Privacy and Data Security Law Update

MARY ELLEN CALLAHAN, MARK PAULDING, AND JULIANNA TABASTAJEWA

RUSSIAN GOVERNMENT ESTABLISHES NEW PROCEDURE FOR MANUAL PROCESSING OF PERSONAL DATA

On September 15, 2008, the Russian government issued Order No. 687, "On Approval of Regulation on Specific Features of Personal Data Processing Performed without Automatic Means," to establish procedures for the manual processing of processing personal data. The order was authorized by the 2006 Russian data protection law and was the first regulation issued related to the law. The order, effective as of October 24, 2008, is of particular importance for staff and personnel management departments and their processing of employees' personal data.

In order to process personal data "without automatic means," the data must be separated from other information (either by recording on separate devices or servers, in special sections or within separate form fields). Without automatic means relates both to manual processing and non-data base processing of personal data. In addition, individuals working with personal data without automatic means must be aware of the method and specific features of their processing and of the categories of such data.

The use of standard document forms may also include information on a person, however, certain conditions must be observed. Thus, if a citi-

Mary Ellen Callahan, Mark Paulding, and Julianna Tabastajewa are attorneys with Hogan & Hartson LLP. The authors can be reached at mecallahan@hhlaw.com, mdpaulding@hhlaw.com and jgtabastajewa@hhlaw.com, respectively. Bret Cohen, Tulasi Leonard, Andrew Graziani, Dmitry Artyunin, and Hanno Timner, attorneys with the firm, assisted with the preparation of this article.

Published in the March 2009 issue of Privacy & Data Security Law Journal.

zen's written consent to process his data is required, a standard form must include a space where he can put a mark of his express consent to processing his data without automatic means.

Manual processing of personal data must be performed in a manner that clearly identifies the storage location of each category of personal data, and establishes a discrete list of persons performing personal data processing or having access to such data. Individuals accessing and using personal data without automatic means must be aware of the method and specific features of their processing and of the categories of such data. In addition, the storage locations of material devices and the access list of individuals involved in the processing must be established as well.

These security standards identified in Order No. 687 requiring storage and access standards for collection, use, and storage of personal information are consistent with other countries that have comprehensive data protection standards, and will be the first in a series of regulations associated with the Russian data protection law.

MASSACHUSETTS REGULATIONS CALL FOR COMPREHENSIVE INFORMATION SECURITY PLANS AND ENCRYPTION FOR PERSONAL INFORMATION

The finalized Standards for The Protection of Personal Information of Residents of the Commonwealth, 201 CMR 17.00, issued by the Massachusetts Office of Consumer Affairs and Business Regulation ("OCABR") on September 22, 2008, continue the recent trend of state laws and regulations designed to increase the security of personal data. While the standards resemble certain elements of the Gramm-Leach-Bliley ("GLB") Act Safeguards Rule and Health Insurance Portability and Accountability Act ("HIPAA") Security Rule, the OCABR has included several mandates that go beyond existing federal mandates.

The standards define personal information as: "a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to

such resident: (a) Social Security Number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account."[1] The standards expressly exclude any such information lawfully obtained from publicly available sources. It is notable that the standards include financial account numbers without security codes, PINs, or similar access controls, unlike the encryption law recently implemented in Nevada.

Furthermore, the standards define the records subject to the regulations as: "any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics." *Id.* Thus, entities subject to the standards must apply them to electronic and hardcopy files.

The standards require entities that own, license, store, or maintain personal information to develop and maintain a comprehensive, written information security plan containing administrative, technical, and physical safeguards. The information security plan should be consistent with the requirements of any other applicable federal or state regulations, such as GLB and HIPAA. The OCABR will assess the compliance of information security plans based on four factors:

1. The size, scope, and type of business;
2. Resources available to the business;
3. Amount of stored personal information; and
4. The need for security and confidentiality of the data.

Nonetheless, all comprehensive security plans are expected to meet certain specific requirements, four of which are of particular note. First, all businesses subject to the standards must contractually obligate all third-party service providers with access to personal information to maintain safeguards for the data. Moreover, applicable businesses must obtain a written certification from service providers stating that they have an information security plan in compliance with the standards before grant-

ing access to personal information of Massachusetts residents. Service providers are not directly regulated by the standards. Instead, it is the responsibility of the regulated business to hold its service providers responsible by contract.

Second, the standards call for the minimalization of stored personal information. Businesses are required to limit data collection to that, and only retain the collected information for as long as "reasonably necessary to accomplish the legitimate purpose for which it is collected."[2] Similar to the Federal Trade Commission's draft principles for online behavioral advertising proposed last year, this provision reflects a growing belief that reducing the amount of personal information collected and the length of time that it is stored will diminish the costs of possible security breaches.

Third, the standards require businesses to document all actions taken in response to any security breach, including a mandatory postincident review. Accordingly, subject businesses should ensure that employees and managers responsible for information security maintain appropriate records of all steps taken to address security breaches and adjust practices going forward.

Fourth, businesses subject to the standards must inventory all paper and electronic records, as well as all computer systems and storage media (including laptops and portable devices) to determine which records contain personal information. Alternatively, the information security plan may treat all business records as if they contain personal information.

The standards include detailed requirements for securing computer systems that contain and/or transmit personal information. Many of these requirements — such as restricting data access to those who need such information, requiring a combination of unique identifier and secure password, and requiring up-to-date malware protection — are consistent with existing federal and state regulations. Like the recent Nevada law, the standards require encryption of all personal information transmitted across public networks.

The standards go beyond the Nevada statute by obligating businesses to encrypt all personal information stored on laptops or other portable devices. While "portable devices" is undefined, it presumably includes personal data assistants, smart phones, removable storage media such as

flash memory devices, and portable hard drives. Moreover, the standards call for the encryption of any data transmitted over wireless networks. Due to some sloppy drafting, this requirement appears to be necessary regardless of whether personal information is involved.

The encryption requirements generated the largest number of responses during the comment period for the rule. Some comments noted that the standards appear to preclude other, similarly effective but less costly, options such as truncation and redaction. However, it is arguable that data that has been truncated or redacted may fall outside the standards' definition of personal information. The definition of personal information does not explicitly include partial social security numbers, identification card numbers, or account numbers. Therefore, such alternative data protection methods may remain viable under the standards.

While the standards do not directly conflict with existing data security regulatory schemes such as GLB or HIPAA, covered entities may find that they must undertake additional steps to comply with the provisions discussed above. On the other hand, entities currently complying with the Payment Card Industry Data Security Standard should find that their current practices are also in compliance with the new Massachusetts regulations.

Neither the standards nor the authorizing statute, M.G.L. ch. 93H, make any explicit provision for extraterritorial enforcement. Nonetheless, the standards conceivably apply to any entity, operating within or outside Massachusetts, that collects personal information from Massachusetts residents. While the ability of the Commonwealth to enforce the standards outside its territory is subject to the general principles of personal jurisdiction, businesses should be aware of the risks associated with noncompliance and assess their practices accordingly.

When initially published, the standards were intended to take effect on January 1, 2009. In light of concerns regarding the costs of compliance, the OCABR has extended the effective date. The general compliance deadline is now May 1, 2009 (which coincides with the FTC's enforcement date for the Red Flags Rule).

While regulated businesses must contractually obligate third-party service providers to provide safeguards for personal information by May

Published in the March 2009 issue of Privacy & Data Security Law Journal.

1, 2009, they are not required to obtain written certifications from service providers until January 1, 2010. Similarly, while personal information stored on laptops must be encrypted by May 1, 2009, encryption of personal data on other portable devices is not required until January 1, 2010.

COUNCIL RELEASES UPDATED VERSION OF PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS

An updated version of the Payment Card Industry Data Security Standard ("PCI DSS") was released October 1, 2008, by the Payment Card Industry Security Standards Council.

The PCI DSS is a set of data security standards for merchants and other businesses that accept credit or debit card payments for product or services, and merchant banks and other financial services businesses that process payment card transactions.

The standard was developed by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. International to facilitate consistent data security measures on a global basis. The PCI DSS includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures.

Penalties for failing to implement and comply with the PCI DSS may include fines, increased rates that the credit card companies charge for each transaction, and revocation of the ability to process payment cards.

Version 1.2 of the PCI DSS went into effect October 1, 2008, and the sunset date of Version 1.1 is December 31, 2008. While Version 1.2 has a number of changes from Version 1.1, none of the changes are substantive, but are simply clarifications, explanations, and enhancements to language in Version 1.1. Guidance from the council provides that assessments started prior to October 1 will be subject to Version 1.1, assessments started between October 1 and December 31 may be subject to either Version 1.1 or 1.2, and assessment started on or after January 1, 2009 must be conducted in accordance with Version 1.2.

Published in the March 2009 issue of Privacy & Data Security Law Journal.

The council plans to enhance the PCI DSS approximately every two years to ensure that the standard includes new or modified requirements necessary to mitigate emerging payment security risks.

COURT UPHOLDS NEW HAMPSHIRE LAW BANNING SALE OF DOCTOR-SPECIFIC PRESCRIPTION DRUG INFORMATION

On November 18, 2008, a federal appeals court in Boston upheld New Hampshire's law banning the sale for marketing purposes of prescription drug information that identifies doctors' prescribing patterns. In vacating the injunction against enforcement of the law, a panel of the U.S. Court of Appeals for the First Circuit overturned the April 2007 decision by the federal district court for the District of New Hampshire, which had ruled that the New Hampshire state law violated the commercial free speech protections of the U.S. Constitution.

The First Circuit opinion dealt a blow to the pharmaceutical industry and companies that collect prescription data for use in drug marketing, and represents the first major setback in the efforts to block implementation of prescriber privacy laws through the courts. The sale of de-identified prescription data has become a lucrative industry.

The New Hampshire law is intended to reduce state health care costs by prohibiting pharmacies, pharmacy benefit managers, insurance companies, and data-mining companies that collect and analyze prescription information from selling or using that information for commercial purposes. This prohibition removes a primary means by which pharmaceutical representatives target physicians to promote brand-name drugs.

The case is a defeat for two large data-mining companies, IMS Health and Verispan, who originally sued in 2006 to block implementation of the New Hampshire law. It was the first state law to prohibit specifically the sale or transfer of information identifying doctors for commercial purposes. The companies argued that the purchase and collection of prescription data were valuable for public health reasons, and that the law

Published in the March 2009 issue of Privacy & Data Security Law Journal.

infringed on their First Amendment rights.

Similar prescriber privacy laws in Vermont and Maine are currently in litigation, with the Maine law pending before the same federal circuit court that just upheld the New Hampshire law. The First Circuit's decision may also offer encouragement to state legislatures considering other similar prohibitions; doctors who object to the disclosure of their prescribing patterns have advocated for such legislation.

In its decision, the First Circuit wrote that the collection and marketing of prescription information is "mind-boggling" in its scope, adding, "[t]he record contains substantial evidence that, in several instances, [drug company representatives] armed with prescribing histories encouraged the overzealous prescription of more costly brand-name drugs regardless of both the public health consequences and the probable outcome of a sensible cost/benefit analysis." Further, the court found that New Hampshire "adequately demonstrated that the Prescription Information Law is reasonably calculated to advance its substantial interest in reducing overall health care costs" within the state.

In 2006, the American Medical Association ("AMA") launched the "Physician Data Restriction Program," which offers physicians the option of withholding their prescribing data from pharmaceutical sales representatives while still making it available for medical research purposes. The program also allows physicians to register complaints against sales representatives or pharmaceutical companies who they believe are using their prescribing data inappropriately.

MORTGAGE COMPANY SETTLES WITH FTC FOR GLB AND SECTION 5 VIOLATIONS

The Federal Trade Commission ("FTC") has reached a settlement deal with a Texas-based mortgage company that it charged with violating federal law (both the Gramm-Leach-Bliley ("GLB") Act and the FTC Act) for failing to provide reasonable and appropriate safeguards to protect personal information and for making false or misleading statements

Published in the March 2009 issue of Privacy & Data Security Law Journal.

about their data security policy.

Premier Capital Lending, Inc. ("PCL") is a mortgage lending company that helps customers finance the purchase of manufactured homes and adjacent land. As part of its business, PCL routinely accesses customers' credit reports from a consumer reporting agency. PCL receives the reports through an online portal that is accessed by employees with authorized user names and passwords.

In March 2006, PCL issued a user name and password to an outside vendor, a seller of manufactured homes. This enabled the seller to access buyers' credit reports without traveling to PCL's office. PCL issued the access without ever visiting the seller's office, auditing the seller's data privacy policies, or evaluating the seller's capacity to protect customers' private information.

By July 2006, a hacker had infiltrated the seller's computer and stolen PCL's user name and password. The hacker used that information to access the online portal of the consumer reporting agency and obtained 317 credit reports on individuals who had no connection to PCL. The hacker also had access to 83 additional credit reports that were requested by the seller through the online portal. PCL learned of the privacy breach in the summer of 2006 and immediately contacted the 317 noncustomers whose credit reports had been illegally accessed.

PCL did not realize that the hacker also had access to the 83 additional reports until more than a year later, and did not inform those customers of the breach until September 2007.

According to the FTC, PCL failed to provide reasonable and appropriate data security for its customers: it never assessed the risks of giving an outside vendor direct access to the consumer reporting agency; it never addressed those risks, failing to evaluate the vendor's security system or provide the vendor with appropriate security safeguards; it failed to monitor consumer-report requests made on its own account; and both before and after PCL discovered the breach, it failed to fully assess the extent of consumer data at risk.

As a result of these failures, the FTC accused PCL and its co-owner and officer, Debra Stiles, of violating the FTC's Safeguards Rule, enacted under the GLB Act. The rule requires financial institutions to develop

Published in the March 2009 issue of Privacy & Data Security Law Journal.

a comprehensive security program that contains reasonable administrative, technical, and physical safeguards to protect customers' personal data. Specifically, the FTC alleged that PCL failed to identify reasonably foreseeable risks or assess the sufficiency of its safeguards, and it failed to design, implement, and monitor a sufficient safeguard system.

Furthermore, the FTC alleged that by holding out to customers that it protected their personal information, PCL violated both the Privacy Rule of the GLB Act and Section 5 of the FTC Act. The Privacy Rule requires financial institutions to provide clear and accurate descriptions of their privacy policies and practices to customers, and Section 5 prohibits false and misleading trade practices. PCL's privacy policy said, in part:

> We take our responsibility to protect the privacy and confidentiality of customer information very seriously. We maintain physical, electronic, and procedural safeguards that comply with federal standards to store and secure information about you from unauthorized access, alteration and destruction. Our control policies, for example, authorize access to customer information only by individuals who need access to do their work.

According to the FTC's complaint, PCL failed to abide by the very standards it claimed to follow. Therefore, its stated policy was false or misleading, and it violated both the Privacy Rule and Section 5. This settlement is another cautionary tale for companies that collect and store personal information — the FTC pointed to PCL's privacy policy as an express statement regarding security standards, and thus PCL's actions were violative of both the Safeguards and Privacy Rules of GLB and Section 5. Companies should confirm that their privacy policies are accurate representations of their security practices.

Published in the March 2009 issue of Privacy & Data Security Law Journal.

GERMAN SOCIAL NETWORKING SITES SUBJECT TO INCREASED SCRUTINY BY DATA PROTECTION AUTHORITIES

Social networking sites ("SNS") are increasingly subject to scrutiny by German State Data Protection Authorities. For example, the Berlin Data Protection Authority is presently conducting an investigation of an SNS, as confirmed by the authority's spokeswomen (although they declined to provide further information on this ongoing matter). It is expected that the investigation will largely focus on this site's compliance with rules established by the so-called "Duesseldorfer Kreis" regarding SNS.

The Duesseldorfer Kreis is an informal association of the 16 State Data Protection Commissioners in Germany. The association convenes twice annually in order to discuss and comment on data protection issues of public interest.

In April 2008, the Duesseldorfer Kreis published a statement setting forth eight main privacy-related principles, which the Kreis believed should be observed by SNS in order to comply with German data protection regulations.

This announcement of the Duesseldorfer Kreis, as with other publications of this association, is legally nonbinding. However, German Data Protection Commissioners, such as the Berlin DPA in its current investigation, will largely depend on the statements of the Duesseldorfer Kreis. The eight data protection principles to be observed by the operator of a Social Network Site include:

- The storage of personal data after termination of a user's access to the site without the users' explicit permission is only admissible in order to invoice the use of the SNS.
- Operators of social networking sites must provide comprehensive information to users with regard to all applicable data protection and privacy regulations, potential violations of privacy rights in connection with the publication of user profiles on the SNS, as well as in relation to users' obligations to safeguard other participants' personal rights.

Published in the March 2009 issue of Privacy & Data Security Law Journal.

- Personal data submitted by the users shall only be used for marketing purposes with the express consent of such users. Further, users should have the opportunity to decide which of their personal data, including information regarding the actual usage of the SNS, shall be used for marketing purposes.
- Storage of personal data and storage of information regarding the usage of the SNS (as well as other Internet services) in order to assist potential criminal investigations, is not admissible.
- Users must have the opportunity to use the SNS on an anonymous basis or with a pseudonym. Users may be requested, however, to disclose their identity to the operator of the system.
- SNS operators must implement all technical and organizational measures necessary to safeguard data security, especially to avoid a systematic or large scale export or downloading of user profile data.
- Establish standard settings safeguarding the users' privacy to the greatest possible extent. Users must be able to choose which groups of other users shall have access to their profiles. Access by Internet search engines shall always require the users' express consent.
- Users must be able to delete their profile information through simple technical means.

It is to be expected that social networking sites that adhere to the aforementioned data protection and privacy principles will successfully pass potential investigations by the state data protection authorities.

DEBT COLLECTORS' FAILURE TO NOTIFY CONSUMERS ABOUT CALL MONITORING MAY BE A DECEPTIVE PRACTICE

On November 7, 2008, the U.S. Court of Appeals for the Ninth Circuit held in *Thomasson v. GC Services LP*,[3] that undisclosed telephone

Published in the March 2009 issue of Privacy & Data Security Law Journal.

call monitoring by a business carrying out its operations does not, as a matter of law, violate the California Information Privacy Act ("CIPA") but may constitute a deceptive practice and violate the Fair Debt Collection Practices Act ("FDCPA").

The appellants, Andrew and Rebecca Thomasson, had appealed the district court's grant of summary judgment to GC Services on their CIPA and FDCPA claims, challenging the court's decision that they failed to present sufficient evidence about whether their calls with GC Services were monitored, whether GC Services failed to provide notice of its alleged monitoring, and whether unrecorded monitoring constituted a deceptive practice in violation of the FDCPA.

Section 632 of CIPA criminalizes intentional eavesdropping by any person (e.g., a third party secretly listening to a conversation between other parties), including a business, who does not obtain the consent of all parties to a confidential communication carried out over a telephone.[4]

The FDCPA provides that "[a] debt collector may not use any false, deceptive, or misleading representation or means in connection with the collection of any debt."[5] The Ninth Circuit has explained that "one such means is '[t]he use of any false representation or deceptive means to collect or attempt to collect any debt or to obtain information concerning a consumer.'"[6]

While the Ninth Circuit found that the Thomassons did not state a cause of action under CIPA (the alleged call monitoring by GC Services was not unlawful because the appellee was one of the two parties to the calls in this case), the court did reverse the district court's ruling in part with respect to the appellant's FDCPA claim. The Thomassons argued that GC Services engaged in deceptive practices by deliberately failing to notify debtors about their call monitoring practices "in order to 'obtain information concerning a consumer.'"[7]

In concluding that the appellants did successfully raise a factual dispute regarding whether GC Services violated the FDCPA by allegedly monitoring consumer calls without notice, the Ninth Circuit highlighted the fact that the appellants not only supplied deposition testimony and multiple affidavits stating that GC Services monitored calls without notice to the consumers but also presented evidence that the appellee

"knew" that delivering notice to consumers that their calls were or could be monitored would increase the likelihood that such debtors would discontinue their telephone calls with GC Services before revealing personal or debt-related information. To avoid running afoul of the FDCPA, therefore, debt collectors should provide consumers with notice of the possibility of call monitoring.

CLASS ACTION COMPLAINT FILED AGAINST NEBUAD AND ISPS OVER DEEP PACKET INSPECTION

On November 10, 2008, a complaint was filed in the U.S. District Court for the Northern District of California against NebuAd, Inc., an online behavioral marketing firm, and six Internet service providers ("ISPs") that partnered with NebuAd. This is the first (of perhaps several) class action lawsuits related to issues associated with behavioral advertising.

NebuAd's technology tracks the web-surfing habits of ISP customers in order to better target ads to them. Plaintiffs — 15 ISP customers from five different states — are seeking class action status and allege violations of the Electronic Communications Privacy Act ("ECPA"), the Computer Fraud and Abuse Act, the California Invasion of Privacy Act, and the California Computer Crime Law.

The complaint alleges that the ISPs utilized NebuAd's technology from November 1, 2007, to July 1, 2008, and that customers were not provided adequate informed notice of the NebuAd service or afforded a meaningful opt-out mechanism. The complaint also alleges that the use of deep packet inspection technology to intercept and review Internet transmissions in order to transmit targeted advertisements violates consumers' privacy rights under ECPA. NebuAd has said that the data it collected was anonymous because it did not know personal information such as users' names or phone numbers and did not retain copies of the IP address associated with users. NebuAd has also said that it did not collect sensitive data, and that users would be able to opt out of the platform.

Published in the March 2009 issue of Privacy & Data Security Law Journal.

The NebuAd technology has attracted attention in part due to the massive amount and scope of information available to the ISPs and through the ISPs to companies like NebuAd. Prior to the filing of this lawsuit, the NebuAd technology attracted the attention of Congress, which sent letters to numerous ISPs asking if they had worked with NebuAd and held hearings in September. NebuAd has said that it will be moving away from behavioral targeting based on data provided by ISPs.

Plaintiffs are seeking damages as well as injunctive relief, including the deletion of data previously collected and an easy and permanent opt-out mechanism in the future.

BELGIAN COURT CURBS ONLINE VIRAL MARKETING: DON'T TELL A FRIEND!

In a decision dated June 24, 2008, that only recently became public, the Commercial Court of Huy — a municipality in the Walloon area of Belgium — prohibited the viral marketing practices of the Belgian dating site NicePeople, following a claim introduced by competing dating site ToiEtMoi.

The idea behind viral marketing is straightforward: customers are encouraged to recommend a company's products or services to their family and friends, often for some kind of reward or compensation. The company in question will typically provide the necessary means to deliver the message, for instance, via e-mail, SMS/MMS, or fax.

For many advertisers viral marketing is the ultimate direct advertising tool, a modern version of mouth-to-mouth publicity that turns existing (and presumably satisfied) customers into efficient salespeople at relatively low cost. However, the case brought before the Commercial Court of Huy illustrates that this type of marketing is heavily restricted under (Belgian) privacy, e-commerce, and fair trade practices rules.

In *ToiEtMoi v. NicePeople*, claimant ToiEtMoi requested a cease-and-desist order on the ground that competitor NicePeople was illegally advertising its online dating services by using two different techniques

Published in the March 2009 issue of Privacy & Data Security Law Journal.

involving e-mail.

An initial technique allegedly used by NicePeople consisted of offering users of its dating site the opportunity to submit, when registering for the service, not only their e-mail address but also the password to access their e-mail inbox. As a result, NicePeople was able to access and collect the e-mail addresses of users' contacts directly from users' e-mail inbox.

As a second technique to promote its dating services, NicePeople would ask users to provide e-mail addresses of friends and acquaintances, who would then receive — allegedly on the users' behalf — an "invitation" to find out more about NicePeople's web site. Users who complied with this request would move up in the site's popularity ranking and have better opportunities to meet other users.

The Commercial Court of Huy concluded that the collection of e-mail addresses of users' friends and acquaintances with a view to using them for viral marketing purposes violated Belgian privacy law. NicePeople initially argued that it was not the responsible "data controller" under Belgian law, as it only provided the technical means for users to send invitation e-mails to their friends and acquaintances. The court, however, disagreed and considered NicePeople as the data controller, since allegedly NicePeople — instead of the users themselves — sent out the e-mails.

In addition, NicePeople asserted that its marketing practices were legitimate because they struck a balance between NicePeople's legitimate interests and the risks to e-mail recipients' privacy. Again the court did not agree, emphasizing that the privacy rights of e-mail recipients prevailed over the web site's interest to engage in viral marketing. According to the court, it was unacceptable that users of NicePeople were rewarded for providing the e-mail addresses of their friends and acquaintances to a commercial web site, and that they were not informed of the fact that the site would send advertising messages to those e-mail addresses.

The court found this particularly disturbing because it was important to avoid that messages would be sent to minors — considering the alleged erotic nature of some parts of the site. In short, the court did not support the premise that via viral marketing, commercial web sites such as

NicePeople would be able to send e-mails to persons who do not want to be associated with those sites and who do not want their children to be exposed to such sites. Consequently, the court decided that NicePeople's viral marketing practice violated Belgian privacy rules, allegedly by processing personal data without legal grounds.

In addition to finding a violation of Belgian privacy law, the court came to the conclusion that NicePeople's viral marketing practices infringed Belgian e-commerce rules, which prohibit the use of e-mail for direct marketing purposes unless the recipients have freely given their prior specific and informed consent (opt-in). This prohibition applies to direct use by the sender, as well as to indirect use — in this case with the help of users enticed into providing the addresses of their acquaintances via NicePeople's viral marketing techniques.

NicePeople suggested that it was entitled to send a first e-mail to potential new customers in order to obtain their prior consent as required by Belgian e-commerce law. The court, however, rejected the argument on the basis that this type of practice would constitute spamming and that the necessary consent should be obtained via other and less intrusive means. The court's view appears to run counter to a guidance note on viral marketing published by the Belgian Ministry of Economic Affairs in 2006, which suggests that prior consent can be asked via e-mail, provided that certain conditions are fulfilled.

Because NicePeople's viral marketing practices were found to violate both privacy and e-commerce rules, the court decided to ban them by issuing a cease-and-desist order under penalty of a fine of € 10,000 per violation. NicePeople has reportedly appealed the decision, so the final outcome in this matter is still uncertain.

Nonetheless, the court's decision is a reminder that novel forms of online advertising should always be vetted under applicable privacy and e-commerce laws before they are implemented. With regard to online viral marketing in particular, the court's decision in *ToiEtMoi v. NicePeople* clearly underlines the importance of obtaining advertising targets' prior consent when marketing in Europe in particular.

Published in the March 2009 issue of Privacy & Data Security Law Journal.

KIDS ACT ALLOWS SOCIAL NETWORKING SITES TO TRACK SEX OFFENDERS

On October 13, 2008, President Bush signed into law the Keeping the Internet Devoid of Sexual Predators Act ("KIDS Act"). The KIDS Act requires convicted sex offenders to register any "Internet identifiers" the sex offender uses or will use, including e-mail addresses and "other designations used for self-identification or routing in Internet communication or posting."

In turn, the Act requires the Justice Department to create a secure system that makes these identifiers available to social networking sites ("SNS"), narrowly defined as web sites with the primary purpose of facilitating online social actions, which allow users to communicate with one another, and which have a user base that is likely to include a substantial number of minors.

An SNS may then cross-reference the identifiers in the National Sex Offender Registry against those provided by its users or prospective users, and use that information to protect the safety of its members. Neither the Justice Department nor the social networking sites may release to the public the Internet identifiers of sex offenders contained in the registry.

Social networking sites are not required to use the registry and are exempted from federal or state liability based on a decision not to do so. They and their agents are also exempted from federal or state civil liability arising out of their use of the registry unless they commit intentional or reckless misconduct, publicly release any of the Internet identifiers, or fail to comply with additional limitations set forth by the Justice Department.

Social networking sites must apply for use of the system — including in the application a statement of purpose as well as a description of policies that ensure compliance with statutory and regulatory mandates — and must pay any fee set forth by the Justice Department for use of the system.

Published in the March 2009 issue of Privacy & Data Security Law Journal.

FCC CLARIFIES JUNK FAX RULES; SENDERS HAVE ADDITIONAL FLEXIBILITY FOR OPT-OUT COMPLIANCE

On October 14, 2008, the Federal Communications Commission ("FCC") released an Order on Reconsideration addressing petitions for reconsideration of its 2006 decision implementing the Junk Fax Prevention Act of 2005.[8]

Under the Junk Fax Prevention Act, unsolicited facsimile advertisements may be sent to recipients with whom the sender has an established business relationship ("EBR") as long as the sender obtained the recipient's facsimile number through: (1) the voluntary communication of such number from the recipient (within the context of the EBR); or (2) a directory, advertisement, or site on the Internet to which the recipient voluntarily agreed to make its facsimile number available for public distribution.

In implementing the Junk Fax Prevention Act, the FCC concluded that a facsimile number obtained from "the recipient's own directory, advertisement, or [I]nternet site" was sufficient under the second option unless the recipient noted on such materials that it does not accept unsolicited advertisements at that number.

Moreover, the FCC stated that senders relying on third parties for obtaining facsimile numbers (e.g., through membership directories and commercial databases) "must take reasonable steps to verify that the recipient consented to have the number listed, such as calling or emailing the recipient."

The Junk Fax Prevention Act also requires that all unsolicited facsimile advertisements include an opt-out notice that contains, among other things, a "cost-free" mechanism for recipients to transmit their opt-out requests.

In its 2006 junk fax decision, the FCC concluded that if a sender designates a web site as its cost-free, opt-out mechanism, a clear and conspicuous description of the opt-out mechanism and procedures must be included on the "first page" of the web site.

In addition, the FCC required senders to include the opt-out notice on the first page of the advertisement (i.e., not the cover page). The FCC also declined to limit the period of time for which a recipient's opt-out

Published in the March 2009 issue of Privacy & Data Security Law Journal.

request remains in effect.

In the Order on Reconsideration, the FCC addressed several concerns raised by two petitions for reconsideration filed by the Direct Marketing Association and Leventhal Senter and Lerman PLLC (on behalf of unnamed broadcast clients).

First, the FCC found that facsimile numbers compiled by third parties on behalf of a sender will be presumed to have been made voluntarily available for public distribution so long as they are obtained from the intended recipient's own directory, advertisement, or Internet site (and assuming that an EBR exists between the sender and recipient). Thus, the sender does not have to engage in any additional verification regarding those facsimile numbers. The FCC noted, however, that senders relying on such third-party compilations remain liable for errors made by the third party.

Second, the FCC clarified that taking "reasonable steps" to verify that a recipient has agreed to make available a facsimile number for public distribution may include methods other than direct contact (calling or e-mailing) with the recipient. As an example, the FCC stated that the recipient "may expressly agree at the point of collection to allow for public disclosure of the facsimile number." If a junk fax complaint is filed, however, the sender has the burden of demonstrating that the circumstances reasonably indicate that the recipient agreed to make the facsimile number available for public distribution.

Third, the FCC clarified that a sender may make clear and conspicuous notice of its cost-free, opt-out mechanism on the "first page" of the web site when the opt-out notice (contained on the first page of the facsimile) directs the recipient to a dedicated web page that allows the recipient to opt-out of future facsimile advertisements. Thus, the entire opt-out mechanism need not appear on the homepage of every sender of unsolicited facsimile advertisements. The FCC stated, however, that a clear and conspicuous link to the opt-out web page should also be provided on the sender's homepage. The FCC also maintained the requirement that senders include the opt-out notice on the cover page of the facsimile instead of the first page of the advertisement.

Finally, the FCC declined to reconsider its decision to limit the time

period for which opt-out requests remain effective, noting that recipients "assume the cost of the paper used, the cost associated with the use of the facsimile machine, and the costs associated with the time spent receiving a facsimile advertisement during which the machine cannot be used by its owner to send or receive other facsimile transmissions."

CAN-SPAM PREEMPTION JURISPRUDENCE NOT AFFECTED BY RECENT DECISIONS

In the past three months, state and federal courts have decided a number of cases involving private actions filed under state antispam laws. Since the CAN-SPAM Act became effective in 2004, the key question in the majority of such actions has been whether CAN-SPAM preempted the state law at issue.

Although two recent cases deviated from the prevailing focus on preemption, both cases involved conduct that occurred prior to the adoption of CAN-SPAM. Therefore, companies sending commercial e-mail can continue to focus their state law compliance efforts on the body of preemption jurisprudence that has been developing uniformly within the federal courts.

On September 12, 2008, the Supreme Court of Virginia overturned the nine-year sentence of a North Carolina resident who was convicted of violating Virginia's antispam statute that provided criminal penalties for "falsify[ing] or forg[ing] electronic mail transmission information…in connection with the transmission of unsolicited bulk electronic mail."[9] The defendant's conduct at issue occurred in 2003, so the preemption provisions of CAN-SPAM did not apply.

The court struck down the statute as unconstitutionally overbroad, given that its facial prohibition of the falsification of sender information unduly burdened anonymous political, religious, or other noncommercial speech, which receives greater protection than commercial speech under the First Amendment. The broad focus of this Virginia law placed it in the minority of state antispam statutes, which usually apply only to com-

Published in the March 2009 issue of Privacy & Data Security Law Journal.

mercial e-mail.

On September 30, 2008, the Southern District of Iowa issued a $236.5 million judgment — $10 per e-mail — against two Arizona residents who ran a business that sent unsolicited e-mail advertisements on behalf of its clients.[10] Under the Iowa antispam statute, the defendants were held liable for misrepresenting information in the transmission path of an e-mail, omitting information identifying the point of origin of an e-mail, and omitting contact information to allow the recipient to decline further unsolicited e-mail. As in *Jaynes*, the conduct at issue occurred prior to the effective date of CAN-SPAM; indeed, the Iowa statute was repealed and replaced by another in 2005.

Given that these decisions could not consider CAN-SPAM's preemption provision, they are not indicative of how courts today interpret state antispam laws. Under the preemption provision, state laws regulating commercial e-mail are preempted except to the extent they prohibit "falsity or deception."[11]

In interpreting this provision, the majority of courts follow the approach of the Fourth Circuit in *Omega World Travel, Inc. v. Mummagraphics, Inc.*,[12] the only federal appellate court decision construing the provision.

In *Omega*, the court held that the provision only exempted from preemption state laws providing causes of action for e-mail-related "common law fraud or deceit." Following this approach, courts have ruled that CAN-SPAM preempts any state antispam statute except to the extent they prohibit fraudulent conduct, and even then have dismissed plaintiffs' claims of fraud unless pleaded with particularity.

Under this approach, the statutes at issue in the recent Virginia and Iowa cases would likely be invalidated — or at least limited to applying to fraudulent conduct — if the preemption provision applied to them. Given the approach prevailing in state law antispam actions, companies sending commercial e-mail can generally continue to rely on the decision in *Omega* in determining whether the state law is preempted by CAN-SPAM.

FRENCH CNIL SAYS "*NON*" TO CELL PHONE ADS

French service providers proposed to install blue tooth antennas in billboards that would transmit messages to cell phone owners as they pass by. The message initially sent to the phone would not contain an advertisement itself, but merely a text informing the user that they can access an advertisement or promotional offer by responding to the message. Cell phone owners would receive the message only if their blue tooth functionality is activated.

In spite of these precautions, the French data protection authority ("CNIL") rejected the system, holding that the consumer needed to give his consent before receiving the initial invitation message. For advertisers, this obviously poses a "chicken and egg" problem because the only way to seek the consumer's consent is to contact the consumer first to ask. The CNIL said that the use of Near Field Communications ("NFC") advertisements would raise fewer problems because users manifest their consent before receiving any message.

In NFC-based advertising, a billboard in the street would propose (on the billboard) that cell phone owners download a promotional offer by placing their cell phone within an inch of the billboard. According to the CNIL, the act of placing one's cell phone within one inch of a billboard constitutes sufficient consent by the user to receive the advertisement.

The CNIL's decision on blue tooth advertisements is logical if one compares the blue tooth message to a commercial SMS or e-mail, the sending of which requires an opt-in by the user. However, it could be argued that a blue tooth communication is less intrusive than an unsolicited SMS because the blue tooth functionality can be disabled without the cell phone user losing his ability to communicate with others by SMS.

One could argue that by activating a blue tooth in public places, the user is opening himself to advertisements much as if the user was surfing on the Internet. Mobile handsets will soon become the principal means to access the Internet, whether by WiFi, 3G, or 4G wireless technologies. It will be critical for data protection authorities to take a technology-neutral position with regard to online advertising, making sure that the rules apply regardless of whether the terminal is fixed or mobile.

Published in the March 2009 issue of Privacy & Data Security Law Journal.

As noted in the earlier article on Belgian viral marketing, European data protection law imposes a strict opt-in rule to unsolicited commercial communications sent by e-mail or SMS. Banner advertisements on the Internet that make use of cookies are subject to more flexible rules because the consumer can easily opt out or otherwise disable the cookies and pop-ups. As the mobile Internet develops, it may be tempting for data protection authorities to extend the strict opt-in rules applicable to unsolicited e-mails and SMSs to all forms of "push" advertising on mobile devices.

However, soon there will be little difference between the fixed and mobile online experience. Each case of online advertising will have to be analyzed individually, based on the data protection rules already developed for the fixed online world.

NOTES

[1] 201 CMR 17.02.
[2] 201 CMR 17.03(g).
[3] *Thomasson v. GC Services LP*, No. 07-56215.
[4] *Id.* at 4 (citing Cal. Penal Code § 632(b); *Ribas v. Clark*, 38 Cal. 3d 355, 363 (Cal. 1985); *Robers v. Ulrich*, 52 Cal. App. 3d 894, 899 (Cal. App. 1975)).
[5] *Id.* at 3 (citing 15 U.S.C. § 1692e).
6 *Id.* (citing 15 U.S.C. § 1692e(10)).
[7] *Id.*
[8] Pub. L. No. 109-21, 119 Stat. 359.
[9] *Jaynes v. Commonwealth*, 666 S.E.2d 303 (Va. 2008).
[10] *Kramer v. Perez*, 2008 WL 4417290 (S.D. Iowa Sept. 30, 2008).
[11] 15 U.S.C. § 7707(b)(1).
[12] 469 F.3d 348 (4th Cir. 2006).

Published in the March 2009 issue of Privacy & Data Security Law Journal.