Delta Airlines suffers privacy boycott

Eugene Oscapella finds that consumers are starting to challenge corporate privacy intrusions by hitting them where it hurts - sales revenues.

The consumer purse is a powerful incentive for companies to respect privacy. One vehicle for flexing the muscle of that purse - the consumer boycott - is being tested on an American air carrier, Delta Airlines, at a time when the airline industry is already on its knees because of weak travel demand.

Bill Scannell, a software executive based in Austin, Texas, began a boycott campaign through his "boycottdelta.org" website in March. His call for a boycott may give many companies good reason to reflect on their privacy practices.

In a recent interview with *PL&B International*, Scannell explained the simplicity of his quest - to be able to travel freely in the United States without having to confront internal border controls. Scannell's immediate concern arose over the cooperation between Delta Airlines and the US Transportation Security Administration on a passenger screening programme. Delta Airlines agreed to test the US CAPPS-II programme, a travellers' profiling system that intends to use extensive data mining of credit history, criminal records, and travel patterns, among other sources of information, to profile all airline passengers.

According to Scannell, Delta began running intrusive background checks in March on anyone who flies Delta from one of three undisclosed airports. These involved credit, banking history and criminal background checks.

Scannell explained to *PL&B International* that if governments do not respond to the privacy concerns of their citizens, the appropriate response may be to "follow the money trail" to the businesses that are cooperating with governments in undertaking intrusive behaviours. In other words, the strongest action that individuals can take to assert their privacy rights may be to withhold their custom from these businesses. It is difficult to take on a government, argues Scannell, but consumers can always use their collective financial might to encourage more responsible corporate behaviour.

Boycotts can have another benefit, he notes. Many groups have written papers about profiling systems such as that being used by Delta. However, most have failed to get the attention of the media or correct the offending conduct. His "Boycott Delta" programme, on the other hand, resulted in extensive coverage on *CNN* and in major media such as the *New York Times*.

> the strongest action that individuals can take to assert their privacy rights may be to withhold their custom

Scannell said that he stopped keeping statistics on visits to his "boycottdelta.org" website in late April, by which time the site had received over six million "hits". By the start of June, he had received 8,900 e-mails on the issue.

FURTHER INFORMATION: For details on the Delta Airlines boycott, see: www.boycottdelta.org

News in brief

SECURITY

A security flaw in Microsoft's Net.Passport authentication service could have exposed the accounts of around 200 million users, according to IT analysts, Gartner. Microsoft has said that it fixed the flaw within eight hours of discovery. However, according to *NewsFactor.com*, the Federal Trade Commission (FTC) may investigate whether the flaw violated the terms of a privacy settlement reached last year between Microsoft and the FTC (see *PL&B International*, September 2002, p.15).

Staff at UK broadcaster, the BBC, are being advised not to use a new internal intranet system set up for registering conflicts of interest. According to *the Guardian*, broadcasting unions are concerned that allegedly lax security controls could leave employee data exposed and the BBC in breach of the Data Protection Act. It is claimed that anyone who knows an employee's name and staff number could gain access to their records. A spokesperson for the BBC has denied that the system breaches the Data Protection Act.

A survey of 500 US workers dealing with customer information has revealed that 66 per cent believe their colleagues present the greatest threat to customer privacy. According to the survey, conducted by Harris Interactive (on behalf of IT security firm Vontu), nearly 70 per cent of respondents said their company had policies regulating the disclosure of personal data. Yet, around 80 per cent said they had not read it. 45 per cent said that it would be easy for a colleague to remove sensitive customer data from the corporate network.

News in brief

ONLINE PRIVACY

On 28th May, the Committee of Ministers of the Council of Europe adopted a declaration on freedom of communication on the Internet. The purpose behind the declaration is to strike a balance between freedom of expression and other rights under the European Convention of Human Rights, such as the Article 8 right to privacy. For the full text of the declaration: www.coe.int

A group of scientists has warned a US House of Representatives Government Reform Committee over the privacy dangers of peer-to-peer file sharing. Programmes such as Kazaa and Morpheus allow users (often employees) to link up their computers and share files online. But scientists have said that failure to properly set up the programmes could leave confidential information such as e-mail, legal documents and password lists, open to outsiders.

The US Direct Marketing Association has condemned the so-called practices of e-mail 'harvesting' and 'dictionary attacks' which are used by spam merchants to compile vast marketing lists for unsolicited advertising. Such practices, says the DMA, constitute abuses of the right to send e-mail legitimately and could impact upon the use of e-mail as a key business communications tool.

The DMA has warned its members to abide by its four pillars of reputable e-mail marketing: (1) honest subject lines (2) accurate header information that has not been forged (3) include physical contact addresses for consumer redress (4) an opt-out that works.

According to e-mail solutions provider, MessageLabs, one in three e-mails is now unsolicited spam advertising. In March this year, MessageLabs analysed 104.9 million e-mails, discovering that 38.1 million were spam. Additional research found that nearly 60 per cent of spam originates from the US.

Unauthorised cookies could violate US federal wiretap law

A recent US Court of Appeals decision provides valuable insight into the legal implications of collecting personal data through web cookies. By **William B Baker**

The US Court of Appeals for the First Circuit ruled on May 9th that a web services company may have violated the Electronic Communications Privacy Act (ECPA) by collecting personal information about consumers without the consent of the websites which the consumers were visiting. The decision, in *In re Pharmatrak, Inc. Privacy Litigation*, 2003 WL 21038761 (1st Cir. 2003), marks an important interpretation of ECPA and has broad implications for the use of third-party cookies in collecting information about individuals who visit Internet websites.

PHARMATRAK'S SERVICE

The Pharmatrak litigation arose from an arrangement by which Pharmatrak provided website monitoring services for a number of pharmaceutical companies. The Pharmatrak service collected information about visitors to the client companies' websites that would be used for intra-industry comparisons of website traffic and usage. For example, Pharmatrak would track whether visitors were first-time or repeat visitors, the "referrer pages" from which they came and similar information. Important to the Court's decision was evidence that the pharmaceutical companies did not want Pharmatrak to collect personal or identifying data about their site visitors.

Pharmatrak provided its service, called "NETcompare", through the use of a "web bug" or "clear GIF"—a tiny graphical image not noticeable by the casual user. HTML code in the pharmaceutical company website would retrieve the web bug from the Pharmatrak server, and Pharmatrak would place a cookie on the user's computer.

Although Pharmatrak denied any intent to collect personal information, several configurations of website usage in fact allowed Pharmatrak to collect personal information about a small number of users of certain sites. In discovery, plaintiffs' expert was able to find detailed user profiles of 232 users on Pharmatrak's servers (Pharmatrak set some 18.7 million cookies during the relevant period).

In their class-action complaint, plaintiffs sued both Pharmatrak and the pharmaceutical companies, declaring that the arrangement violated a number of federal and state privacy laws, including Titles I and II of ECPA, the Computer Fraud and Abuse Act and several Massachusetts statutory and common laws. The US District Court granted summary judgment to defendants on these claims. (See "Light Shining on Web Beacons," in the December 2002 edition of *Privacy In Focus*). On appeal to the First Circuit, plaintiffs sought review only of the District Court's dismissal of the claim based on Title I of ECPA.

ECPA TITLE I

Title I of ECPA extended to data and electronic transmissions the protections that prior federal law had accorded to oral and wire communications. Title I, in relevant part, creates a private right of action against a party who "intentionally intercepts…any…electronic communication." "Intercept" is the "acquisition of the contents of any...electronic...communication through the use of any electronic…device." ECPA establishes a defence of prior consent to an interception, which either party to the communication may provide.

The issues before the Court of Appeals were whether Pharmatrak's service had constituted an impermissible "interception" and, if so, whether its pharmaceutical clients had "consented" to such interception. Taking the latter question first, the Court of Appeals held that the burden of proving consent, at least in a civil case, fell upon Pharmatrak. The Court ruled that the party claiming consent must prove either actual consent or, in its absence, show "convincingly" that implied consent was given.

PHARMATRAK'S ACTIONS CLASSED AS "INTERCEPTION"

Second, the Court of Appeals held that Pharmatrak's collection of personal data constituted an "interception" under ECPA. After discussing whether ECPA requires that an "interception" must occur contemporaneously with the transmission that is intercepted, or whether some delay is possible, the Court ruled that Pharmatrak was engaged in an interception under even the narrowest interception standard. Specifically, the Court concluded that Pharmatrak's obtaining the data in real-time was sufficient to constitute an "interception" under ECPA.

In so holding, the Court was unpersuaded by Pharmatrak's argument that two separate communications had occurred — one between the user and the pharmaceutical company site, and a second between the user and Pharmatrak. The Court found that contention immaterial, holding that ECPA does not necessarily require the acquisition to be the "same communication" as the intercepted "transmission". "Separate, but simultaneous and identical, communications satisfy even the strictest real-time requirement."

The Court remanded the case to the District Court for further action on whether the "intent" requirement of ECPA was satisfied. The issue had not been briefed, and the Court found the record unclear on whether Pharmatrak had acquired the personal information through technical glitches unknown to it. Citing legislative history, the Court noted that inadvertent interceptions do not provide a basis for civil or criminal liability under ECPA.

> Consent to collections of personal data can be either express or implied, but both third-party providers and websites will want to address this topic directly in their contracting lest they become ensnarled in needless litigation.

NO CONSENT WAS GIVEN

On the facts, the Court ruled that consent was not present. Under the prevailing standard in the First Circuit, the Court ruled that the pharmaceutical companies' consent extended only to the communications that they had intended to allow. Said the Court: "Far from consenting to the collection of personally identifiable information, the pharmaceutical clients explicitly conditioned their purchase of [the Pharmatrak service] on the fact that it would not collect such information."

The Court distinguished this case from *In re DoubleClick Inc. Privacy Litigation*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001) and *Chance v Avenue A, Inc.*, 165 F. Supp. 2d 1163 (W.D. Wash. 2001) on the grounds that, in those cases, the host websites had enlisted the services of DoubleClick and Avenue A for the purpose of creating user profiles.

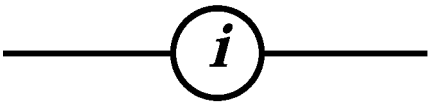
The Court also found that no consumer consent could be implied, because the pharmaceutical companies' websites "gave no indication that use meant consent to collection of personal information by a third party." The Court stated that "deficient notice will almost always defeat a claim of implied consent."

CASE IMPLICATIONS

The case is interesting for several reasons. First, the Court opted for a comparatively narrow definition of "consent" under ECPA. Under this approach, websites and in particular, third-party providers of monitoring services need to have clear understandings of what information is to be collected from or about web users. Consent to collections of personal data can be either express or implied, but both third-party providers and websites will want to address this topic directly in their contracting lest they become ensnarled in needless litigation.

Second, the Court held that third-party website monitoring could constitute an "interception" under ECPA. Accordingly, businesses engaged in profiling and tracking consumer data on other parties' websites must take steps to ensure that they do not run afoul of ECPA's restrictions, and may be at a competitive disadvantage relative to data-mining firms that do not monitor website activities.

Third, the Court did not address whether the use of "Web bugs" or "clear GIFs" is inherently illegal. Rather, the Court's analysis focused not on what the technology was, but rather on what it did. In that sense, the Court appears to have affirmed, at least in principle, the lower court's decision that web bugs are not, per se, nefarious or violations of ECPA.



AUTHOR: William B Baker is a partner in the Privacy, Internet & E-Commerce, Postal and Communications practices at Wiley Rein & Fielding in Washington, DC. He can be reached by telephone at: +1 202 719 7255 or E-mail: wbaker@wrf.com.

Benetton backs down over tracking technology

Plans to introduce hi-tech tracking devices into the retail sector have been met with stern opposition from consumer groups. **Eugene Oscapella** reports.

In apparent response to a boycott campaign launched by an American consumer interest group, CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering), the Benetton Group announced that it is not currently inserting tracking technology devices into its clothing. However, the global clothing retailer announced in the same April press release that it is now analysing RFID (Radio Frequency Identification) technology to evaluate its technical characteristics.

Benetton also announced that it reserved the right to "take the most appropriate decision to generate maximum value for its stakeholders and customers," suggesting that it has not discounted the use of such tracking devices in the future. The company produces and sells more than 100 million garments worldwide under its name.

CASPIAN's concern arose over a new consumer goods tracking system called Auto-ID, which couples radio frequency identification (RFID) technology with highly miniaturised computers. This permits products to be identified and tracked at any point along the supply chain. Each item would be uniquely identifiable through a numbering scheme called ePC ("electronic product code"). This would eventually replace the existing Universal Product Code (UPC). For example, tiny RFID devices (which Benetton refers to as "smart labels") could be implanted in clothing. An RFID reader could then identify the individual piece of clothing as it travelled from factory to transportation centre to retail shop.

Opponents of RFID fear uses of the technology can go far beyond simple inventory control. A purchase of clothing made with a credit card, for example, could link the purchaser and the item of clothing in a database. If the thirst for assembling masses of information in the name of national security and crime control continues (see, for example, "Total Information Awareness", *PL&B International*, Feb 2003, p.8) governments could use this tracking capability to monitor the movements of individuals through their clothing or other items they carry - without their knowledge or permission. Scanning devices placed at strategic locations - the entrance to a public gathering, for example - could identify any item of clothing or other product carrying an RFID chip.

> The European Central Bank is quietly working to embed RFID tags in the fibres of Euro bank notes by 2005...allowing police agencies to literally "follow the money"

Other databases may permit the items to be linked with a specific individual.

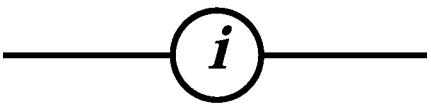
Katherine Albrecht, CASPIAN founder and director and a Harvard University doctoral candidate, spoke extensively about the potential secondary uses by government of such tracking devices at the April 2003 Computers, Freedom and Privacy Conference (CFP) in New York City and at the Privacy Activists Congress held the day after the CFP conference.

In a statement released in March urging the boycott of Benetton clothing, Albrecht explained the concerns about RFID technology: "Manufacturers of these chips are already promoting them as a way to track individuals and inventory their belongings. It would be easy for Benetton to link your name and credit card information to the serial number in your sweater, in essence 'registering' that sweater to you," she explained. "Then any time you go near an RFID reader device, the sweater could beam out your identity to anyone with access to the database - all without your knowledge or permission."

RFID technology can be highly miniaturised and will eventually become very inexpensive, according to Albrecht. RFID tags may cost less than one cent each by 2004, and can be as small as a grain of sand.

Albrecht also suggests that the European Central Bank is quietly working to embed RFID tags in the fibres of Euro bank notes by 2005. This would provide information about where the bank notes have been, allowing police agencies to literally "follow the money". "If and when RFID devices are embedded in banknotes," she wrote in one law journal article, "the anonymity that cash affords in consumer transactions will be eliminated."

What is the solution for consumers? Delegates at the CFP conference learned that the chips can be disabled by microwaving them - a new use for this staple kitchen product.



FURTHER INFORMATION: For details on the Benetton boycott, see: www.boycottbenetton.org/rfid_overview.html; www.boycottbenetton.org/press.html