MEITAR LIQUORNIK GEVA & LESHEM BRANDWEIN

PRIVACY UPDATE: THE IMPORTANCE OF A WELL-DRAFTED PRIVACY POLICY

Too often we think privacy policies are just boilerplate forms that you can plunk down on your website and then scratch that annoying item from your "to do" list. Unfortunately, in light of a recent U.S. federal district court case, Mortensen v. Bresnan Communications, LLC, companies would be well-advised to pay careful attention both to what their privacy policy says and how it is presented to users.

Factual Background: Online Behavioral Advertising

Defendant Bresnan, an Internet Service Provider, had allowed NebuAd, Inc., a California start-up, to install a device onto its network that engaged in "deep packet inspection". Stripped of opaque technical-sounding terminology, this means that NebuAd both analyzed emails of Bresnan's users and tracked their web surfing in order to create a user profile. NebuAd would then use this profile to target online behavioral advertising. If a user, for example, waxed poetic in his emails about the romantic bed & breakfasts of Asbury Park, NJ and visited I-Love-New-Jersey.com (this is all quite hypothetical, of course!), the user might begin receiving online ads containing discounted passes to the Garden State Parkway and Atlantic City casinos.

Plaintiffs, who sought to represent a class of aggrieved subscribers, claimed that their ISP Bresnan profited from NebuAd's activities and that Bresnan had not properly obtained the users' consent to collect their personal information. Plaintiffs specifically alleged: (1) violation of the Electronic Communications Privacy Act; (2) invasion of privacy; (3) violation of the Computer Fraud and Abuse Act; and (4) trespass to chattels. Bresnan moved to dismiss the complaint, but was only partially successful. Although the court's opinion began in a predictable fashion in favor of the defendant, in a surprising turn, the court permitted the class action to proceed.

If you have any questions regarding the matters in this legal update, please contact the following attorneys or call your regular Meitar contact.

David Mirchin
TEL. 972 3 610 3199
FAX. 972 3 610 3667
dmirchin@meitar.com

Electronic Communications Privacy Act ("ECPA")Claims—Defendant Wins

The ECPA, known as the Wiretap Act, prohibits intercepting (or assisting intercepting) electronic communications unless the person has given prior consent to such interception. The question the court addressed was whether users had implicitly given consent to the surveillance.

Bresnan argued that users had consented since its *Online Privacy Notice* and *Online Subscriber Agreement* stated that the ISP "and its agents" could monitor electronic postings and transmissions, as well as use equipment to collect information on users' internet usage. Specifically, these policies indicated that Bresnan could collect information on: (1) the "web sites you review", (2) "your electronic browsing", and (3) "the text of e-mail or other electronic communications you send or receive". The policies also indicated that this information could be disclosed to third parties.

Besides these general notices, Bresnan also gave users specific notice that the NebuAd trial would begin and provided a link for customers to opt out.

The court dismissed the plaintiffs' Wiretap Act claim, concluding that Bresnan had given notice, on three separate occasions, to users that their email and browsing history would be monitored and could be passed on to third parties. Accordingly, the court concluded that users had consented, or at least acquiesced in, the interception of their messages.

Invasion of Privacy Claims—Defendant Wins

Plaintiffs' next claim was that Bresnan committed a tort by violating the users' privacy. To prevail on

such a claim, the plaintiff must show that: (a) the plaintiffs expected privacy, and (b) this expectation was objectively reasonable.

For the same reasons that the court rejected the plaintiffs' Wiretap Act claims — that the users were given adequate notice that their communications would be intercepted — the court dismissed the privacy claims. While the users may have expected their communications to be private, this was not an objective, reasonable expectation because Bresnan had informed them three times that their messages were not private.

Computer Fraud and Abuse Act—Plaintiffs Win

A person violates the Computer Fraud and Abuse Act (CFAA) if he or she accesses someone else's computer without authorization or exceeds the authorized access so as to "obtain or alter information" in the computer. Plaintiffs must, in the aggregate, suffer economic loss or damages of $5,000 in order to bring a claim under the CFAA.

Since the users gave their consent to their emails being provided to third parties, the court held that Bresnan did not access the computers without authorization.

The court did, however, hold that Bresnan "exceeded authorization" since neither the *Privacy Notice*, the *Online Subscriber Agreement*, nor the NebuAd appliance trial hyperlink provided notice that NebuAd would place cookies on the user's computers that would alter the user's privacy protocol and security settings. Accordingly, the court concluded these changes to the privacy settings exceeded authorization, and therefore plaintiffs' CFAA claims would not be dismissed.

Trespass to Chattels—Plaintiffs Win

Trespass to chattels is a medieval, obscure doctrine of violating someone's personal property (as opposed to the more well-known trespassing on land), which was largely moribund until some creative attorneys in the late 1990s resuscitated it in the internet context in the case of *Thrifty-Tel v. Bezenek (Cal. 1996)*. Plaintiffs in Mortensen claim that the ISP, by permitting NebuAd to alter the privacy and security settings, interfered with the users' possessory interest in their computers and thereby caused damage to the computers.

Just, as with the CFAA claim, altering the privacy and security settings was held sufficient to state a claim of trespass to chattels.

Analysis and Recommendations

NebuAd's appliance has been criticized for its invasion of privacy not just by the plaintiffs in this case, but also during Congressional hearings held in 2008. In particular, members of Congress railed against NebuAd for not obtaining explicit, proactive consent from users to monitor their email. Texas Congressmen Gene Green called NebuAd's opt-out procedures "contemptible". Pennsylvania Congressman Mike Doyle said the practice "goes against everything the country's been founded on". Michigan Representative Bart Stupak wondered, "Why do I have to opt out? Why should the burden be on the American consumer?"

In the wake of this criticism, major customers of NebuAd terminated their agreements and NebuAd has since gone out of business.

The lessons from this case, however, have outlived the company. Even though I believe the court's conclusions on both the CFAA and trespass claims are not at all convincing (including on the issue of whether plaintiffs truly can make a claim for economic damages under CFAA or can prove actual damage to their computers on the trespass claim, as required by the leading case in this area, the California Supreme Court opinion in *Intel v. Hamidi*), I would suggest that the lessons of the Mortensen v. Bresnan holding are that companies should review their privacy practices in the following ways:

1. Privacy Policy Must be Specific. In dismissing the plaintiffs' claims under both the Wiretap Act and for invasion of privacy, the court stated the users had consented since the privacy policies clearly stated that Bresnan or third parties might monitor their emails and web browsing. On a similar theory, the court refused to dismiss the CFAA and trespass to chattels claims, since the privacy policies had not specifically stated that the NebuAd appliance would alter the privacy and security settings. Lesson One: companies should review their privacy policies to make sure that all of the following are clearly described: first, any proposed uses of users' information; second, use of any cookies; and third, any alterations of computer settings of users.

This advice is also consistent with various recent Federal Trade Commission enforcement actions in the privacy area. In June 2009, the FTC settled a case against Sears and Kmart that charged that they failed to disclose adequately the scope of personal information they collected from users who downloaded a particular software application. Last November, the FTC settled charges against

EchoMetrix that it failed to adequately inform parents using its web monitoring software that information collected about their children would be disclosed to third-party marketers.

2. Multiple Privacy Notices. In finding that the users had consented to the ISP's monitoring device, the court noted positively that users had received three notices from the ISP—the privacy policy, the online subscriber agreement, as well as a specific notice that the NebuAd trial was about to begin and that that users could opt out of the trial. Lesson Two: for potentially invasive or unexpected uses of a user's personal information, multiple notices should be given. Specific, timely notices of particular uses are much more powerful and convincing to a court than general, older notices.

3. Minimize Use of Personal Information. In this case, the court gave significant weight to user consent, even as part of a non-negotiable, standard form privacy policy and terms of use. In addition, the court looked favorably upon the opt-out procedure, rather than requiring explicit consent to opt-in to the NebuAd trial. Companies may not be so fortunate in the future. This is especially true in Israel, where courts are not sympathetic to standard form agreements in the consumer context.

Under the deep packet inspection technology, it is not clear that a user who opted out of the trial did not in fact have his personal emails or web activity collected. Rather, it may be that the information was simply not passed along to target advertisements. Lesson Three: companies should evaluate whether their privacy practices as implemented minimize the amount of personal data collected and limit the collection to the purposes identified in their privacy policy. Both courts and regulators are increasingly conscious of protecting the privacy of users, and unreasonable practices may not be upheld, even if there is some generic allusion to such collection and use of personal information in a website policy.

This update is provided by our firm for informational purposes only and is not intended as legal advice.

MEITAR LIQUORNIK GEVA & LESHEM BRANDWEIN | LAW OFFICES | WWW.MEITAR.COM

16 Abba Hillel Silver Rd. Ramat Gan, 52506, Israel,
Tel. + 972 3 6103100 Fax. + 972 3 6103111