Privacy and Data Security Law Update

TRACY B. GRAY, WIM NAUWELAERTS, AND SARAH REISERT

NEW NEVADA LAW REQUIRES ENCRYPTION FOR TRANSMISSION OF PERSONAL INFORMATION

Nevada's new data security law, which mandates that customer personal information be encrypted prior to transmission, went into effect on October 1, 2008.

Companies that do business on a nationwide basis should consider whether their existing data security policies and procedures comply with this new state law. Specifically, the new Nevada law states: "a business in this State shall not transfer any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission."[1]

The Nevada statute, signed into law in 2005 and effective this month, defines "personal information" as a "person's first name or first initial and last name in combination with any of the following: (a) social security number or employer identification number; (b) driver's license number or identification card number; or (c) account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's finan-

---

Tracy B. Gray, Wim Nauwelaerts, and Sarah Reisert are attorneys with Hogan & Hartson LLP. Winston J. Maxwell, Tarah S. Grant, Tulasi A. Leonard, Matthew F. Wood, and Jamillia P. Ferris, attorneys with the firm, assisted with the preparation of this article.

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

cial account."[2] This definition of "personal information" is reasonably clear, and is consistent with state data breach notification laws, including Nevada's.

However, other terms used in the new law are more ambiguous, leaving the scope of the law uncertain. For example, on its face, the statute does not limit the terms "customer" or "personal information" to Nevada residents, although there are obviously jurisdictional issues with this omission.

Moreover, while this law states that it applies to a "business in this state," it is not clear whether a business that is geographically located outside of Nevada with personal information from Nevada residents may nonetheless be subject to the law as a result of "doing business" within the state.

While numerous states have enacted laws that require businesses to take affirmative steps to safeguard certain types of personal information and to notify persons whose personal information might be compromised in the event of a security breach, Nevada's new law goes one step further by specifically requiring the "encryption" of personal information. (The new law supplements and does not replace or modify Nevada's current data breach notification law.)

Notably, however, the new law's definition of "encryption" is broad, giving businesses some leeway in adopting compliance procedures. "Encryption" is defined as "the use of any protective or disruptive measure, including, without limitation, cryptography, enciphering, encoding, or a computer contaminant to: (i) prevent, impede, delay, or disrupt access to any data, information, image, program, signal, or sound; (ii) cause or make any data, information, image, program, signal, or sound unintelligible or unusable; or (iii) prevent, impede, delay, or disrupt the normal operation or use of any component, device, equipment, system, or network."

Companies operating nationally should verify that their information security policies address "transmission" and otherwise satisfy the requirements of this new Nevada law.

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

TELEMARKETING SALES RULE AMENDMENTS AFFECT CALL ABANDONMENT AND PRERECORDED CALLS

On August 19, 2008, the Federal Trade Commission ("FTC") issued two amendments to the Telemarketing Sales Rule ("TSR") that affect prerecorded calls. The first amendment modifies the TSR's method of calculating the maximum permissible level of "call abandonment," and became effective on October 1. The other amendment expressly bars prerecorded telemarketing calls unless a consumer previously has agreed to receive such calls from the seller.

The Technical Amendment

On October 1, 2008, the FTC implemented a new method for measuring the maximum call abandonment rate prescribed by the TSR's call abandonment safe harbor. Call abandonment generally results when telemarketing equipment known as predictive dialers reach more consumers than can be connected to a sales representative and either hang up on some consumers or leave a period of "dead air" before a sales representative can speak with the consumer.

While the TSR prohibits telemarketers from abandoning calls, the FTC nevertheless provides a safe harbor to preserve telemarketers' or sellers' ability to use these predictive dialers. To fall within the safe harbor, telemarketers and sellers must ensure that:

1. No more than 3 percent of all calls answered by a person are abandoned;
2. The telephone rings for at least 15 seconds or four rings;
3. A prerecorded message is played, stating the name and telephone number of the seller whenever a sales representative cannot be accessed within two seconds of the consumer hearing a completed greeting; and
4. Records documenting compliance are maintained.

The previous TSR standard for measuring the permissible call aban-

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

donment rate under this safe harbor required that a seller or telemarketer employ "technology that ensures abandonment of no more than three percent of all calls answered by a person, measured by *per day calling campaign.*" Sellers and telemarketers will now employ technology that calculates the call abandonment rate "*over the duration of a single calling campaign, if less than 30 days, or separately over each successive 30-day period or portion thereof that the campaign continues.*"

The amended standard is designed to permit the use of smaller, segmented calling lists, which are intended to ensure that telemarketing offers target those consumers who are most likely to be interested in the product or service, without an appreciable increase in call abandonment. The FTC proposed this amendment to remedy the problem that arises from the use of predictive dialers with such calling lists — when the group of consumers to be called is smaller, the deviation from expected answering and abandonment rates is greater.

Now, as a result of this amendment, sellers and telemarketers will not need to implement inefficient procedures, such as relying on manual dialing, slowing outgoing calls, or expanding campaigns to larger groups of consumers to minimize the effect of variations in the abandonment rate, in order to comply with the amended call abandonment standard.

The Prerecorded Call Amendment

The amendment to prerecorded call requirements will take effect in two stages. First, the requirement that prerecorded calls provide an automated interactive opt-out mechanism will take effect on December 1, 2008. This amendment, which added Section 310.4(b)(1)(v)(B) to the TSR, requires that any "outbound telephone call" delivering a prerecorded message must follow these six requirements:

1. Allow the consumer's telephone to ring for at least 15 seconds or four rings before an unanswered call is disconnected;
2. Begin the prerecorded message within two seconds of the completed greeting to the person called;
3. Disclose promptly at the outset of the call the means by which the

person called may assert a Do-Not-Call request at any time during the message;

4. If the call could be answered in person, promptly make an automated interactive voice and/or key press-activated opt-out mechanism available at all times during the message that automatically adds the telephone number called to the seller's entity-specific Do-Not-Call list and thereafter immediately terminates the call;
5. If the call could be answered by an answering machine or voicemail service, promptly provide a toll-free telephone number that also allows the person called to connect directly to an automated voice and/or key press-activated opt-out mechanism that is accessible at any time after receipt of the message; and
6. Comply with all other requirements of the TSR and applicable federal and state laws.

Second, the prohibition against delivering prerecorded messages without the prior express written consent of the consumer will take effect nine months later, on September 1, 2009. Consequently, telemarketers and sellers will no longer be able to initiate outbound telephone calls that deliver a prerecorded message "to induce the purchase of any good or service" unless they have obtained from the call recipient an express written agreement that demonstrates or includes:

1. The seller obtained the consumer's authorization to place such calls after providing clear and conspicuous disclosure that the purpose of the agreement is to permit delivery of prerecorded calls to the consumer;
2. The seller obtained written consent without requiring the agreement to be executed as a condition of purchasing any good or service;
3. The consumer's willingness to receive prerecorded calls on behalf of a specific seller; and
4. The consumer's telephone number and signature, which may be obtained in any matter permitted by the E-Sign Act.

When fashioning the Section 310.4(b)(1)(v) amendment, the FTC carved out two exemptions. All healthcare-related calls subject to the Health Insurance Portability and Accountability Act will be exempt from the amended TSR requirements, while calls made by for-profit telemarketers on behalf of a non-profit charitable organization to its members or donors will be subject to the opt-out requirements but will be exempt from the prior written agreement requirement.

The FTC also made clear that calls that comply with the opt-out and written agreement requirements will not violate the call abandonment prohibition, discussed above, solely because the consumer is connected within two seconds to a recording instead of a telemarketer. Otherwise, all calls that deliver noninteractive prerecorded messages will be prohibited.

The FTC will revoke its forbearance policy upon implementation of the opt-out requirements on December 1, 2008. Nevertheless, sellers may place prerecorded calls to both existing and new customers with whom they have an Established Business Relationship ("EBR") until stage two of the Prerecorded Call Amendment takes effect on September 1, 2009, so long as they comply with Section 310.4(b)(1)(v)(B). Once stage two of the amendment takes effect, the written agreement requirement will replace the EBR requirement as the sole authorization for placing prerecorded calls to numbers on the registry.

Sellers and telemarketers that deliver prerecorded calls should ensure that their calling systems are modified to reflect the FTC's recent amendments. In particular, such sellers and telemarketers should conduct the needed employee training on the new TSR requirements and should implement the necessary mechanisms, such as revised contracts, redesigned web sites, and/or new policies to obtain and record customers' express written consent before attempting to deliver prerecorded calls.

ARTICLE 29 WORKING PARTY EVALUATES WORLD ANTI-DOPING AGENCY'S INTERNATIONAL PRIVACY STANDARD

In the wake of the recent Beijing Olympic Games and with a view to preserving a level playing field in international sports, the Anti-Doping

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

Organizations ("ADOs") — consisting of sports movements and governments — are exposing athletes worldwide to more rigorous and more frequent doping tests.

As members of the World Anti-Doping Agency ("WADA"), ADOs must comply with WADA's Anti-Doping Code (the "Code") when testing athletes for doping and processing their personal data for that purpose. The processing of personal data for anti-doping purposes is a contentious issue, given the fact that data and samples collected from athletes are freely exchanged between the different authorities and across borders.

The Standard vs. the Code

In light of the controversy surrounding data processing in doping cases, WADA introduced an international standard (the "Standard") for the protection of athletes' privacy and personal information. On September 20, 2008, WADA approved the final version of the Standard, but urged for continued cooperation and dialogue with European governments to better protect the privacy of athletes.

The Standard lays down minimum privacy protection and provides guidance to national and international ADOs, as well as event organizers regarding the collection and further handling of athletes' personal data. The Standard should be read in conjunction with the Code, in particular Article 14, which deals with public disclosure and data privacy. Both the updated version of the Code and the Standard are expected to enter into full force and effect on January 1, 2009.

The Standard vs. the EU Data Protection Directive

On August 1, 2008, the Article 29 Working Party published its Opinion 3/2008, which assesses the Standard under the principles of the EU Data Protection Directive (the "Directive"). While Opinion 3/2008 considers the previous version of the Standard (before WADA approved the final version on September 20, 2008), it still provides a useful discussion on the possible shortcomings of the Standard from a privacy perspective.

First, the Working Party welcomes the fact that the Directive is mentioned in the preamble of the Standard and that the Standard emphasizes

that data protection issues should not be ignored by ADOs. The Working Party adds, however, that the Standard does not provide the high level of data protection imposed by the Directive.

For instance, the Standard raises concerns with relation to the Anti-Doping Administration and Management System ("ADAMS"), a web-based database management tool for data entry, storage, sharing, and reporting designed to assist stakeholders and WADA in their anti-doping operations. It is not clear what kind of sensitive data may be processed in ADAMS (e.g., race, gender, etc.) and what rules and policies apply to their processing.

Furthermore, the legal basis invoked by WADA for processing of personal data raises questions. WADA claims that athletes' consent is obtained, but, as the Working Party notes, under the Directive consent must be informed and freely given. The Working Party apparently is not convinced that the consent obtained from athletes meets this test.

In addition, the Working Party queries whether WADA needs to gather genetic information relating to athletes for the purpose of preventing doping in sports. The Working Party also invites WADA to agree on a maximum retention period for athletes' personal data, with an obligation to erase the data when it is no longer needed for doping control purposes.

The Article 29 Working Party's Verdict

Suitable data protection ensures that doping in sports is combated with appropriate means, while respecting athletes' privacy rights. However, while the Standard is a step in the right direction, the question remains whether it offers an adequate level of data protection in accordance with the Directive. The Working Party does not seem to think so. Whether WADA will take all of the Working Party's comments and recommendations into account and amend the Standard accordingly, remains to be seen.

SIXTH CIRCUIT DECISION LEAVES OPEN CONSTITUTIONALITY OF STORED COMMUNICATIONS ACT

The Sixth Circuit *en banc* has reversed a Sixth Circuit panel decision, *Warshak v. United States*,[3] in which the *Warshak* Panel held that the gov-

ernment's attempt to compel disclosure of communications kept in electronic storage for more than 180 days without a search warrant or prior notice violated the Fourth Amendment.[4]

The *en banc* court concluded that the question presented was unripe and, consequently, left unresolved the issue of whether the Fourth Amendment renders unconstitutional the provisions of the Stored Communications Act ("SCA") that provide for compelled production of stored communications without a warrant or prior notice to the user.

Under § 2703(d) of the SCA, a court may issue an order for compelled disclosure of certain communications based on "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing investigation."[5] Required prior notice of the disclosure may be delayed under certain circumstances.[6]

Relying on these provisions of the SCA, the government requested that a magistrate judge issue orders to compel certain ISPs (NuVox Communications and Yahoo!) to produce account information related to Steven Warshak, a target of a government investigation. The requested information included "[t]he contents of wire or electronic communications (not in electronic storage unless greater than 181 days old) that were placed or stored in directories or files owned or controlled by Warshak."

The magistrate granted the government's request after concluding that the government had demonstrated "reasonable grounds to believe that the records or other information sought [were] relevant and material to an ongoing criminal investigation," and that the prior notice requirement could be avoided because notice "would seriously jeopardize the investigation."

A year later, the government gave Warshak notice of the orders issued to the ISPs. In response, Warshak filed a complaint against the government and sought a preliminary injunction, in which he alleged that § 2703(d) violated the Fourth Amendment because the searches were based on a showing of less than probable cause and were not supported by a warrant.

The U.S. District Court for the Southern District of Ohio granted

Warshak's motion for a preliminary injunction finding that Warshak was likely to succeed on his Fourth Amendment claim. That court concluded that Internet users have a reasonable expectation of privacy in e-mails, and that the magistrate's orders authorized warrantless searches on less than probable cause.

The district court also found that Warshak faced imminent harm in light of the magistrate's prior orders and the government's refusal to not seek additional orders in the future. The Warshak Panel affirmed the lower court's opinion.

The Sixth Circuit *en banc* has now vacated the decision stating that, because Warshak now had notice of the previous orders and investigation, the actual question presented was whether the government would conduct another ex parte search of Warshak's e-mails. The court held that this issue was unripe because, inter alia, the uncertainty (and indeed, unlikelihood) that the government would conduct such an ex parte search of Warshak's e-mail account in the future and, even if such a search were to occur, what accounts or types of accounts would be at issue.

The court stated that this uncertainty would require it to hypothesize as to how a service provider would respond to a future request for records, as well as speculate as to the terms of that service provider's agreement with its users. In particular, without knowing the terms of the agreement between the user and the relevant service provider, the appropriate limits on the user's reasonable expectation of privacy were unknown.

In addition, the Sixth Circuit rejected the assertion that Warshak faced a risk of hardship because the challenged provisions (and their absence of primary conduct regulations) did not require Warshak to do anything to avoid future adverse consequences. Furthermore, the court stated that individuals subject to unreasonable searches and seizures could file a motion to suppress, or a post hoc challenge under other statutes.

The opinion garnered a dissent from five of the judges, who decried the court's failure to directly answer whether the delayed notification under the SCA is constitutional and characterized the decision as "another step in the ongoing degradation of civil rights"—a statement that like-

ly will be echoed by privacy advocates who have argued in favor of a Fourth Amendment expectation of privacy in the content of e-mail communications.

Ultimately, the Sixth Circuit's recent decision precluded targets of ex parte government searches from prospectively challenging searches brought under § 2703(d), leaving such challenges to the electronic communications providers, who have immunity from suit under SCA § 2703(e) and may have little incentive to bring such a claim when faced with a government request for access to electronic records.

FEDERAL DISTRICT COURT RULING REQUIRES A WARRANT TO OBTAIN CELL PHONE USER LOCATION INFORMATION

A federal judge in the Western District of Pennsylvania has ruled that the government must procure a search warrant before covertly obtaining information about cell phone users' geographic location from their wireless service providers.

The ruling perpetuates a continued split on this issue, with several courts concurring with this decision, while other federal courts have found that a warrant is not necessary under similar circumstances. The issue is not yet resolved, and may need to be addressed by appellate courts in order to get consensus.

The opinion issued on September 10, 2008, upheld a more extensive February 2008 federal magistrate's ruling. That magistrate's decision required the government to show probable cause when seeking a court order that would compel a wireless provider to turn over location tracking information without the subscriber's knowledge or consent.

The key issue in such cases is the need for law enforcement to satisfy the Fourth Amendment's probable cause standard. As the Pennsylvania magistrate stressed, "the issue is not whether the Government can obtain movement/location information, but only the standard it must meet to obtain a Court Order for such disclosure."

The Department of Justice argued that the Stored Communications Act ("SCA"), 18 U.S.C. § 2703, authorizes a wireless carrier to provide

detailed location information obtained by tracking the specific cell tower sites with which a subscriber's mobile device communicates. The government sought the information in this instance to follow the movements of a suspected drug trafficker, relying on language in the statute that allows a court to issue an order on a showing of "specific and articulable facts" demonstrating reasonable grounds to think that user records or "other information" may be relevant and material in an ongoing criminal investigation.

The Pennsylvania magistrate's decision rested on the Fourth Amendment and several statutory grounds, finding in particular that the SCA excluded "tracking device" communications from the law's definition of the information that the government may obtain under this statute. Courts in other districts have reached the opposite conclusion.

For example, a 2006 decision in the Southern District of Texas determined that no warrant was necessary, so long as the government sought cell-site information obtained during calls made by or to the subscriber, but did not seek information (such as GPS signals) that could be used to track the location of the phone when no call was in progress. A 2007 Massachusetts federal court decision held that the government could obtain historical cell-site data without a warrant, but distinguished historical records from real-time information that could be used to track a cell phone user's present whereabouts.

Despite these contrary outcomes, the Pennsylvania decision falls in line with federal court decisions denying government requests in the District of Columbia, Indiana, Maryland, New York, and Wisconsin. In the Pennsylvania case, the magistrate decided that the government should not have the benefit of the relatively lenient "specific and articulable facts" standard, as probable cause jurisprudence "require[s] only that the Government support its belief of criminal activity and the probable materiality of the information to be obtained."

The order expressed concern that, absent such a showing, governmental abuse could occur because of the ex parte nature of warrantless requests, the low cost of obtaining the information, and the undetectable nature of the process used to transfer information to the requesting authorities.

While acknowledging the "important and sometimes critical crime prevention and law enforcement value of tracking suspected criminals," the Pennsylvania magistrate concluded that the value of warrantless access to this information was outweighed by the need for more stringent judicial review to protect civil liberties such as the rights of privacy and free association. The magistrate focused on the need to protect "extraordinarily personal and potentially sensitive" location information that is frequently and broadly sought by the government, but without subscriber consent.

Another interesting point of comparison, beyond the different outcomes in the U.S. court system, is the treatment of cell phone users' geographic location information under European Union privacy directives. For example, in electronic communications and personal privacy standards adopted as early as 2002, the EU generally has prohibited the collection and processing of location data without the explicit consent of the mobile device user. Nevertheless, these same EU standards permit member states to restrict such privacy rights when necessary to trace nuisance calls or to provide emergency services.

No matter the resolution of the split between U.S. courts, wireless providers can expect to continue receiving court orders requiring them to provide cell phone location information without subscriber consent. If higher courts ultimately determine that warrants are necessary in such instances, however, that decision could reduce the government's willingness or ability to make requests as frequently.

ARTICLE 29 WORKING PARTY RELEASES UPDATE ON GOOGLE DISCUSSIONS

On September 16, 2008, the Article 29 Working Party published a brief status report on its ongoing dialogue with Google regarding how Google is protecting the privacy rights of its search engine users in Europe. The dialogue with Google emerged from a previous Working Party opinion (published on April 4, 2008), in which the Working Party examined the responsibilities and duties of search engine providers under European data protection law.

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

In reaction to that opinion, Google recently confirmed its willingness to cooperate with the Working Party to enhance Internet users' privacy protection. Google also announced two modifications to its existing data protection practice.

First, the retention period for users' personal data will be reduced from 18 to nine months. After nine months, IP addresses associated with requests carried out via the search engine will be made anonymous, at which time they will no longer be considered personal data under the EU Data Protection Directive. Second, a link to Google's privacy policy will appear on its homepage.

The Working Party applauded these changes in its September 16, 2008, press release, but emphasized that Google's data retention period is still too long (the Working Party does not see a basis for a retention period beyond six months).

Also, the parties strongly disagree about other important issues, such as the applicability of European data protection law. Google believes that the European rules on data protection are not applicable to the company, even though it has servers and establishments in Europe.

The Working Party's position, on the other hand, is that the EU Data Protection Directive generally applies to the processing of personal data by search engines, even if they are headquartered outside Europe. The Working Party intends to organize hearings with Google to address the outstanding points of dissension.

NINTH CIRCUIT PRESERVES CALIFORNIA'S RESTRICTIONS ON INFORMATION SHARING WITH AFFILIATES

Decision May Further Restrict Financial Institutions' Activities

Financial institutions that want to share customer information with their affiliates must now give California residents more notice and control over how that information is shared. The Ninth Circuit recently ruled that the Fair Credit Reporting Act ("FCRA") does not preempt California's Financial Information Privacy Act (commonly referred to as "SB1") from being applied to any information that is not a "consumer report."[7]

This ruling adds clarity to an earlier Ninth Circuit decision that held that the FCRA preempts SB1 with respect to consumer reports.[8] The Ninth Circuit found that while the FCRA preemption provisions constrained SB1's notice and opt-out requirements, the court could sever the preempted application of the provisions. The court believed this interpretation clearly furthered the legislature's intent when passing the law. The majority therefore found that the FCRA only prohibits SB1's application to consumer report information and that the law could be applied to all other data.

Judge Wallace dissented from the opinion, arguing that, while SB1 gives the court authority to sever any "phrase, clause, sentence or provision," such authority does not extend to differing applications of the statute.

This decision means that non-consumer report information is now subject to California's stricter privacy regulations regarding affiliate sharing. Under the FCRA, consumer reports include any information that is:

1. provided by a consumer reporting agency;
2. bears on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living (the so-called "seven characteristics"); and
3. is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment purposes; or certain government licenses.

Therefore, the sharing of information about California residents not captured by this definition is constrained by SB1. Because courts have held that virtually all information about consumers bears on one of the seven characteristics, the critical questions in determining whether information is a consumer report and therefore exempt from SB1 are whether it is: (1) provided by a consumer reporting agency, and (2) expected to be used for one of the purposes discussed above.[9]

The practical impact of this decision is that financial institutions that

wish to share information other than consumer reports with their affiliates must provide California residents with notices that follow the prescribed statutory language, and allow them to opt-out and prevent companies from sharing that information (there are exceptions to the opt-out requirements, including data transfers done at the request of the consumer and transfers necessary to administer a transaction). Moreover, companies may draft their own notices, but they must be approved by banking regulators or the Office of Attorney General.

Ultimately, this ruling likely will have the biggest effect on financial institutions' ability to cross market products offered by affiliates to California residents.

EUROPEAN DATA PROTECTION AUTHORITIES TO FOCUS ON TRANSATLANTIC DISCOVERY REQUESTS

France's data protection authority, the CNIL, has decided to focus on transatlantic data transfers in the context of U.S. litigation and administrative investigations. The CNIL held a number of hearings in Spring 2008 to understand the scope of the problem and potential solutions.

On June 6, 2008, the American Chamber of Commerce in France presented to the CNIL a position paper intended to educate the CNIL about U.S. procedures, and in particular the ability of parties in a civil litigation to seek a protective order to safeguard the confidentiality of personal data.

The CNIL has not yet issued any recommendations, but intends to raise the issue at a European level within the Article 29 Working Party. (CNIL Chairman Alex Türk also currently chairs the Article 29 Working Party.)

Pre-trial discovery has often been a source of confusion and concern for Europeans. France enacted a blocking statute decades ago to protect French companies from discovery requests and administrative investigations in the United States.

At the time, the concern was that far-reaching discovery requests could be a way for U.S. companies to obtain competitively sensitive information about their European counterparts. Now the concern seems

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

to be that U.S. litigation may require the transfer of massive amounts of personal data to the United States without adequate protection.

During its testimony before the CNIL, the American Chamber of Commerce in France emphasized that discovery requests are subject to intense negotiation between the parties, the objective being to narrow the discovery request to cover only information that is truly relevant to the litigation. So-called "fishing expeditions" are not tolerated by U.S. courts.

The American Chamber of Commerce delegation also explained that the parties may ask the court to issue a protective order to ensure that information communicated to the other party in the context of U.S. litigation is kept confidential and destroyed or returned once the litigation is finished.

The CNIL has not yet issued formal guidelines regarding how to comply with discovery requests while still respecting European data protection law. One approach the CNIL (and the Article 29 Working Party) may consider is to issue a blanket authorization that would apply to the processing and transfer of personal data in the context of U.S. litigation, provided that the information is covered by a protective order issued by a U.S. court, which guarantees a certain level of protection.

The CNIL and/or the Article 29 Working Party would likely establish a list of criteria that the U.S. protective order would have to satisfy to qualify for the blanket authorization. This approach would equate to creating a special safe harbor for discovery requests that meet certain criteria.

YOUR USB FLASH DRIVE MAY BE WORTH A MILLION: DON'T LOSE IT!

"The cost of a USB flash drive may be insignificant but the value of the data it might contain can be priceless." With this statement in a study published by the European Network and Information Security Agency ("ENISA") in June, Executive Director Andrea Pirotti alerted companies to supervise their employees' use of USB flash drives.

In today's digital environment, the use of portable devices such as USB flash drives by corporate end-users is becoming more popular. These tools are convenient when traveling or working at home, and the

capacity for storing data on USB flash drives has increased significantly in recent years. However, the data on these plug and play devices is often insufficiently protected and their use is not always subject to corporate policies, back-up requirements, or encryption measures.

ENISA's recent study shows that the loss of a USB flash drive by a corporate end-user may have devastating financial consequences for a company. According to ENISA, the average cost per breach ranges from approximately $100,000 to $2.5 million. These figures can be explained by the fact that USB flash drives often contain sensitive business information.

According to a study conducted by the Ponemon Institute, more than half of the employees interviewed confessed to copying sensitive business information to USB flash drives, even though the vast majority of their employers prohibit such practice.

In the United States, loss of personal information stored on USB drives would trigger data breach notification state laws, and associated requirements.

Consistent with similar U.S. recommendations, ENISA emphasized the need for educating employees sufficiently about the risks involved in using USB flash drives and similar devices. ENISA also encouraged companies to develop security policies that employees should follow. Other preventive measures, such as the use of encryption methods, should also be considered.

Although not covered by the ENISA study, data breaches as a result of USB flash drive loss or theft can have major legal consequences. For instance, if confidentiality is a common clause in many business contracts today, loss of data relating to such business contracts could be viewed as a contractual breach.

Recently, the British government terminated its agreement with a consulting firm after the firm lost the personal data of convicts in England and Wales. UK Home Secretary Jacqui Smith ended the contract saying that "this was a clear breach of the robust terms of the contract covering security and data handling."

The ENISA study makes it clear that corporate end-users should handle USB flash drives with extreme care. They should always keep in

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

mind that losing data on a USB flash drive could harm the company's reputation or financial position, lead to the loss of jobs, or even result in the company's bankruptcy.

NINTH CIRCUIT EXPECTED TO RULE ON E-MAIL "INTERCEPTIONS" UNDER THE WIRETAP ACT

The U.S. Court of Appeals Ninth Circuit currently is reviewing the extent to which the "interception" prohibitions of the federal Wiretap Act apply when e-mails are copied in transit. The court's decision could have a significant impact on Internet privacy issues, particularly with respect to e-mail surveillance.

In *Bunnell v. Motion Picture Association of America*,[10] the MPAA allegedly violated the federal Wiretap Act by paying Rob Anderson, a former employee of TorrentSpy (a peer-to-peer search engine that facilitates file-sharing) $15,000 to hack in to the TorrentSpy e-mail server. Anderson allegedly hacked in to the server in 2005 and obtained copies of internal company e-mail messages (including e-mails and financial statements sent by TorrentSpy executives) as they were being transmitted. He then e-mailed the copies to the MPAA.

At issue in the case is whether Anderson's copying constitutes an "interception" under the federal Wiretap Act. That Act bars unauthorized interception of electronic communications, including e-mail, while the communications are being transmitted. The Act does not extend, however, to communications and data that are being stored on a server.

Because Anderson allegedly made copies of the e-mail messages while they were stored on the e-mail server, the trial court held that Anderson's actions did not violate the Wiretap Act. Although the e-mail messages were stored only for milliseconds before continuing on to their destination, the court agreed with MPAA that the actions technically did not constitute an "interception." Justin Bunnell, a TorrentSpy employee, appealed the decision.

The Electronic Privacy Information Center ("EPIC") and the Electronic Frontier Foundation ("EFF") both filed *amicus curiae* briefs in the Ninth Circuit case in support of Bunnell. EPIC argued that in pass-

ing the Wiretap Act, Congress "intended to bar the interception of e-mail messages at all stages of the messages' transmittal" and that the lower court's decision "threatens to strip citizens of vital privacy safeguards."

EFF stated that upholding the district court decision "would remove a vast amount of communications from the protection of the Wiretap Act," noting that "under the district court's holding, law enforcement officers could engage in the contemporaneous acquisition of emails just as Anderson did, without having to comply with the Wiretap Act's requirements."

It also stated that "without the threat of liability under the Wiretap Act, Internet service providers could intercept and use the private communications of their customers," and that "individuals could freely monitor others' email for criminal or corporate espionage purposes without running afoul of the Wiretap Act."

As privacy advocates point out, a decision in favor of the MPAA could have widespread consequences with respect to both private and public-sector e-mail surveillance. Moreover, depending on how the transmissions are made, the decision in *Bunnell* could impact other Internet-based transmissions and online activity.

NOTES

[1] Nev. Rev. Stat. § 597.970 (2005).

[2] *Id.*

[3] *Warshak v. United States*, 490 F.3d 455 (6th Cir. 2007).

[4] *Warshak v. United States*, 2008 WL 2698177 (6th Cir. July 11, 2008).

[5] 18 U.S.C. § 2703(d).

[6] Id. §§ 2705(a)-(b).

[7] *American Bankers Association v. Lockyer*, —- F.3d ——, 2008 WL 4070308.

[8] *American Bankers Association v. Gould*, 412 F.3d 1081 (9th Cir. 2005).

[9] *See TransUnion v. Federal Trade Commission*, 267 F.3d 809 (D.C. Cir. 2001) ("[A]lmost any information about consumers arguably bears on their personal characteristics or mode of living.").

[10] Bunnell is case number 07-56640 in the U.S. Court of Appeals for the Ninth Circuit.