppose a news website uses DoubleClick. A person visits the news website. The website checks with DoubleClick to see if DoubleClick recognizes the person. If the person's computer has a DoubleClick cookie, DoubleClick then looks up the profile associated with the cookie and sends the website advertisements tailored to that person's interests. Suppose Person A likes tennis and Person B likes golf. When Person A goes to the news website, a banner ad for tennis might appear. When Person B visits the same site, a banner ad for golf might appear.

The plaintiffs in the *DoubleClick* case raised an SCA claim and a Wiretap Act claim. Regarding the SCA claim, the Act provides:

> [W]hoever (1) intentionally accesses without authorization a facility through which an electronic information service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains . . . access to a wire or electronic communication while it is in electronic storage in such system shall be punished. . . . 18 U.S.C. § 2701(a).

Although the court ultimately concluded that the SCA did not apply, its reasoning was very controversial. The court first held that an individual's computer, when connected to the Internet, was a "facility through which an electronic information service is provided." This means that when DoubleClick accessed cookies on people's computers, it was "intentionally access[ing] without authorization a facility through which an electronic information service is provided." However, the consent exception to this provision of the SCA is that "users" may authorize access "with respect to a communication of or intended for that user." § 2701(c). The individuals whose computers were accessed were obviously users, and they did not consent. But the websites that the users visited that used DoubleClick cookies were also "users" in the court's interpretation, and they consented. Only one party needs to consent for the SCA consent exception to apply.

Moreover, the court noted that the SCA only applies to "temporary, intermediate storage of a wire or electronic communication," § 2510(17), and that DoubleClick's cookies were not "temporary" because they exist on people's hard drives for a virtually infinite time period.

Commentators argue that the court's application of the SCA is wrong because a "facility" refers to an Internet Service Provider, not an individual computer. Indeed, this was the conclusion of *In re Pharmatrak.* Consider Orin Kerr:

> [T]he Stored Communications Act regulates the privacy of Internet account holders at ISPs and other servers; the law was enacted to create by statute a set of Fourth Amendment-like set of rights in stored records held by ISPs. The theory of the *Doubleclick* plaintiffs turned this framework on its head, as it

> attempted to apply a law designed to give account holders privacy rights in information held at third-party ISPs to home PCs interacting with websites.[56]

Regarding the Wiretap Act claim, DoubleClick conceded, for the purposes of summary judgment, that it had "intercepted" electronic communications. Orin Kerr also takes issue with this concession:

> [T]he Wiretap Act prohibits a third-party from intercepting in real-time the contents of communications between two parties unless one of the two parties consents. This law had no applicability to Doubleclick's cookies, as the cookies did not intercept any contents and did not intercept anything in real-time. The cookies merely registered data sent to it from Doubleclick's servers.[57]

DoubleClick argued that even if it intercepted electronic communications, the consent exception applied, since one party (the websites using DoubleClick) consented. The court agreed. The consent exception, however, does not apply if even with consent the "communication is intercepted for the purpose of committing any criminal or tortious act." 18 U.S.C. § 2511(2)(d). The court concluded: "DoubleClick's purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money by providing a valued service to commercial Web sites."

3. ***Web Bugs.*** Beyond cookies, another device for collecting people's data is called a "web bug." As one court describes it, web bugs (or "action tags") are very tiny pixels on a website that can record how a person navigates around the Internet. Unlike a cookie, which can be accepted or declined by a user, a web bug is a very small graphic file that is secretly downloaded to the user's computer. Web bugs enable the website to monitor a person's keystrokes and cursor movement. Web bugs can also be placed in e-mail messages that use HTML, or HyperText Markup Language. E-mail using HTML enables users to see graphics in an e-mail. A web bug in an e-mail message can detect whether the e-mail was read and to whom it was forwarded. According to computer security expert Richard M. Smith, a web bug can gather the IP address of the computer that fetched the web bug; the URL of the page that the web bug is located on; the URL of the web bug image; the time the web bug was viewed; the type of browser that fetched the web bug image; and a previously set cookie value. Is the use of a web bug a violation of federal electronic surveillance law?