

Lawsuits Challenge The NSA's Warrantless Data Mining And Surveillance Program

RANDY GAINER

This article discusses public information about the National Security Agency's data mining and electronic eavesdropping program, describes the issues in the lawsuits challenging the program, reports on the current status of the litigation, and analyzes the legal issues at stake.

A May 11, 2006 article in *USA Today*¹ reported that the National Security Agency (NSA) “has been secretly collecting the phone call records of tens of millions of Americans, using data provided by AT&T, Verizon, and BellSouth.”² The *USA Today* report followed December 2005 articles in *The New York Times*³ that described the NSA collection of call records in less detail and disclosed that the NSA was intercepting international e-mails and phone calls with one end in the United States. On June 23, 2006, the *L.A. Times*,⁴ the *Wall Street Journal*, and *The New York Times* reported that the Central Intelligence Agency and the Treasury Department have “gained access to financial records from a vast international database and examined banking transactions involving thousands of Americans and others in the United States.”⁵

The December and May disclosures of the NSA's domestic surveillance and data mining program prompted the filing of at least 22 lawsuits against the government and against telecommunications companies. The lawsuits challenge the government's use of the data, the companies' dis-

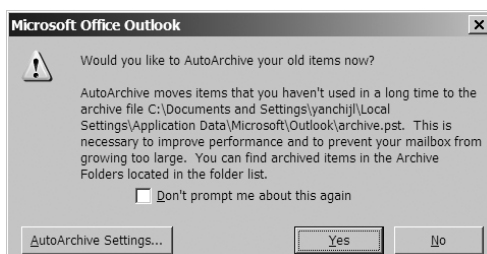
Randy Gainer is a partner in the Seattle office of Davis Wright Tremaine LLP. His practice emphasizes litigating computer system disputes and advising businesses about data security and privacy issues. The views expressed in this article are those of the author and not of Davis Wright Tremaine or any of its clients. Mr. Gainer can be reached at randygainer@dwt.com.

E-Discovery Perils: The AutoArchive Function — Not Gone, But Forgotten?

THOMAS J. SMITH

This article examines the hidden perils, from an e-discovery and records management perspective, of the AutoArchive function contained in Microsoft Outlook, the most popular e-mail program in use today in personal computers (PCs). Among other things, the AutoArchive function can bury electronic data many levels deep into a PC user's hard drive, where it may be missed inadvertently in responding to a subpoena or discovery request in litigation, or where it may be kept inadvertently longer than required by the applicable records management policy. PC users must be aware of the consequences of an active AutoArchive function on their PC.

An employee of a Fortune 500 company is sitting at her desk, busily responding to the dozens of e-mails she receives daily. Suddenly a prompt pops up on her screen that looks like this:



Thomas J. Smith is a partner in the Pittsburgh office of Kirkpatrick & Lockhart Nicholson Graham LLP. Mr. Smith, who concentrates his practice in the area of complex commercial litigation, is a founding member of the firm's Records Management & E-Discovery Practice Group, and has regularly counseled clients in matters involving complex records preservation and collection issues, litigation "holds," e-discovery, and records management and retention policies. He can be reached at tsmith@king.com.

closure of the data, or both.⁶ Lawsuits challenging the government's use of the financial records may be next.

GOVERNMENT DATA MINING, PAST AND PRESENT

“Data mining” is generally accepted to mean “the iterative process of detecting and extracting . . . patterns from large data basis.”⁷ Data mining “facilitates the ability to sort through masses of information through database exploration, extract specific information in accordance with defined criteria, and then identify patterns of interest to its user.”⁸ Commercial companies, such as Amazon.com, use data mining to identify patterns of buying behavior so that they can market to targeted consumers with information that is tailored to those consumers.

Commercial companies such as Acxiom, LexisNexis, and others, have also been collecting information from publicly available databases and buying data from private companies for years. These “data aggregators” sell data in the private sector and to the federal government on “over 150,000,000 individuals residing in over 100,000,000 households” in the United States.⁹

Prior to the September 11 attacks, federal agencies used data mining techniques to identify fraudulent misuse of government funds.¹⁰ After the September 11 attacks, the Department of Justice and the Department of Defense have mined government data and data purchased from private companies to try to identify terrorists.¹¹ The NSA reportedly uses software algorithms to analyze the call record data that it is obtaining from telecommunications companies to attempt to identify patterns that point to individuals, telephone numbers, or Internet addresses that the government then focuses on for further investigation. The NSA likely attempts to cross-reference its call record analyses with results from analyzing data that it purchases from data aggregators, including travel and financial records. The June 2006 report that the CIA and Treasury Departments have obtained the entire database of international money transfer records from the Society for Worldwide Interbank Financial Telecommunication (Swift) likely provided another huge database for the government to mine.¹²

The anti-terrorist data mining programs have been criticized by

technologists because statistical principles dictate that the programs will produce too many “false positives” to be useful.¹³ These critics point out that, even if a program is 99.9% accurate, it will produce one false positive in each 1,000 searches. Given that the government is reportedly analyzing millions, billions, or more of pieces of information, the analyses will produce thousands of false positive “hits.” This appears to be what has occurred, according to another report: the FBI was overwhelmed by a stream of thousands of dead-end “leads” generated by the NSA after the September 11 attacks.¹⁴

Privacy experts also criticize the data mining programs because they rely on data that can be erroneous, which can produce serious consequences.¹⁵ Daniel Solove provides a real-world example of a woman who was wrongly arrested for burglary but whose arrest record was not cleared from the state’s criminal databases. She was later fired from her job as a substitute school teacher and only rehired after she could prove that the information in the database was wrong.¹⁶ The use and misuse of such data can lead to a sense of frustration and powerlessness.¹⁷

Several Senators are among those who have criticized the NSA’s data mining program.¹⁸ On the other hand, Bush administration officials defend the warrantless collection and analysis of massive databases, claiming, for example, that the use of the Swift financial data enabled law enforcement to capture an al Qaeda operative in Thailand in 2003 and helped convict an individual in New York in 2004 of laundering funds for al Qaeda.¹⁹ Critics of the data mining programs respond that, even if the programs generate positive results, they could have been and should have been authorized by statutes or court orders rather than by unilateral executive action.

LEGAL CHALLENGES TO THE NSA PROGRAM

Pending Cases

The Electronic Frontier Foundation (EFF),²⁰ the ACLU,²¹ and the Center for Constitutional Rights²² challenged the NSA program in lawsuits filed in January 2006.²³ The plaintiffs in the EFF case, *Hepting v. AT&T*, claimed that AT&T violated the Electronic Communications

Privacy Act and other federal and California statutes, and violated the First and Fourteenth Amendments to the United States Constitution as an agent of the government. The ACLU and the CCR lawsuits claim that NSA's interception of international phone calls and e-mail traffic, as well as its data mining of call records, violate the Foreign Intelligence Surveillance Act (FISA), and the First and Fourth Amendments to the United States Constitution.

After the *USA Today* article was published in May 2006, more than 20 class action lawsuits were filed against Verizon, AT&T, and BellSouth, alleging that the companies' participation in NSA data mining violates federal communications statutes. Most of the class actions filed after the May 2006 *USA Today* article seek compensatory and punitive damages, as well as other relief.²⁴

Hearings To Date

Hearings on substantive issues have been held in both the *ACLU* and *Hepting* cases. On June 12, 2006, Judge Anna Diggs Taylor of the Eastern District of Michigan heard the ACLU's motion for partial summary judgment and for an injunction against the NSA. Judge Taylor earlier denied the NSA's motion to stay consideration of the plaintiffs' motion until after the court resolved the government's state secrets motion.²⁵ The ACLU motion challenges the NSA's interception of the contents of international e-mails and telephone calls. The ACLU claimed that such interceptions violate FISA and the First and Fourth Amendments.

In their briefs and at oral argument on the motion, ACLU attorneys described how the NSA program has disrupted the communications of the journalists, scholars, and criminal defense attorneys who are among the plaintiffs in the action and explained why such concrete injuries provide standing. The ACLU also explained why the Authorization for Use of Military Force (AUMF), which Congress passed after the September 11 attacks and which authorized the war in Afghanistan, did not authorize the NSA to conduct warrantless domestic surveillance. The ACLU also explained why it contends that the president does not have authority under Article II of the Constitution to ignore the provisions of FISA and of Title III of the Omnibus Safe Streets Act that provide that electronic

surveillance may only be conducted with a FISA Court order or a search warrant.

Government lawyers for the NSA explained in their briefs and at oral argument why the government believes the state secrets doctrine requires dismissal. (This claimed defense was the subject of a separate hearing on July 10.) They also argued that the plaintiffs do not have standing because their injuries are allegedly subjective, that the president has inherent power as Commander in Chief to override or ignore FISA and Title III, and that the AUMF authorized the warrantless domestic electronic surveillance. The court issued a decision in the case after this article was submitted. See *ACLU v. NSA*, 438 F. Supp. 2d (E.D. Mich., August 17, 2006).

In the *Hepting* case pending in the Northern District of California, Judge Vaughn R. Walker held a hearing on June 23, 2006. The government, which intervened in the action, asked the court to dismiss the case or to grant summary judgment to the defendants on the basis of the state secrets privilege. On June 20, Judge Walker issued an order asking 11 questions, which he directed the parties to be prepared to address at oral argument.²⁶ Judge Walker's questions ranged, from whether an interlocutory appeal and stay should be granted if the case were dismissed, to whether an expert on state secrets should be appointed to advise the court if the case is not dismissed.²⁷

The government argued that the "very subject matter" of the *Hepting* action is a state secret, or if it is not, that the plaintiffs cannot make out a *prima facie* case and the defendants cannot prove valid defenses without risking the disclosure of state secrets.²⁸ The *Hepting* plaintiffs countered that the government's state secret claim should be denied for five reasons:

- (1) Congress has limited the applicability of the state secrets privilege by adopting FISA and other statutory limitations;
- (2) Plaintiffs' claims can be proved by information available in the public record, through declarations of plaintiffs' witnesses, and by the government's admissions;

- (3) The issue of whether the government “certified” that AT&T could lawfully provide call records to the NSA is not a valid defense to plaintiffs’ claims;
- (4) Plaintiffs can establish their standing from public records or through limited discovery; and
- (5) If the state secrets privilege applies, it should be applied to specific factual issues and not as a basis for wholesale dismissal.²⁹

Law professors from the University of San Francisco, Cornell, Ohio State, George Washington University, and Duke University, who are represented by two Stanford Law School professors, filed an *amicus* brief supporting the *Hepting* plaintiffs’ arguments on the state secrets issues.³⁰ The law professor *amici* argued that the defendants can successfully oppose the *Hepting* plaintiffs’ claims by one of three options: by disputing the evidence provided by plaintiffs’ witnesses; by acknowledging the interceptions but claiming that they acted pursuant to a court order issued under 18 U.S.C. § 2518, or by claiming that they relied on an invalid court order but in good faith, pursuant to 18 U.S.C. § 2520(d).³¹ The *amici* point out that, while the court may need to review “a piece of paper” to assess the latter defense, the court could examine such a document *in camera* without risking the disclosure of state secrets.³²

The government in its reply in *Hepting* contends that plaintiffs have not established standing or a *prima facie* case; that public disclosure of some facts does not preclude the assertion of the state secrets privilege; that plaintiffs contradict their position by demanding discovery; that the state secrets privilege is derivative of the president’s Article II powers, which has not been superseded by Congressional action; and that Congress has not abrogated certain statutory privileges on which the government relies.³³

At oral argument on the state secrets motion, Judge Walker reportedly raised questions about the limits of the privilege.³⁴ The court issued a decision in the case after this article was submitted.³⁵

Motions To Transfer And Consolidate

Verizon filed a motion on May 24, 2006 in the Judicial Panel on

Multidistrict Litigation (JPML). The motion asks the panel to transfer and consolidate for pre-trial proceedings the approximately 20 class action cases challenging telecommunications companies' disclosure of call records to the NSA. The motion relies on 28 U.S.C. § 1407.

The government filed a response to Verizon's motion on June 19 that concurs with Verizon's motion and asks that five "added actions" be transferred to the D.C. District Court, together with the cases identified by Verizon. The government named the ACLU and CCR cases among the five "added actions" that it asked to be transferred and consolidated.³⁶ In its response to the Verizon motion, the government stated that it intended to invoke the state secrets privilege in all of the cases subject to the requested transfer.³⁷ After the JPML declined to treat the government's request in its response as a motion to transfer the "added actions," the government wrote a letter to the JPML asking that the "added actions" be treated as "tag-along" cases pursuant to the panel's rules.³⁸

The *Hepting* and *Terkel* plaintiffs filed responses to Verizon's motion to the JPML, objecting to the proposed transfer and consolidation. The plaintiffs in the five "added actions" should have an opportunity to oppose any proposed transfer and consolidation of those cases.³⁹ The court issued a decision in the case after this article was submitted. See *In re NSA Telecommunications Litigation*, 2006 WL 2347798 (JPML, August 9, 2006).

FUNDAMENTAL SEPARATION OF POWERS PRINCIPLES ARE AT ISSUE IN THE NSA CASES

The government can take effective action against al Qaeda and other terrorists and still comply with the law, as the government's experience with almost thirty years of FISA orders demonstrates. During operation of the FISA court, only four of more than 19,000 requests for FISA surveillance orders have been denied, 180 were modified, and the remaining 18,451 were granted without modification.⁴⁰ Both the FISA Court and other federal courts regularly review classified information and do so without leaking it or otherwise damaging national security.⁴¹ If the Bush administration believed it needed even more permissive domestic surveil-

lance powers, it could have asked Congress to amend FISA or could have asked for other authority for its warrantless data mining and eavesdropping programs.

In *Youngstown Sheet & Tube Co. v. Sawyer*,⁴² Justice Jackson stated in his concurrence that the president's Article II powers as Commander in Chief are "subject to limitations consistent with a constitutional Republic whose law and policy-making branch is a representative Congress."⁴³ He explained:

When the President takes measures incompatible with the expressed or implied will of Congress, his power is at its lowest ebb, for then he can rely only on his constitutional powers minus any constitutional powers of Congress over the matter. Courts can sustain exclusive Presidential control in such a case only by disabling the Congress from acting upon the subject.⁴⁴

The cases challenging the NSA's warrantless data mining and electronic surveillance program ask the courts to determine whether Congress' prohibition of domestic electronic surveillance for foreign intelligence purposes should be upheld. If not, then Congress will be disabled from regulating such surveillance.

If the courts accept the government's two arguments—that the president has Article II power to ignore statutory prohibitions and that the state secrets privilege prevents the courts from questioning that power—the president will have succeeded in expanding his powers to a dangerous level. As recently as 2004 the Supreme Court held that courts must ensure that power is never "condense[d] . . . into a single branch of government."⁴⁵

The decisions of the courts in the cases challenging the NSA's domestic surveillance and data mining programs will undoubtedly be appealed. The cases will likely be decided ultimately by the Supreme Court. The most critical issue among the many important issues in the cases is whether the courts will allow the president to usurp key powers of both Congress and the courts.

NOTES

- 1 Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, A1.
- 2 *Id.*
- 3 James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, NY TIMES, Dec. 16, 2005, A1; and James Risen and Eric Lichtblau, *Spy Agency Mined Vast Trove, Officials Report*, NY TIMES, Dec. 24, 2005, A1.
- 4 Josh Meyer and Greg Miller, *Secret U.S. Program Tracks Global Bank Transfers*, L.A. TIMES, June 23, 2006, available at <http://www.latimes.com/news/nationworld/nation/la-na-swift23jun23,0,6482687.story?coll=la-home-headlines> (last visited June 26, 2006).
- 5 Eric Lichtblau and James Risen, *Bank Data Sifted in Secret by U.S. to Block Terror*, NY TIMES, June 23, 2006, A1.
- 6 See Verizon's Schedule of National Security Agency Actions for Transfer and Coordination, MDL Docket No. 1791, filed May 24, 2006, which lists 20 such actions, three of which have been voluntarily dismissed. See also the United States' schedule of added National Security Agency actions for transfer and coordination, MDL Docket No. 1791, filed June 19, 2006, which lists five cases.
- 7 Jesus Mena, *Data Mining Your Web Site*, 5 (Digital Press 1999).
- 8 Prepared Statement of Mark A. Forman, Associate Director for Information Technology and E-Government, Office of Management & Budget, Hearing Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations & Census on March 25, 2003 ["March 25 Hearing"], Serial No. 108-11 at 26.
- 9 *Id.* at 230.
- 10 *Id.* at 28-30; Testimony of Florida State Senator Paul Dackery, March 25 hearing, *supra* note 8 at 8-9.
- 11 For example, the Electronic Privacy Information Center reported that the Justice Department obtained an \$11,000,000 contract for Choicepoint databases and that the Homeland Security Department

- queries private sector data basis 20,000 times a month. “Hearing on Data Mining: Current Application and Future Possibilities,” EPIC letter, March 25, 2003, March 25 Hearing, *supra* note 8 at 90-91. The Department of Defense proposed the Total Information Awareness program, later renamed the “Terrorist Information Awareness Program,” which was cancelled after opposition to the program made it untenable. See Gina Marie Stevens, *Privacy: Total Information Awareness Programs and Related Access, Collection, and Protection Laws*, Cong. Res. Serv. (Mar. 21, 2003).
- 12 Eric Lichtbleu and James Risen, *supra* note 5. The government denies that it is mining the Swift database and states that its searches of the database are targeted. *Id.*
- 13 Jennifer Granick, *Mass Spying Means Gross Errors*, WIRED, Jan. 18, 2006, available at <http://www.wired.com/news/columns/1,70035-0.html> (last visited June 26, 2006); and Bruce Schneier, *Why Data Mining Won't Stop Terror*, WIRED, March 9, 2006, available at <http://wired.com/news/columns/1,70357-0.html> (last visited June 24, 2006).
- 14 Lowell Burkman, Eric Lichtbleu, Scott Shane, and Don Van Natta, Jr., *Spy Agency Data After Sept. 11 Led FBI to Dead Ends*, NY TIMES, Jan. 17, 2006, A1.
- 15 Daniel J. Solove, *The Digital Person*, 47 (New York University Press 2004).
- 16 *Id.* at 46-47.
- 17 *Id.* at 50-51.
- 18 See, e.g., William Branigan, *NSA Call-Tracking Program Sparks Alarm*, WASH. POST, May 11, 2006, available at <http://www.washingtonpost.com/wp-dyn/content/article/2006/05/11/AR2006051100539.html>, quoting Senators Specter, Leahy, Reid, and Feinstein criticizing the reported call record data mining.
- 19 Eric Lichtblau and James Risen, *Bank Data Sifted*, *supra* note 5, at A10.
- 20 *Hepting v. AT&T Corp.*, No. C-06-0672-VRW (N.D. Ca.).
- 21 *ACLU v. NSA*, No. 2:06-cv-10204-ADT-RSW (E.D. Mich.)
- 22 *Center for Constitutional Rights v. Bush*, 06-cv-313-GE (S.D.N.Y.).

- 23 In addition to challenging the NSA's data mining of call records, the ACLU and CCR cases challenge another aspect of the program, the interception of the content of e-mails and telephone calls with one end in the United States.
- 24 One exception is *Terkel v. AT&T*, 06-C-2837 (N. D. Ill.), which seeks only injunctive relief. *See also Terkel v. AT&T*, 2006 WL 2088202 (N.D. Ill., July 25, 2006).
- 25 Order denying defendants' motion to stay consideration of plaintiffs' motion for partial summary judgment, 2:06-cv-10204 (May 31, 2006).
- 26 The order that includes the questions is available at <http://www.eff.org/legal/cases/att/order620.pdf> (last visited June 26, 2006).
- 27 *Id.*
- 28 Notice of Motion and Motion to Dismiss or, in the Alternative, for Summary Judgment by the United States of America (redacted public version), 14-29, *available at* <http://www.eff.org/legal/cases/att/GovMotiontoDismiss.pdf>, (last visited June 25, 2006).
- 29 Plaintiffs' Opposition to Motion to Dismiss or, In the Alternative, for Summary Judgment by the United States of America based on the State Secrets Privilege (redacted public version), 3-4, and 10-58, *available at* <http://www.eff.org/legal/cases/att/264-SSP-Opp-Mtn-Redacted-Memo.pdf> (last visited June 25, 2006).
- 30 Brief of Amicus Curiae Law Professors In Support of the Plaintiffs' Opposition to Notice of Motion and Motion to Dismiss or, in the alternative, for Summary Judgment by the United States of America, *available at* <http://www.eff.org/legal/cases/att/lawprofamicusmtd.pdf> (last visited June 25, 2006).
- 31 *Id* at 3.
- 32 *Id.*
- 33 United States' Reply in Support of the Assertion of the Military and State secrets privilege in Motion to Dismiss or, in the alternative, for Summary Judgment by the United States, 3-25, *available at* <http://www.eff.org/legal/cases/att/usreply616.pdf> (last visited June 25, 2006).
- 34 John Markoff, *U.S. Pushes For Dismissal of Lawsuit Against AT&T*,

- N.Y. TIMES, June 24, 2006, A8.
- 35 *Hepting v. AT&T*, 2006 WL 2038464 (N.D. Ca., July 20, 2006).
- 36 The other three “added cases” were *Al-Haramain Islamic Foundation v. Bush*, 06-cv-00274-KI (D. Or.); *Shubert v. Bush*, 06-cv-02282-FB-MDG (E.D. N.Y.); and *Guzzi v. Bush*, 06-cv-0136-JEC (N.D. Ga.).
- 37 United States Motion and Response, MDL Docket No. 1791, 3.
- 38 See JPML Rule 1.1, and 7.4.
- 39 See JPML Rule 7.4.
- 40 See FISA Annual Reports to Congress 1979-2004, available at <http://www.fas.org/irp/agency/doj/fisa/#rept> (last visited June 26, 2006).
- 41 See generally Classified Information Procedures Act, 18 U.S.C. app. III §1, *et seq.*; and *United States v. Rezaq*, 134 Fd.3d 1121 (D.C. Cir 1998).
- 42 343 U.S. 579 (1952).
- 43 343 U.S. at 630, 645-46 (Jackson, J., concurring).
- 44 343 U.S. at 637-38 (Jackson, J., concurring).
- 45 *Hamdi v. Rumsfeld*, 542 U.S. 507, 536 (plurality opinion).

The employee's response to this seemingly innocuous "AutoArchive" prompt could have a significant impact on the company's ability to comply fully with its discovery obligations in ongoing and future litigation, or may cause an inadvertent violation of the company's own records retention policy. Why? Because by clicking either "Yes" or "No," she may unwittingly be making an inappropriate e-mail storage decision. Certain risks accompany the use of the AutoArchive function included in software on many personal computers, and companies should take steps to eliminate or manage those risks.

WHAT IS AUTOARCHIVE?

The most popular e-mail program in use today in personal computers (PCs) is Microsoft Outlook. Outlook may be used for sending, receiving, and storing e-mails, as well as for multiple other functions, such as maintaining addresses, keeping calendars and schedules, and tracking tasks. Microsoft has built into its Outlook program a function that it calls "AutoArchive." So, when one uses Outlook, one gets the AutoArchive function along with it. While the AutoArchive function can be "turned off," the ordinary default setting is "on."

WHAT DOES AUTOARCHIVE DO?

The primary function of AutoArchive, as the prompt itself advertises, is to improve performance by saving space. In an organization where many PCs are tied together to form a network, e-mails are typically stored not on the hard drives contained within each individual user's PC, but, rather, on a general network server, sometimes referred to as an "Information Store."¹ As one might expect, especially in a large organization using many PCs, the Information Store may become overloaded with data, which impedes and slows the retrieval of information, and generally lessens the performance of the e-mail system. AutoArchive, as set up within Outlook by Microsoft, runs automatically at scheduled intervals, offering the user the prompt shown above. By selecting "Yes," the user moves certain e-mails to a selected hard drive, often on the user's own PC. The e-mails that are moved vary,² but might include, for instance, e-mails

in the user's Inbox and Sent Items that are more than a certain number of days old. Once moved by virtue of the AutoArchive function, these e-mails are no longer stored on the Information Store, thereby lessening the burden on the Information Store and, theoretically at least, enhancing performance of the organization's e-mail system. If the user selects "No" on the AutoArchive prompt, then his or her e-mails remain exactly where they had been residing, on the Information Store.

Unfortunately, many PC users do not know what the AutoArchive function is, what it is intended to do, nor whether, in the particular user's circumstance, AutoArchive is a good thing or a bad thing. Many users, when receiving the AutoArchive prompt, click "Yes," without knowing the specific consequences of that choice. Many others, operating from the same lack of knowledge, click "No." Worse yet, even in world class Fortune 500 companies, some of the Information Systems personnel may not fully understand the AutoArchive function. This article discusses the impact of AutoArchiving, particularly as it relates to records management and e-discovery issues.³

THE "YES" RISK

When a user clicks on "Yes" after receiving the AutoArchive prompt, a subset of the user's e-mails and other information stored in Outlook will be moved from the Information Store to, in most cases, the hard drive on his or her individual PC, often referred to as the "C: drive."⁴ While moving e-mails to the C: drive arguably places the e-mails more comfortably in control of the user (because the e-mails are now located in the user's office, on the PC sitting on his or her desk), he or she has created certain risks by this action:

First, e-mails stored on the Information Store typically are backed up for disaster recovery purposes. E-mails stored on C: drives are less likely to be backed up. Therefore, if a computer virus infected the computer system and C: drive, or if a fire or other disaster physically destroyed the computer system and C: drive, then e-mails that had been stored on the Information Store before the virus or disaster could be recovered from the backup media.⁵ Any e-mails moved to the C: drive after the date of the last retained backup likely would be lost.

Second, unless the user is familiar with the AutoArchive function, he or she may not even be aware that, by clicking “Yes,” he or she has moved e-mails to the C: drive. If at a later time the user wants or needs to retrieve a particular e-mail and cannot find it in Outlook, the user may assume incorrectly that he or she previously deleted the e-mail and may discontinue the search. E-mails stored in AutoArchive on a user’s C: drive are not identified or listed anywhere on the user’s Outlook screen or PC “desktop” page. One finds AutoArchived e-mails only if one knows he or she has them, and knows where and how to look for them. AutoArchived information is typically “buried” about seven levels deep on a C: drive, and can be obtained only by executing a series of steps and/or clicks.⁶

Third, if a user is unaware that he or she has moved electronically stored information into the C: drive by clicking “Yes” to the AutoArchive prompt, then, when the user’s employer becomes subject to a subpoena or to discovery requests in litigation, the user will not know to search his or her AutoArchived information for potentially responsive evidence. The organization’s IS personnel also may not be aware that the user has moved certain information into the C: drive and, to the extent that the IS or IT department is assisting in responding to the subpoena or discovery request, it too may fail to identify potentially responsive evidence in the C: drive. Such failures to locate and produce potentially relevant evidence, when ultimately discovered, can lead to the imposition of increasingly substantial sanctions by courts.⁷

Fourth, many organizations have sound, detailed records management policies, clearly delineating how long records should be retained. Substantial cost savings can flow from implementation of a records management program that encourages disposal of records that are no longer needed for business reasons or legal compliance. Not only are storage expenses reduced, but retrieval of records that must be retained is easier and less costly when not impeded by the retention of records that should have been deleted when they reached the end of their retention period. By clicking “Yes” to the AutoArchive prompt, a user unknowingly may be archiving and retaining records that, pursuant to the organization’s own records management policy, should not be retained.

It should be noted that, if the AutoArchive prompt pops up while the user is keyboarding an e-mail, then a keystroke on the letter “y,” or on the “Enter” key, or possibly on other keys, in some systems has been interpreted by the computer as a click on “Yes,” causing the AutoArchive prompt to disappear and resulting in the user having unintentionally and unknowingly AutoArchived certain information.

THE “NO” RISK

The risk associated with clicking “No” to the AutoArchive prompt is the potential unknowing deletion of electronically stored information. When a user clicks on “No” after receiving the AutoArchive prompt, his or her e-mails and other information stored in Outlook will remain in Outlook. Many e-mail systems automatically delete e-mails after a certain number of days. If a user’s e-mail system is set up for such automatic deletions, and if the user is not aware of that fact, then, by clicking on “No” and allowing the e-mails to remain in the Outlook mail boxes, the user may be unknowingly allowing e-mails to be deleted that should be retained pursuant to a record retention policy or a litigation hold.

CONCLUSION

In a large organization, with hundreds or thousands of users on a PC network, the AutoArchive function, if it is activated on the network but users are not educated about it, can result in the inadvertent and unknowing archiving of very large quantities of e-mails and other electronically stored information. If a subpoena or discovery request is served upon the organization, and it is aware of the existence of the AutoArchives, the costs of searching and processing this quantity of extra data can be substantial. If the company is not aware of the existence of such “buried” information, the costs can be even more devastating because, when discovered, the failure promptly to have produced the information can lead to substantial sanctions by a court or investigating agency.

As with any aspect of an electronic information system, education of its users is imperative, as is auditing of its functions.

To reduce the risks associated with the AutoArchive function, an

organization should either (i) “turn off” the function in its system, and make sure that it remains turned off as PCs are replaced or reconfigured; and/or (ii) establish a sound user education program, and conduct regular audits of the information being AutoArchived.

To paraphrase a wise Latin warning, “Caveat prompctor.” (Loosely translated: Let the user beware of prompts.)

NOTES

- 1 A “server” is generally a network computer used to store data or software for multiple users on the network.
- 2 The AutoArchive function allows users to choose in advance which e-mails are to be moved when “Yes” is selected on the AutoArchive prompt. Absent a specific selection by the user of the e-mails to be AutoArchived, the AutoArchive function will apply varying “default” criteria.
- 3 “E-discovery” is a term that refers broadly to requests made in litigation or investigations (including subpoenas, deposition notices, interrogatories, document requests, etc.) for electronically stored information, including e-mails and other electronic records or data.
- 4 A knowledgeable user can modify the default settings on the AutoArchive so that AutoArchived information is sent to a hard drive other than the C: drive.
- 5 Backup media are used to copy, usually on at least a daily and weekly basis, the data on the Information Store and keep it at a location separate from the computer system so that it can be used to recover information in the event of a disaster that impacts the computer system.
- 6 To identify and retrieve information stored in the AutoArchive folder on a C: drive, a user could (i) double-click on “My Computer” on his or her desktop, (ii) double-click on “Local Disk (C:),” (iii) double-click on “Documents and Settings,” (iv) double-click on her username, (v) double-click on “Local Settings” (vi) double-click on “Application Data,” (vi) double-click on “Microsoft,” and then (vii) double-click on “Outlook.”

- 7 For example, in *Coleman Holdings, Inc. v. Morgan Stanley & Co.*, No. CA 03 5045 (15th Jud. Cir., Palm Beach Cty., Fla.) (May 16, 2005), based on the defendant's failure to timely produce responsive electronically stored information, the court precluded the defendant from raising certain defenses and the jury ultimately awarded to the plaintiff \$600 million in compensatory damages and \$850 million in punitive damages.

California Court Blocks Subpoenas Aimed at Bloggers' Source of Trade Secret Information

PATRICK E. PREMO AND GAURAV MATHUR

A recent court ruling has substantial implications for trade secret owners trying to protect their proprietary and confidential information.

On May 26, 2006, the California Court of Appeals, Sixth District, issued a unanimous decision striking down subpoenas to Internet “news” sites seeking the source of leaked trade secret information.¹

The 69-page opinion, which was certified for publication, is significant because it extends the same constitutional protections to online “news” reporters, editors and publishers, including amateur bloggers, that have traditionally been reserved to print publications, such as newspapers, magazines, radio and television broadcasters. In so doing, the court dealt a blow to efforts by trade secret owners to protect proprietary and confidential information. The court did not view this simply as a trade secrets case:

“[t]his case involves not a purely private theft of secrets of venal advantage, but a journalistic disclosure to, in the trial court’s words, ‘an interested public.’ In such a setting, whatever is given to trade secrets law is taken away from the freedom of speech...it seems plain that where

Patrick E. Premo is a partner in the Litigation and Electronic Information Management Groups of Fenwick & West LLP. Gaurav Mathur is an associate with the firm. The authors can be reached at ppremo@fenwick.com and gmathur@fenwick.com, respectively.

both cannot be accommodated, it is the statutory quasi-property right that must give way, not the deeply rooted constitutional right to share and acquire information.”

The decision demonstrates the importance of strictly enforcing and auditing compliance with company policies, practices and procedures to guard against the unauthorized disclosure of confidential and trade secret information. It also shows the need to review current policies to ensure that they adequately deal with the unique dangers presented by the proliferation of electronic information and the ease of disclosure over the Internet. Finally, the opinion highlights the need for trade secret owners to conduct an extremely thorough internal computer forensics analysis as a precondition, or indeed alternative, to civil discovery.

CASE BACKGROUND

Apple Computer, Inc. brought an action in California Superior Court alleging that unknown persons caused the wrongful publication of Apple’s trade secret product information related to a device code-named “Asteroid” or “Q97.” Asteroid was an add-on device that would allow users to plug musical instruments into Apple computers and create digital audio recordings. Two Internet “news” sites devoted to Apple products posted verbatim excerpts of technical specifications and a reproduction of a copyrighted rendering of the product design.

Suspecting that some of its own employees had disclosed the alleged trade secrets to these Web sites, Apple conducted an internal investigation led by its corporate security department to determine the source of the leak. The investigation led Apple to believe that the documentary source of the leak was a particular set of electronic slides. However, the identity of persons responsible for the leak remained a mystery, despite interviews of approximately 29 employees and forensic searches of Apple’s e-mail servers for communications regarding the disclosed product information. In an effort to identify the source of the leak, Apple sought and obtained authority to issue civil subpoenas to the operators of the two Web sites where the information appeared and to the e-mail service provider for one of the publishers. Nfox, the e-mail service provider, later confirmed that it

in fact had in its possession copies of e-mails sent to the Web site operator about Asteroid. The operators of the Web sites sought a protective order to prevent Nfox from handing over any e-mail records to Apple.

APPELLATE COURT'S DECISION

The appellate court issued a writ of mandate directing the trial court to grant the motion for protective order for the following reasons.

- (1) The subpoenas violated the federal Stored Communications Act because they sought the content of private e-mail communications;²
- (2) The bloggers that operated the Internet "news" sites were entitled to protect their confidential sources and unpublished information under California's reporter's shield in the same manner as printed news publications;³ and
- (3) The Internet "news" site operators could invoke the qualified reporter's privilege under state and federal constitutional guarantees of a free press, which the Company failed to make a sufficient showing to overcome.⁴

FEDERAL STORED COMMUNICATIONS ACT

The court initially held that the subpoenas for e-mails sent to the third party Web sites were unenforceable under the federal Stored Communications Act (SCA).⁵ The SCA prevents an electronic communications service provider from knowingly disclosing the content of an e-mail stored by the service provider. The court rejected Apple's primary argument that there was an implied exception under the Act permitting the limited civil discovery at issue. The Act aims to encourage innovative forms of communications, like e-mail, by granting them the same protections from unwanted disclosure as the more traditional means.

The court distinguished this case from so called "John Doe" lawsuits in which litigants are permitted to subpoena Internet service providers to

obtain the identities of subscribers who posted anonymous defamatory messages on Web sites. Here, the source of the leaked information did not post the information directly himself or herself, but rather provided the information to the operators of the blog, who in turn made the disclosure. The specific content of the e-mails being subpoenaed therefore remained private and protected from disclosure under the Act.

CALIFORNIA REPORTER'S SHIELD

The court next determined that the operators of the Internet “news” sites qualified under California constitutional protections afforded to traditional media. The California reporter’s shield provides an “absolute protection to nonparty journalists in civil litigation from being compelled to disclose their information sources or any unpublished information obtained in the course of gathering information.” The court refused to set forth any test or principle for drawing a line between “legitimate” versus “illegitimate” journalism. The court held that the shield laws are intended to protect the gathering and dissemination of news and that is exactly what the Web site operators did in this case. The sole purpose of the Web sites was to provide its readers with information and news about a particular type of information. The fact that the Web sites simply reprinted “verbatim copies” of Apple’s internal information instead of distilling or editing the information in any way did not justify a denial of the reporter’s shield protection.

The court also held that operators of news oriented Web sites fall within the ambit of “publishers” and thus the reporter’s shield extends to such Web site operators. Finally, the court determined that digital media sources like Web sites are equivalent to newspapers and magazines and thus covered by the law. The court reasoned that the shield is intended to protect the gathering of news for dissemination to the public. Limiting this shield only to traditional print media would not advance this basic purpose of the law. Indeed, the law explicitly covers two non-print sources of news: television and radio. However, the court did indicate that the shield likely does not cover non-recurring publications such as books, pamphlets, or flyers.

QUALIFIED REPORTER'S PRIVILEGE

Finally, the court determined that the operators of the Internet user sites could invoke a qualified constitutional privilege, which protects news reporters, editors, or publishers from compelled disclosure of the identities of confidential sources and unpublished information supplied by such sources. Such reporter's privilege is lost where there is a need sufficient to outweigh the inhibitory effect of such disclosure upon the free flow of ideas and information.⁶ The court balanced the following five factors and concluded that the reporter's privilege was not overcome in this case:

- i. "Nature of litigation and whether reporter is a party." The need for information outweighs the rationale for free press privilege where the reporter or publisher is a party to the litigation. Compelled disclosure is particularly appropriate in a libel action against a reporter. Since Apple had not named the Web site operators as defendants in its trade secret action, the court held that this factor weighed against compelled disclosure. The court was not persuaded by the fact that the petitioners might be named as defendants in the pending trade secrets suit.
- ii. "Relevance of information sought." The court held that this factor favored disclosure because the identity of the misappropriator goes to the heart of a trade secret misappropriation claim. Such information was critical to Apple's case. The court, however, reduced the weight given to this factor because there was no guarantee that Apple would learn the identity of the misappropriator even if it obtained the discovery it sought. Apple's trade secrets could have been disclosed to the Web sites anonymously.
- iii. "Exhaustion of alternative sources." Compelled disclosure of sources requires a showing that there are no other practical means of obtaining the information. Such disclosures are considered by the courts as a "last resort." This factor was consid-

ered dispositive in the court's decision not to compel disclosure. In concluding that Apple's investigatory efforts to identify the misappropriators were lacking, the court held that "Apple has failed to establish that there is any information that it cannot obtain by means other than the present discovery." Although Apple questioned employees who were known to have access to the documentary source of the leak, the court complained that none of the Apple employees were deposed or questioned under oath. The court also felt that the Company should have followed up with two individuals who were known to have contributed to the drawings in the challenged articles. Finally, the court also focused on the absence of any investigation of how the source files were subsequently processed and handled by the individuals who initially had access to them. Overall, the court thought there was a failure to fully exploit "internal computer forensics."

- iv. "Importance of preserving confidentiality." The importance of preserving confidentiality of a reporter's sources is high when the information relates to matters of great public importance and when the risk of harm to the source is a substantial one. While the court recognized Apple's obvious interest in protecting its own trade secrets, it reasoned that such a "quasi-property" right must give way to the constitutional right of free speech. The court noted that "[t]he newsworthiness of petitioner's articles thus resided not in any technical disclosures about the product but in the fact that Apple was planning to release such a product, thereby moving into the market for home recording hardware."

The court appears to have been influenced by its doubt as to whether the information at issue was truly a trade secret. The court openly questioned "[w]hether or not confidential marketing plans constitute trade secrets under the governing statutory language." The court also gave less deference to a trade secret relating to a plan to release a product as opposed to a trade secret relating to how the product was made.

- v. “Prima facie case.” The *prima facie* case factor relates to the demonstrated strength of the plaintiff’s case on the merits. The court held that this factor weighed in favor of disclosure because it was reasonable to infer that someone had violated their duty of confidentiality owed to Apple and that the information leaked to the Web sites was a trade secret.

IMPACT OF DECISION ON TRADE SECRETS PROTECTION

This decision has substantial implications for trade secret owners trying to protect their proprietary and confidential information. The appellate court has made it extremely difficult to obtain discovery against third party Internet “news” providers that have published the trade secret information. Thus, it is imperative for trade secret owners to institute and adhere to strict internal controls to prevent such disclosures in the first place. They should also review current policies to ensure they adequately address the proliferation of electronic information and the ease of its transmission.

This decision also highlights the increasingly important role of computer forensics to determine the source of the leaked information. Computer forensics, which often includes review of firewall logs, e-mail servers and any Web or instant messaging monitoring devices, can be far less disruptive than the interrogations under oath of company employees proposed by the court in its opinion. Oftentimes, it is also far more effective at isolating the source of the disclosure.

NOTES

- 1 See *O’Grady et al. v. The Superior Court of Santa Clara County*, Case No. H028579 (Cal. App. May 26, 2006).
- 2 18 U.S.C. §§ 2701-2712.
- 3 Cal. Const. Art I, § 2(b), Cal. Evid. C. § 1070.
- 4 U.S. Const. Amend. I; Cal. Const. Art I, § 2(a).
- 5 18 U.S.C. §§ 2701-2712.
- 6 See *Mitchell v. Superior Court*, 37 Cal.3d 268 (1984).