

US Privacy decrees spark headlines, but where's the bottom line?

By Judith A Sullivan

US REGULATORS HAVE MADE A PLEDGE to get tough on privacy breaches in the corporate sector. But, will this hard line approach cut any ice with the corporations which count? *PL&B International* takes a look at the issues.

Federal Trade Commission (FTC) consent decrees with US giants such as Microsoft and Eli Lilly may warm the hearts of privacy advocates. However, the longer-term and somewhat thornier issue is the degree to which such events will force other companies to take the necessary steps to boost privacy protection for their customers.

The consensus of opinion is a resounding "maybe". Interviewing experts, examining comments sent to the FTC and looking at coverage in the US press, has revealed only slight behaviour changes on the part of companies for whom a breach of customer privacy could well lead to a public rap on the knuckles, or worse, steep fines.

Momentum has been building up over the past year. In August, the FTC and Microsoft signed a consent decree that calls on the IT giant to accurately describe the strengths and the limitations of its online authentication service, Net Passport (see *PL&B Int*, Sept 2002, p.15). The settlement is valid for 20 years and could cost Microsoft \$11,000 for each day of non-compliance. The FTC is expected to make a final decision on the settlement terms by the end of this year.

Another milestone occurred in January when pharmaceutical company Eli Lilly faced a similar complaint that led to a settlement with the FTC. The case followed the accidental disclosure by the Prozac maker of details for around 700 users of the anti-depressant drug. Though

the lapse was attributed to human error, it nonetheless led to financial penalties.

FTC staff attorney Ellen Finn defined both cases as landmarks. In the case of Eli Lilly, the FTC wanted to send the message that "inadvertent error can give rise to action." As to the more recent case, "there was an important message with Microsoft that goes beyond Lilly. We will not wait until there is a breach," said Finn.

SETTING AN EXAMPLE

"The FTC is serious about getting meaningful relief," Finn said. The hope is that companies would sit up and take note – a sentiment many share, but some doubt. One reason for the sceptical stance is that Microsoft is an easy target that everyone has heard of and many love to hate. As is customary, the FTC opened a 30-day comment period for the consent decree, which spawned several comments, some them suggesting that Microsoft a) escaped lightly, and b) will not suffer unduly.

Microsoft makes one point about the effect in its own apology for the FTC decree on its corporate website. The company's market dominance will, by definition, entail changes among the companies it works with. "We have been working to raise the bar for Internet security and privacy and believe that the agreement with the FTC will raise it further – for both ourselves and industry," said Brian Arbogast, Corporate Vice President of Microsoft.

One 49-page comment to the FTC was drafted for Catavault, a Pennsylvania-based authentication software maker, previously PINvault.com. It had much to quibble with in the consent decree, which was grudgingly referred to as "a good baby step". Catavault's main concern was that the decree does not fully "safeguard consumer choice or technological innovation, which in an open and efficient market, serve as the most effective safeguards regarding the security, privacy and functionality of the single sign-on [SSO] market." [SSO is a method of online authentication.]

In a press release, FTC chairman Timothy J Muris held Microsoft up as an example of what not to do. "Companies that promise to keep personal information secure must follow reasonable and appropriate measures to do so. It's not only good business, it's the law."

Some might argue with both clauses of that last comment. Sources interviewed by *PL&B International* suggested that in tough economic times, "good business" means selling more goods or services than the next guy. Jittery shareholders are not necessarily thrilled to hear of huge expenditures on privacy and security products and staff. Dan Jaye, co-founder of Engage Technologies, said retreat – not advancement – has marked the corporate approach to privacy in the past 12 months or so. "Privacy is not seen as anything that can help the top line." In his own dealings with *Fortune*

1,000 companies, Jaye said, he has noted virtual "apathy" to privacy-related issues in recent months, where companies are grappling with accountancy scandals, flip-flops on the stock markets and shrinking margins.

Gary Clayton, chairman and founder of the Privacy Council, said that while the FTC is perceived as aggressive in this arena, executives' grasp of privacy issues remains shaky. In-house legal staffs at major companies whom Clayton has met "were not very aware of privacy issues, although they had some concerns about what should be done," Clayton said.

Like Jaye, Clayton noted that like most things, privacy is bottom-line dependent. "There is not much money available in companies to spend on privacy and those taking a leadership position are few." Edward Kelly, an attorney at law firm Ropes & Gray, pointed out that when companies are "fighting for survival," concerns about matters like privacy tend to fall by the wayside.

In a similar vein, the paradigm shift that will put privacy on the top of a business agenda has yet to occur, claimed Internet Law and Policy Forum executive director Andrew Konstantaras. At a recent conference on the issue, attendees seemed concerned but did not perceive the Microsoft case as a watershed. Yet people are beginning to realise, "you cannot treat your privacy policy like a press release...The FTC will make you stick to what you say," Konstantaras said.

CONSENT DECREES – SLAPS ON THE WRIST OR TOUGH SANCTIONS?

In its response to the FTC Microsoft ruling, original plaintiff the Electronic Privacy Information Center (EPIC) suggested the decree lacks sufficient transparency to guarantee consumers "adequate information about security and privacy risks in the Passport System."

In addition, wrote EPIC, the software giant is not alone in offering a less than secure authentication system. According to EPIC, other companies that "have business models dependent on the exploitation of individuals' personal data" include AOL (Screen Name Service) and Liberty Alliance's online identification and authentication service.

[Liberty Alliance is a consortium whose members include American Express, AOL, France Télécom, Nokia, Sony and Vodafone, among others.]

Consumer privacy advocate Senator Ernest Hollings admitted that some companies self-regulate with care but he said many have no privacy policy to speak of and feel "safe in the knowledge that they face virtually no legal jeopardy for selling personal information." This comment came in April, when the FTC had lambasted Eli Lilly but had not yet completed its Microsoft inquiry.

Since then, the FTC has the will to bring enforcement actions, as is evidenced by the news as PL&B International went to press that it was investigating the privacy practices of some of the top US pharmacies, including the Rite Aid Corporation and Walgreen. It has adopted other tacks too and launched a segment on its website that takes a light-hearted approach to security and privacy. It is based on a turtle called Dewie with a strong shell. The FTC's Finn said the newly created pages aim to add an educational dimension to the FTC's enforcement role.

A HODGEPODGE OF LAWS

Some observers have cheered the FTC on. Washington DC attorney John Kamp, of Wiley Rein & Fielding LLP, anticipates that the Microsoft decree will lead to a standard of care. "We think it will become a standard that states will pick up."

The FTC can only do so much and Muris' "it is the law" statement is debatable. "The laws" might be a more appropriate description. Privacy legislation, for example, varies from industry to industry with the financial services and the health care sectors more tightly regulated than others. But, the US does not have one privacy law affecting all companies that do business across the 50 states and the District of Columbia.

Several states have passed different laws indicating that they are serious about privacy, especially online privacy. In Minnesota, a controversial law passed last May requires all internet sites that collect data to use an opt-in policy. Vermont's controversial finan-

cial industry standards require an "opt-in" for sharing data with third parties, whereas federal law specifies opt-out.

On a federal level, bipartisan attempts in the House of Representatives to introduce the Online Consumer Privacy Protection Bill (HR 4678) have been dragging on for well over a year. South Carolina's Ernest Hollings is just one legislator who has sponsored a bipartisan bill (S2201) in the upper house and it, too, has been on the books for years. S2201 has not moved beyond the committee approval stage, reached last May.

In addition to other provisions, the Hollings bill would add teeth to the FTC's current authority to impose civil penalties. The bill includes the provision that an injured data subject could receive up to \$200 (euro 206), which is not an option now.

Engage Technologies' Dan Jaye, who has testified on privacy matters repeatedly, says congressional elections this month could have an impact on the future of the bills. One shift to either a Democratic House majority or a Republican majority in the Senate might prompt the two houses to conceive a joint bill addressing online and offline privacy, he suggested.

By the end of this year, or early 2003, we should see further developments, including either enforcement of the Microsoft decree (or amendments to it) and an assessment of its long-term impact on US business.



Judith A Sullivan is PL&B International's contributing editor.

For further information on the Microsoft settlement, see:

*www.ftc.gov/opa/2002/08/microsoft.htm;
www.ftc.gov/os/comments/microsoftcomments; and
www.microsoft.com/presspass/features/2002/aug02/08-08passport.asp*