Privacy and Information Security Law

Randy Canis

CLASS 15

Marketing and Tracking;
Cookies and Transactional Marketing

Domestic Cookies Litigation

2

In re DoubleClick Inc. Privacy Litigation

- 2001 S.D.NY
- Issue
  - Do the use of advertising cookies violate Internet users' rights?

3

In re DoubleClick Inc. Privacy Litigation

Possible Causes of Action

•Federal Law

1)18 U.S.C. §2701 - Electronic Communications Privacy Act ("ECPA")

2)18 U.S.C. §2510 - Federal Wiretap Act ("Wiretap Act"), -

3)18 U.S.C. §1030 - Computer Fraud and Abuse Act ("CFAA")

•State Law

1)Common law invasion of privacy;

2)Common law unjust enrichment;

3)Common law trespass to property; and

4)Sections 349(a) and 350 of Article 22A of the New York General Business Law.

4

In re DoubleClick Inc. Privacy Litigation

- "DoubleClick specializes in collecting, **compiling and analyzing information about Internet users** through proprietary technologies and techniques, and using it to target online advertising. DoubleClick has placed **billions of advertisements** on its clients' behalf and its services reach the majority of Internet users in the United States."

5

In re DoubleClick Inc. Privacy Litigation

- "When users visit any of these DoubleClick-affiliated Web sites, a 'cookie' is placed on their hard drives.[] Cookies are computer programs commonly used by Web sites to store useful information such as usernames, passwords, and preferences, making it easier for users to access Web pages in an efficient manner. However, Plaintiffs allege that **DoubleClick's cookies collect 'information that Web users, … consider to be personal and private**, such as names, e-mail addresses, home and business addresses, telephone numbers, searches performed on the Internet, Web pages or sites visited on the Internet and other communications and information that users would not ordinarily expect advertisers to be able to collect.' [] DoubleClick's cookies store this personal information on users' hard drives until DoubleClick electronically accesses the cookies and uploads the data."

6

In re DoubleClick Inc. Privacy Litigation

- "The cookies capture certain parts of the communications that users send to DoubleClick-affiliated Web sites. They collect this information in three ways: (1) 'GET' submissions, (2) 'POST' submissions, and (3) 'GIF' submissions."

7

In re DoubleClick Inc. Privacy Litigation

- **GET information** – part of the URL string that essentially is the query
- **POST information** – info filled into forms on a webpage
- **GIF information** – GIF tags are the size of a single pixel and are invisible to users. Unseen, they record the users' movements throughout the affiliated Web site, enabling DoubleClick to learn what information the user sought and viewed

8

In re DoubleClick Inc. Privacy Litigation

- Opting-Out
- "[U]sers can easily and at no cost prevent DoubleClick from collecting information from them. They may do this in two ways: (1) visiting the DoubleClick Web site and requesting an **'opt-out' cookie**; and (2) configuring their browsers to **block any cookies** from being deposited."

9

In re DoubleClick Inc. Privacy Litigation

- "In June 1999, DoubleClick purchased Abacus Direct Corp. ("Abacus") for more than one billion dollars. Abacus was a direct-marketing services company that maintained a database of names, addresses, telephone numbers, retail purchasing habits and other personal information on approximately ninety percent of American households, which it sold to direct marketing companies. Plaintiffs allege that **DoubleClick planned to combine its database of online profiles with Abacus' database of offline customer profiles in order to create a super-database capable of matching users' online activities with their names and addresses**. …"

10

In re DoubleClick Inc. Privacy Litigation

- “On March 2, 2000, Kevin O'Connor, DoubleClick's CEO and Chairman of the Board, announced that he had made a ‘mistake’ by planning to merge DoubleClick's and Abacus' databases and stated that DoubleClick would undertake **no such merger until it reached an agreement with the United States government and Internet industry regarding privacy standards**. It is unclear whether DoubleClick had already merged any of the information.”

11

In re DoubleClick Inc. Privacy Litigation

- ECPA offense from cookie placement
- "(a) Offense. Except as provided in subsection (c) of this section whoever(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...."

12

In re DoubleClick Inc. Privacy Litigation

- ECPA Exception (as defense)
- "(c) Exceptions.-Subsection (a) of this section does not apply with respect to conduct authorized... (2) by a user of that [wire or electronic communications] service with respect to a communication of or intended for that user;"

13

In re DoubleClick Inc. Privacy Litigation

- "Assuming that the communications are considered to be in 'electronic storage,' it appears that plaintiffs have adequately pled that **DoubleClick's conduct constitutes an offense under §2701(a), absent the exception under §2701(c)(2)**. Therefore, the issue is whether DoubleClick's conduct falls under §2701(c)(2)'s exception. This issue has three parts: (1) what is the relevant electronic communications service?; (2) were DoubleClick-affiliated Web sites 'users' of this service?; and (3) did the DoubleClick-affiliated Web sites give DoubleClick sufficient authorization to access plaintiffs' stored communications 'intended for' those Web sites?"

14

In re DoubleClick Inc. Privacy Litigation

- Who is a user under the ECPA?

18 U.S.C. §2510(13) "user" means any person or entity who—

(A) uses an electronic communication service; and

(B) is duly authorized by the provider of such service to engage in such use

15

In re DoubleClick Inc. Privacy Litigation

- Websites are also "users" under the ECPA
  - Users means person or entity
  - People and entities sign up for Internet access

16

In re DoubleClick Inc. Privacy Litigation

18 U.S. Code § 2701(a) Offense.—Except as provided in subsection (c) of this section whoever—

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

17

In re DoubleClick Inc. Privacy Litigation

18 U.S. Code § 2701(c) Exceptions.—Subsection (a) of this section does not apply with respect to conduct authorized—

(1) by the person or entity providing a wire or electronic communications service;

(2) by a user of that service with respect to a communication of or intended for that user; or

(3) in section 2703, 2704 or 2518 of this title.

18

In re DoubleClick Inc. Privacy Litigation

- "[P]aintiffs [also] argue that '[t]he individual plaintiff ("user") owns the personal computer ("facility"), while the Web sites she visits do not. [And that] [u]nder basic property and privacy notions, therefore, only she can authorize access to her own messages stored on that facility.' [] Again, plaintiffs seem to ignore the statute's plain language. The general rule under §2701(a) embodies plaintiffs' position that only those authorized to use a 'facility' may consent to its access. Nevertheless, **Congress explicitly chose to make §2701(a)'s general rule subject to §2701(c)(2)'s exception for access authorized by authors and intended recipients of electronic communications.** Thus, plaintiffs' argument is essentially that this Court should ignore §2701(c)(2) because Congress failed to take adequate account of 'basic property and privacy notions.' However, it is not this Court's role to revisit Congress' legislative judgments."

19

In re DoubleClick Inc. Privacy Litigation

- "Examining DoubleClick's technological and commercial relationships with its affiliated Web sites, we find it **implausible to infer that the Web sites have not authorized DoubleClick's access**. In a practical sense, the very reason clients hire DoubleClick is to target advertisements based on users' demographic profiles. DoubleClick has trumpeted this fact in its advertising, patents and Securities and Exchange filings. [] True, officers of certain Web sites might not understand precisely how DoubleClick collects demographic information through cookies and records plaintiffs' travels across the Web. However, that knowledge is irrelevant to the authorization at issue. **Title II in no way outlaws collecting personally identifiable information or placing cookies**…"

20

In re DoubleClick Inc. Privacy Litigation

- "**Plaintiffs' GET, POST and GIF submissions to DoubleClick-affiliated Web sites are all 'intended for' those Web sites**. In the case of the GET and POST submissions, users voluntarily type-in information they wish to submit to the Web sites, information such as queries, commercial orders, and personal information. GIF information is generated and collected when users use their computer 'mouse' or other instruments to navigate through Web pages and access information. Although the users' requests for data come through clicks, not keystrokes, they nonetheless are voluntary and purposeful. Therefore, **because plaintiffs' GET, 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)**."

21

In re DoubleClick Inc. Privacy Litigation

18 U.S. Code § 2510(17) "electronic storage" means—

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication;

22

In re DoubleClick Inc. Privacy Litigation

- "Section 2510(17) (A)'s language and legislative history make evident that 'electronic storage' is not meant to include DoubleClick's cookies either. Rather, it appears that the section is specifically targeted at communications temporarily stored by electronic communications services incident to their transmission …"

23

In re DoubleClick Inc. Privacy Litigation

- "[I]t is clear that DoubleClick's cookies fall outside §2510(17)'s definition of electronic storage and, hence, § 2701's scope. … [B]ecause the cookies and their identification numbers are never in 'electronic storage' under the ECPA, they are not protected by Title II and DoubleClick cannot be held liable for obtaining them.

24

In re DoubleClick Inc. Privacy Litigation

- "To summarize, plaintiffs' GET, POST and GIF submissions are excepted from §2701(c) (2) because they are 'intended for' the DoubleClick-affiliated Web sites who have authorized DoubleClick's access. The cookie identification numbers sent to DoubleClick from plaintiffs' computers fall outside of Title II's protection because they are not in 'electronic storage' and, even if they were, DoubleClick is authorized to access its own communications."

25

In re DoubleClick Inc. Privacy Litigation

- "The Wiretap Act provides for criminal punishment and a private right of action against:[]
  - 'any person who(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept wire, oral, or electronic communication [except as provided in the statute].' 18 U.S.C. §2511."

26

In re DoubleClick Inc. Privacy Litigation

- "DoubleClick claims that its actions fall under an explicit statutory exception:
  - 'It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception *unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or any State*.' 18 U.S.C. §2511(2)(d) ('§2511(2)(d)') (emphasis added)."

27

In re DoubleClick Inc. Privacy Litigation

- "To summarize, we find that the **DoubleClick-affiliated Web sites are 'parties' to plaintiffs' intercepted communications under the Wiretap Act and that they consent to DoubleClick's interceptions**. Furthermore, we find that plaintiffs have failed to allege that DoubleClick has intercepted plaintiffs' communications for a 'criminal or tortious' purpose. Accordingly, we find that DoubleClick's actions are exempted from liability under the Wiretap Act by §2511(2)(d) and, thus, we dismiss Claim II."

28

In re DoubleClick Inc. Privacy Litigation

- CFAA
- "[18 U.S.C. § 1030] (a) whoever ... (2)(c) intentionally accesses a computer without authorization, or exceeds authorized access, and thereby obtains ... information from any protected computer if the conduct involved an interstate or foreign communication ... shall be punished as provided in subsection (c) of this section."

29

In re DoubleClick Inc. Privacy Litigation

- "However, section 18 U.S.C. §1030(e)(8) ('§1030(e)(8)') limits the 'damage' civilly recoverable to the following instances:
  - '(e)(8) the term `damage' means any impairment to the integrity or availability of data, a program, a system, or information that *(A) causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals*; [B. Impairs medical care; C. Causes physical injury; D. Threatens public health or safety].' (emphasis added)"

30

In re DoubleClick Inc. Privacy Litigation

- "[T]o the extent that some value could be placed on these losses, we find that the plaintiffs have failed to allege facts that could support the inference that the damages and losses plaintiffs incurred from DoubleClick's access to any *particular* computer, over one year's time, could meet §1030(e)(8) (A)'s damage threshold. Accordingly, Count III of the Amended Complaint is dismissed."

31

In re DoubleClick Inc. Privacy Litigation

- State Claims
- Dismissed because now no basis for the case to be heard in Federal Court….

32

In re Pharmatrak, Inc. Privacy Litigation

- 2003 1st Circuit
- Issue
  - Does the collection of personal and identifying information through the web violate the ECPA?

33

In re Pharmatrak, Inc. Privacy Litigation

- "We hold that the district court incorrectly interpreted the 'consent' exception to the ECPA; we also hold that Pharmatrak 'intercepted' the communication under the statute. We reverse and remand for further proceedings. This does not mean that plaintiffs' case will prevail: there remain issues which should be addressed on remand, particularly as to whether defendant's conduct was intentional within the meaning of the ECPA."

34

In re Pharmatrak, Inc. Privacy Litigation

- "When a user visited the website of a Pharmatrak client, Pharmatrak's HTML code instructed the user's computer to contact Pharmatrak's web server and retrieve from it a tiny, invisible graphic image known as a '**clear GIF**' (or a '**web bug**'). The purpose of the clear GIF was to cause the user's computer to communicate directly with Pharmatrak's web server. **When the user's computer requested the clear GIF, Pharmatrak's web servers responded by either placing or accessing a 'persistent cookie' on the user's computer**. On a user's first visit to a webpage monitored by NETcompare, Pharmatrak's servers would plant a cookie on the user's computer. If the user had already visited a NETcompare webpage, then Pharmatrak's servers would access the information on the existing cookie."

35

In re Pharmatrak, Inc. Privacy Litigation

- "While it was marketing NETcompare to prospective pharmaceutical clients, **Pharmatrak repeatedly told them that NETcompare did not collect personally identifiable information**. It said its technology could not collect personal information, and specifically provided that the information it gathered could not be *used* to identify particular users by name. … Michael Sonnenreich, Chief Executive Officer of Pharmatrak, stated unequivocally at his deposition that none of his company's clients consented to the collection of personally identifiable information."

36

In re Pharmatrak, Inc. Privacy Litigation

- "The following **personal information was found on Pharmatrak servers**: names, addresses, telephone numbers, email addresses, dates of birth, genders, insurance statuses, education levels, occupations, medical conditions, medications, and reasons for visiting the particular website.[] Pharmatrak also occasionally recorded the subject, sender, and date of the web-based email message a user was reading immediately prior to visiting the website of a Pharmatrak client. Most of the individual profiles assembled by plaintiffs' expert contain some but not all of this information."

37

In re Pharmatrak, Inc. Privacy Litigation

- "**On the undisputed facts, the client pharmaceutical companies did not give the requisite consent**. The pharmaceutical clients sought and received assurances from Pharmatrak that its NETcompare service did not and could not collect personally identifiable information. Far from consenting to the collection of personally identifiable information, the pharmaceutical clients explicitly conditioned their purchase of NETcompare on the fact that it would not collect such information."

38

History Sniffing

39

In the Matter of Epic Marketplace, Inc

- "Epic is an advertising company that engages in **online behavioral advertising**, which is the practice of **tracking a consumer's online activities** in order to deliver advertising targeted to the consumer's interests."

40

In the Matter of Epic Marketplace, Inc

- "Epic purchases advertising space on publishers' websites and contracts with advertisers to place their advertisements on the websites."

41

In the Matter of Epic Marketplace, Inc

- "Epic collects data on consumers who visit the websites within the Epic Marketplace Network. When a consumer visits a website within the Epic Marketplace Network, **Epic sets a new cookie in the consumer's browser or automatically receives a cookie it previously set**. Cookies are small text files that are commonly used to store information about a consumer's online activities, including information such as the content of advertisements that a consumer views or the pages a consumer visits within a particular website."

42

In the Matter of Epic Marketplace, Inc

- Epic engaged in history sniffing
- "'**[H]istory sniffing**' … is the practice of determining whether a consumer has previously visited a webpage by checking how a user's browser styles the display of a hyperlink. For example, if a consumer has previously visited a webpage, the hyperlink to that webpage may appear in purple, and if the consumer has not previously visited a webpage, the hyperlink may appear in blue. History-sniffing code would sniff whether the consumer's hyperlinks to specific webpages appeared in blue or purple."

43

In the Matter of Epic Marketplace, Inc

- "The code allowed Epic to determine whether a consumer had visited any of over 54,000 domains. Among the domains that Epic 'sniffed' were pages relating to fertility issues, impotence, menopause, incontinence, disability insurance, credit repair, debt relief, and personal bankruptcy. … Based upon its knowledge of which domains a consumer had visited, **Epic assigned the consumer an interest segment**. Epic's interest segments included sensitive categories such as 'Incontinence,' 'Arthritis,' 'Memory Improvement,' and 'Pregnancy-Fertility Getting Pregnant.' **Epic used this history-sniffing data for behavioral targeting purposes**."

44

In the Matter of Epic Marketplace, Inc

- "History sniffing **circumvents** the most common and widely known method consumers use to **prevent online tracking**: deleting cookies. **Deleting cookies does not prevent a website from querying a consumer's browsing history**. Consumers could only protect against history sniffing by deleting their browsing history and using private browsing mode, or, with regard to Epic's history sniffing, opting out of receiving targeted advertisements from Epic."

45

In the Matter of Epic Marketplace, Inc

- Privacy Policy
  - "Epic Marketplace automatically receives and records anonymous information that your browser sends whenever you visit a website which is part of the Epic Marketplace Network. We use log files to collect Internet protocol (IP) addresses, browser type, Internet service providers (ISP), referring/exit pages, platform type, date/time stamp, one or more cookies that may uniquely identify your browser, and responses by a web surfer to an advertisement delivered by us."

46

In the Matter of Epic Marketplace, Inc

- "Respondents' statement describing their privacy and online behavioral targeting practices did not disclose that Epic was engaged in history sniffing."

47

In the Matter of Epic Marketplace, Inc

- "In settling the FTC's complaint, Epic Marketplace, Inc., and Epic Media Group, LLC **agreed to no longer use history sniffing**, which allows online operators to test specific sites in a browser to see if consumers have visited those sites in the past. The companies are required to delete and destroy all data collected using the technology."

48

Self-Regulatory by Trade Organizations and the FTC

49

2013 NAI Code of Conduct

- "The Network Advertising Initiative ("NAI") is the leading self-regulatory body governing "third parties" in the online advertising ecosystem. The NAI is currently composed of more than 90 member companies and expanding."

50

2013 NAI Code of Conduct

- "The NAI Code governs only NAI member companies. It does not govern all data collection by member companies, but is limited to their **'Interest Based Advertising' and 'Ad Delivery Reporting' activities** as defined in this Code."

51

2013 NAI Code of Conduct

- Applies to the US only
- Technology neutral
- "NAI Code applies only to NAI members, and only to the extent they are engaged in activities addressed by the NAI Code."

52

2013 NAI Code of Conduct

3 Categories of data

1)Personally Identifiable Information (PII)

2)Non-PII

3)De-Identified Data

53

2013 NAI Code of Conduct

- PII
- "[A]ny information used or intended to be used to identify a particular individual, including name, address, telephone number, email address, financial account number, and government-issued identifier."

54

2013 NAI Code of Conduct

- De-Identified Data
- "[D]ata not linked or reasonable linkable to a particular company or device."

55

2013 NAI Code of Conduct

- Transparency requirement including a privacy notice and an ability to opt-out
- Appropriate level of user control including various opt-outs and opt-ins depending upon data type and usage

56

2013 NAI Code of Conduct

- Use Limitations
- Transfer Restrictions
- Data Access, Quality, Security, and Retention

57

2013 NAI Code of Conduct

- Accountability including annual compliance reviews and reports and an ability for users to submit questions and concerns

58

Self-Regulatory Principles For Online Behavioral Advertising

- FTC 2009 Analysis

59

Self-Regulatory Principles For Online Behavioral Advertising

- **Online behavioral advertising** – "the practice of tracking an individual's online activities in order to deliver advertising tailored to the individual's interests"

60

Self-Regulatory Principles For Online Behavioral Advertising

- Type of Activity
- "In many cases, the information collected is not personally identifiable in the traditional sense – that is, the information does not include the consumer's name, physical address, or similar identifier that could be used to identify the consumer in the offline world. Instead, businesses generally use 'cookies' to track consumers' activities and associate those activities with a particular computer or device."

61

Self-Regulatory Principles For Online Behavioral Advertising

- Asserted Benefits
- "[D]elivering more relevant ads to consumers, subsidizing free online content, and allowing businesses to market more precisely and spend their advertising dollars more effectively."

62

Self-Regulatory Principles For Online Behavioral Advertising

- 4 concepts in the original principals

1)transparency and control

2)reasonable security and limited data retention

3)material changes to privacy policies

4)obtain affirmative express consent before use of sensitive data

63

Self-Regulatory Principles For Online Behavioral Advertising

- "1. Transparency and Consumer Control
- Every website where data is collected for behavioral advertising should provide a **clear, concise, consumer-friendly, and prominent statement** that (1) data about consumers' activities online is being collected at the site for use in providing advertising about products and services tailored to individual consumers' interests, and (2) consumers can choose whether or not to have their information collected for such purpose. The website should also provide consumers with a clear, easy-to-use, and **accessible method for exercising this option**. Where the data collection occurs outside the traditional website context, companies should develop alternative methods of disclosure and consumer choice that meet the standards described above (i.e., clear, prominent, easy-to-use, etc.)"

64

Self-Regulatory Principles For Online Behavioral Advertising

- "2. Reasonable Security, and Limited Data Retention, for Consumer Data
- Any company that collects and/or stores consumer data for behavioral advertising should provide **reasonable security** for that data. Consistent with data security laws and the FTC's data security enforcement actions, such protections should be based on the sensitivity of the data, the nature of a company's business operations, the types of risks a company faces, and the reasonable protections available to a company. Companies should also **retain data only as long as is necessary** to fulfill a legitimate business or law enforcement need."

65

Self-Regulatory Principles For Online Behavioral Advertising

- "3. Affirmative Express Consent for Material Changes to Existing Privacy Promises
- As the FTC has made clear in its enforcement and outreach efforts, a company must keep any promises that it makes with respect to how it will handle or protect consumer data, even if it decides to change its policies at a later date. Therefore, **before a company can use previously collected data in a manner materially different from promises the company made when it collected the data, it should obtain affirmative express consent from affected consumers**. This principle would apply in a corporate merger situation to the extent that the merger creates material changes in the way the companies collect, use, and share data."

66

Self-Regulatory Principles For Online Behavioral Advertising

- "4. Affirmative Express Consent to (or Prohibition Against) Using Sensitive Data for Behavioral Advertising
- Companies should collect **sensitive data** for behavioral advertising only after they **obtain affirmative express consent from the consumer** to receive such advertising."

67

European Cookies

68

Directive 2002/58/EC (as Amended)

69

Directive on privacy and electronic communications

- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

70

Directive on privacy and electronic communications

- "(24) 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**."

71

Directive on privacy and electronic communications

- "(25) However, such devices, for instance so-called "**cookies**", can be a **legitimate and useful tool**, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions. Where such devices, for instance cookies, are **intended for a legitimate purpose**, such as to facilitate the provision of information society services, their use should be **allowed on condition that users are provided with clear and precise** information in accordance with Directive 95/46/EC **about the purposes of cookies or similar devices** so as to ensure that users are made aware of information being placed on the terminal equipment they are using. **Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment.**"

72

Directive on privacy and electronic communications

- This is particularly important where users other than the original user have access to the terminal equipment and thereby to any data containing privacy-sensitive information stored on such equipment. Information and the right to refuse may be offered once for the use of various devices to be installed on the user's terminal equipment during the same connection and also covering any further use that may be made of those devices during subsequent connections. The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible. **Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose**."

73

Program Completed