THE USA-PATRIOT ACT

Jonathan Band
Charles Kennedy
Morrison & Foerster, LLP

On October 26, 2001, President Bush signed into law the Uniting and Strengthening America By Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 (the "Act"), which is designed to deter and punish terrorist acts in the United States and around the world. This article summarizes the Act's provisions concerning electronic surveillance and computer fraud.

I. Overview

The Act responds to the September 11 terrorist attacks by enabling law enforcement and intelligence agencies to work together more closely and by updating criminal investigative procedures to account for 21st century communications such as e-mails and the Internet. It authorizes the sharing of information for criminal investigators at the federal, state and local levels, and investigators who are gathering intelligence overseas. It provides for enhanced wiretap and surveillance authority, strengthens border controls, and broadens penalties, including life in prison, for terrorist activities.

The Act aims to crack down on money laundering by targeting the way terrorists move money such as bulk cash smuggling, international wire transfers, and informal black market brokers known as "hawalas." It establishes a system to identify, report, and disrupt money laundering activities and gives the Treasury Secretary the power to block transfers of funds to the United States from foreign banking systems used by, or likely to be used by, terrorists and criminal organizations because those foreign jurisdictions have weak or nonexistent anti-money laundering regimes.

Many parts of the Act had been under consideration for some time but could not be enacted because of concerns about unwarranted government intrusions and erosions of civil liberties. Even in the aftermath of September 11, lawmakers agreed to sunset several of the Act's provisions after four years, permitting Congress to revisit these contentious issues.

Because of the complexity and broad scope of the Act, this memorandum addresses only the two parts of the Act of greatest interest to the information technology industry: the enhanced surveillance procedures of Title II; and the amendments to the Computer Fraud and Abuse Act in Tit le VIII.[1]

II. Title II: Enhanced Surveillance Procedures

[1] A memorandum that discusses the Act's money laundering provisions can be found at http://www.mofo.com/news/general.cfm?concentrationID=5&ID=600&Type=5.

In the wake of the terrorist attacks on September 11, federal law enforcement authorities asked Congress for substantial new authority to monitor electronic communications and obtain access to stored voice messages, e-mails and customer records. Congress responded quickly to these requests, and the Act significantly changes the rules that communications companies and their customers must follow when confronted with electronic surveillance and access demands.[2] The principal new provisions are:

1. Right to Disclose Subscriber Information. Service providers sometimes are confronted with law enforcement requests for subscriber information that are not accompanied by a warrant, subpoena or other process. Until now, the Electronic Communications Privacy (the "ECPA"), 18 U.S.C. § 2703 *et seq*., has prevented compliance with such requests. Under section 212 of the Act, a service provider may (but is not required to) disclose subscriber information to law enforcement agencies where the service provider "reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay."

Service providers also have had no right under the ECPA to disclose customer records even where necessary to render service or protect the rights or property of the service providers. (Oddly enough, the ECPA has permitted service providers to disclose the *contents* of customer communications when necessary to protect service providers' rights or property.) The Act permits service providers to disclose customer records to anyone where necessary to protect the service providers' rights or property. Service providers should develop appropriate procedures to respond to requests for voluntary disclosure. They may also need to modify their privacy policies to reflect that they might disclose this information to law enforcement authorities.

Section 210 of the Act authorizes the nationwide service of subpoenas for subscriber information and expands the list of items subject to subpoena. Specifically, subscriber information subject to subpoena now includes "records of session times and durations," as well as "any temporarily assigned network address." In the Internet context, such records include the Internet Protocol address assigned by the provider to the customer or subscriber for a particular session as well as the remote IP address from which a customer connects to the provider. Investigators also may use a subpoena to obtain the "means and source of payment" that a customer uses to pay a communications provider account, "including any credit card or bank account number." Law enforcement officials expect this information to be valuable in identifying users of Internet services where a company does not verify its users' biographical information.

2. Business Records Under the Foreign Intelligence and Surveillance Act ("FISA"). Section 215 would remove the "agent of a foreign power" standard for court-ordered access to certain business records under Sections 501 through 503 of FISA, 50 U.S.C. §1861, and would expand the scope of court orders by inserting a new Section 501 to include access to other records and tangible items, such as books, documents, and papers. Authority granted under this section may be used for an investigation to protect against international terrorism or clandestine

[2] The United States Government recently signed the new Council of Europe Cybercrime Convention. Ratification may require further changes to federal criminal law and procedure.

intelligence activities or to obtain foreign intelligence information on non-U.S. persons. This provision marks an improvement over the original legislation that contained broad permission for the U.S. Attorney General to obtain copies of educational records without a court order. In contrast, the Act requires a court order and a certification by the Attorney General that he has reason to believe that the records contain information that is relevant to an investigation of terrorism.

3. Pen Register/Trap and Trace Authority. The Act substantially enlarges the ability of law enforcement to install so-called "pen register" and "trap and trace" devices. These are devices and functionalities that record telephone numbers and e-mail routing and addressing information. Pen registers record the numbers and routing information of calls sent *from* a telephone or computer; trap and trace devices record the telephone numbers and routing information of calls and messages sent *to* a telephone or computer.

Pen registers and trap and trace devices have become more controversial in recent years. Notably, some Internet service providers questioned whether existing law permitted the use of those devices to capture routing information for e-mail and other computer communications. Also, the Federal Government's use of "Carnivore" technology to monitor computer communications has aroused the concern of Internet and civil liberties groups.

Section 216 of the Act confirms that pen register orders and trap and trace orders apply to computer communications as well as traditional telephone service. The Act also makes clear, however, that these orders authorize only the capture of routing and addressing information and may not be used to intercept the contents of communications, which still may be acquired only by the more rigorous process of obtaining an interception order. The Act also requires law enforcement to report to a court on every use of Carnivore-type technology and requires the government to use reasonably available technology that limits interceptions "so as not to include the contents of any wire or electronic communications."

The Act also provides, in section 222, for compensation to service providers (as well as landlords, custodians and other persons) who furnish facilities and technical assistance in support of pen register/trap and trace orders. The Act also states that service providers are not required to design or modify their networks, along the lines required in other contexts by the Communications Assistance for Law Enforcement Act (the "CALEA"), in order to comply with pen register/trap and trace orders.

Finally, the new Act simplifies law enforcement's task in obtaining and executing pen register/trap and trace orders by permitting federal officials to obtain a single order that may be enforced anywhere in the country. This departs from the former law, which required federal officials to apply for a new pen register/trap and trace order in every jurisdiction where a target telephone or other device was located.

4. Roving Wiretaps and Nationwide Search Warrants. Section 206 of the Act authorizes the use of roving wiretaps in the course of foreign intelligence investigations and brings the FISA in line with criminal procedures in the ECPA which already allow surveillance to

follow a person who uses various communications devices or locations. This authority departs from current law, which requires a separate court order identifying each telephone company or other communications provider whose assistance is required. The change recognizes the ease with which targets of potential investigations change phones to evade current surveillance techniques. Under the Act, the court order need not specify a particular communications carrier where the court finds that the actions of the person whose communications are to be intercepted could have the effect of thwarting the identification of a specified facility or place. The Act also extends the duration of the FISA surveillance of an agent of a foreign power, other than a U.S. person, from 90 days to 120 days, and expands the period for extensions from 90 days to one year. The Act also extends the usual period for physical searches under the FISA from the present 45 days to 90 days.

5. Obtaining Voice Mail and Other Stored Voice Communications. Several of the Act's provisions broaden the scope of the Government's ability to search for and seize stored communications, such as voice mail and e-mail messages. *See* section 209. Under previous law, the ECPA permitted law enforcement to access stored non-voice communications, such as e-mail, with an ordinary warrant, but did not permit access to stored *wire* communications, such as voice mail, unless the government met the stronger requirements for an interception (*i.e.*, wiretap) order.

Section 211 of the Act subjects law enforcement access to cable subscriber records to the same rules as access to other electronic records by amending the Cable Communications Policy Act to clarify that the ECPA, the wiretap statute, and the trap and trace statute govern disclosures by cable companies that relate to the provision of communications services, such as telephone and Internet services. The changes would, however, preserve the Cable Act's primacy with respect to records revealing what ordinary cable television programming activity a subscriber chooses, such as "pay per view" shows.

Section 220 of the Act also authorizes courts with jurisdiction over an offense to issue search warrants for electronic communications in electronic storage anywhere in the country, without requiring the intervention of judges in districts where Internet service providers are located.

6. Expansion of Surveillance Authority To Terrorist Acts. Sections 201 and 202 of the Act expands the list of crimes that may be used as predicates for wiretaps to include certain offenses that focus on terrorist threats. In addition to crimes that relate directly to terrorism and the use of chemical weapons, the list would include felony violations of the Computer Fraud and Abuse Act that are committed by terrorists to support and advance illegal objectives.

7. Intercepting Computer Trespasser Communications. Under section 217 of the Act, computer service providers who are victims of attacks by computer trespassers are authorized to permit law enforcement officials to monitor trespassers on their computers in certain cases. A computer trespasser is defined as a person who accesses a computer without authorization and, thus, has no reasonable expectation of privacy in any transmitted communications. A computer trespasser does not include a person known to the computer

service provider or who has a contractual relationship with the owner or operator. A computer service provider could include a company that provides Internet access to its employees or that operates a website.

In some instances, law enforcement authorities may inform the computer service provider that its computers are being trespassed, and request the provider to permit it to monitor the trespasser. Because of the scope and complexity of the anti-terrorism surveillance measure and the absence of a "Good Samaritan Clause" limiting service providers' liability for good faith interceptions under section 217, firms need to develop procedures for handling such requests. They also may need to modify their privacy policies to inform subscribers that they may permit such interceptions. They should consider seeking the assistance of counsel before responding to requests for access to customer communications or records.

8. Sunset Provisions. The Act provides a four-year sunset, on December 31, 2005, for many of the provisions of Title II. Certain authorities granted under Title II could be "grandfathered" for pending investigations of offenses that occurred prior to the sunset. The sunset provision does not apply to certain provisions of Title II, such as: (1) authority to share grand jury information with intelligence agencies under section 203(a); (2) the so-called "sneak and peak" authority for surreptitious search and seizure provided by section 213; (3) the expanded scope of subpoenas for records of communications provided by section 210; and (4) new authority for pen registers and trap and trace devices in criminal investigations provided by section 216.

III. Section 814: Deterrence and Prevention of Cyberterrorism

The Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (the "CFAA"), is the primary federal statute prohibiting computer fraud and hacking. Originally passed in 1984, the CFAA has been expanded repeatedly as federal prosecutors have confronted new forms of cybercrime.

The Act continues this trend. It broadens the CFAA's definition of a "protected computer" to include computers used in interstate or foreign commerce that are physically located outside of the United States. Given the global nature of computer networks, computer hackers within the United States may attack systems located entirely outside the United States. Alternatively, hackers in foreign countries may route communications through systems located within the United States, even as they hack from one foreign country to another. This amendment will make it possible for U.S. law enforcement to assist in the investigations or prosecutions of international hacking cases.

The Act eliminates the current directive to the Sentencing Commission requiring that all violations, including misdemeanor violations, of certain provisions of the CFAA be punished with a minimum term of six months' imprisonment. This change will provide more latitude to government officials in imposing punishments, other than imprisonment, that might provide adequate punishment and deterrence.

Some of the Act's amendments directed at the CFAA's criminal provisions necessitated other changes to preserve the s*tatus quo* with respect to private civil actions brought under the CFAA. Because of ambiguities in the statute relating to civil actions, this effort to preserve the *status quo* required codification of the better reasoned judicial interpretations of the CFAA. These amendments should bring greater consistency and certainty to CFAA actions, and reduce its use in class action litigation.

A(1): The $5,000 Threshold Prior to the USA PATRIOT Act

Although the CFAA was enacted to deal with cybercrime, the broad wording of its provisions has allowed plaintiffs' attorneys to use it in a wide range of computer and Internet torts, including class actions relating to the implanting of "cookies" and the installation of allegedly defective software. What has helped limit the abuse of the CFAA is a $5,000 loss threshold for bringing a private action.

Section 1030(g) of title 18 provides that "any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." Prior to the USA PATRIOT Act, Section 1030(e)(8) defined "damage" as "any impairment to the integrity or availability of data, a program, a system, or information, that ... causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals." Most of the CFAA's violations require a showing of damage. A private cause of action for any of these violations, therefore, could be brought only if there was an impairment which caused $5,000 of loss, in accordance with the definition of "damage."

However, some of the CFAA's violations do not involve "damage." For example, 1030(a)(2)(c) prohibits exceeding authorized access and thereby obtaining information. No showing of damage is required. The question, then, was whether the $5,000 threshold could be avoided by bringing the private action under the "loss" prong of Section 1030(g)'s "damage or loss" formulation.

The court in *In Re DoubleClick Inc. Privacy Litigation*, 154 F.Supp.2d 497 (S.D.N.Y. 2001), answered this question in the negative. The court observed that "Sections 1030(g) and 1030(e)(8)(A)'s language concerning 'loss' is plainly inconsistent." 154 F. Supp.2d at 520. Finding "facial contradictions" in the statute, the court carefully reviewed the provision's legislative history and the rulings of earlier courts. It ultimately concluded that all "injuries, whether described as 'damage' or 'loss,' are subject to Section 1030(e)(8)(A)'s $5,000 threshold." *Id.* at 523. Other courts agree with *DoubleClick*'s analysis. *See, e.g., Chance v. Avenue A., Inc.*, No. C00-1464C, 2001 WL 1172770 (W.D. Wash. Sept. 14, 2001).

A(2): The $5,000 Threshold under the USA PATRIOT Act

When Senator Leahy introduced his anti-terrorism bill as S. 1510 on October 4, 2001, it contained amendments of the CFAA reportedly intended to facilitate criminal prosecutions by the Justice Department. There was no intent to change private causes of actions under the CFAA.

While retaining the basic definition of damage as "any impairment to the integrity or availability of data, a program, a system, or information," S. 1510 moved the $5,000 loss threshold to a new subsection (a)(5)(B). It then added the following sentence to subsection (g) concerning private causes of action: "A suit for a violation of subsection (a)(5) may be brought only if the conduct involves one of the factors enumerated in subsection (a)(5)(B)." The unintended affect of these two changes taken together was to eliminate the existing threshold of $5,000 of loss for violations of subsections other than (a)(5).

Fortunately, the USA PATRIOT Act ultimately passed by Congress corrected this problem. The new sentence in 1030(g) now provides "A civil action for a violation of *this section* may be brought only if the conduct involves 1 of the factors set forth in ... subsection (a)(5)(B)." (Emphasis supplied.) By replacing "subsection (a)(5)" with "this section," the USA PATRIOT Act ensures that the $5,000 threshold applies to all CFAA violations, not just violations of subsection (a)(5).[3] This correction to S. 1510 in essence codified *DoubleClick*'s interpretation of 1030(g), thereby eliminating the "facial contradiction" concerning the $5,000 threshold, and rendering the CFAA more understandable and predictable.

B: Impairment and Loss

Prior to the USA-PATRIOT Act, the "damage or loss" formulation of 1030(g) caused another significant uncertainty with respect to violations, such as (a)(2)(C), which did not specifically require a showing of "damage:" whether a plaintiff had to show an "impairment" to its system before it could bring a civil action.. As discussed above, "damage" was defined in (e)(8)(A) as "any impairment to the integrity or availability of data, a program, a system, or information, that ....causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals." Since plaintiffs had to show $5,000 of loss, did they also have to show "impairment" to their systems? In other words, to bring a private action, did a plaintiff have to show all the elements of damage in (e)(8)(A), even though the violation itself did not refer to damage? Did the word "loss" in 1030(g) "damage or loss" formulation have no significance whatsoever?

The USA PATRIOT Act eliminated this uncertainty through the interaction between the new sentence in 1030(g) and the new (a)(5)(A)(i), which speaks of a $5,000 loss, but makes no mention of either damage or impairment. Now, a civil action unquestionably can be brought so long as the unlawful conduct causes a $5,000 loss; no showing of any impairment whatsoever is required. The USA PATRIOT further eliminates uncertainty by providing for the first time a definition of "loss" in new 1030(e)(11): "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."

[3] The only exceptions to the $5,000 threshold are conduct involving: impairment of medical records or treatment; physical injury; threats to public health; and damage to a computer used by a government entity.

The use of the word "reasonable" in the phrase "any reasonable cost" is significant. Clearly, Congress did not want a company's over-reaction to a minor violation to enable the company to overcome the $5,000 loss threshold. A company's response would have to be proportionate to the single act violating the statute.

C(1): Aggregation Prior to the USA PATRIOT ACT

Section 1030(e)(8)(A) permitted aggregation of losses "during any 1-year period to one or more individuals" to arrive at the $5,000 threshold. Prior to the enactment of the USA PATRIOT Act, there was some uncertainty concerning what losses could be aggregated. For example, the court in *In re America Online, Inc. Version 5.0 Software Litigation*, No. 00-1341, 2001 U.S. Dist. LEXIS 6595 (S.D. Fla., April 19, 2001), aggregated the loss experienced by all the separate computers allegedly harmed by AOL's software. In contrast, the *DoubleClick* court aggregated only the losses resulting from a single act to a single computer. It reached this conclusion based on close textual analysis of the statute. *See also Thurmond v. Compaq Comp. Corp*., No. 99CV711, 2001 WL 1136136 (E.D. Tex. Mar. 15, 2001); *Chance v. Avenue A., supra*.[4] This narrower reading of aggregation appears to have been the majority view prior to the USA PATRIOT Act.

C(2): Aggregation Under the USA PATRIOT Act

S. 1510 as introduced would have overturned the majority view on aggregation. As noted above, S. 1510 moved the $5,000 threshold from (e)(8)(A) to a new subsection (a)(5)(B)(i). Further, S. 1510 added to (a)(5)(B)(i) a parenthetical clause addressing aggregation. The new provision read: "loss to 1 or more persons during any 1-year period *(including loss resulting from a related course of conduct affecting 1 or more other protected computers)* aggregating at least $5,000 in value...." (Emphasis supplied.) The parenthetical clause apparently was inserted at the request of the Justice Department to make it easier to prosecute CFAA offenses. However, the impact of the clause would have been to reject in civil cases the rigorous aggregation approach followed by the *DoubleClick, Thurmond* and *Chance* courts, and instead to impose the overly broad aggregation approach followed by the *AOL* court.

Once again, the USA PATRIOT Act solved a problem unintentionally created by S. 1510 as introduced. The new 1030(a)(5)(B)(i) reads as follows: "loss to 1 or more persons during any 1 year period (*and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only*, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value...." (Emphasis supplied.) This new wording in the parenthetical clause simultaneously has two results. First, it makes clear that in proceedings brought by the U.S. government, courts must follow the liberal *AOL*, multiple act to multiple computer, aggregation approach. Second, it makes equally clear that in all other proceedings, *i.e*., in private causes of action, courts must follow the narrower *DoubleClick/Thurmond/Chance*, single act to a single computer, aggregation approach.[5] Here,

[4] A single act to a single computer could cause loss to more than one person if, for example, a denial of service attack disabled a server which provided Internet access for hundreds of businesses and individuals.

too, the USA PATRIOT Act's amendments eliminated a major source of uncertainty regarding the CFAA.

D: Negligent Design

Prior to the adoption of the USA PATRIOT Act, several courts refused to dismiss complaints alleging CFAA violations arising from the distribution of products which harmed the plaintiffs' computers. In *In re America Online Inc. Version 5.0 Software Litigation*, for example, the plaintiffs claimed that the AOL access software interfered with the access software of other Internet service providers; that it disrupted customers' local area networks; and that it caused instability in the customers' computer systems and applications, leading to system crashes. The court found that the plaintiffs stated a claim for violation of 1030(a)(5)(A): "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer." *See also Shaw v. Toshiba Am. Info. Sys., Inc*., 91 F.Supp. 2d 926 (E.D. Tex. 1999); *North Texas Preventative Imaging, L.L.C. v. Eisenberg*, No. CV96-71, 1996 U.S. Dist. LEXIS 19990 (C.D. Cal. Aug 19, 1996).

In an effort to limit the use of the CFAA in these sorts of "products liability" cases, Congress included in the USA PATRIOT Act the following amendment to 1030(g): "No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware." Thus, in the *AOL* case referenced above, the plaintiffs would have to show that the disruptions caused by the software were intentional, and not merely the result of negligent design.

Arguably, this sentence does nothing more than underscore the existing second clause of (a)(5)(A)(i): "as a result of such conduct, *intentionally* causes damage without authorization, to a protected computer." Likewise, the 1996 Senate Judiciary Committee Report stated that this provision would impose liability on persons "only if they *intend* to cause damage to the computer, not for recklessly or negligently causing damage." S. Rep. 104-357 at 11. The new sentence's emphasis that negligent design could not trigger a private cause of action appears to have been necessitated by decisions such as *AOL*, which implied that "defective design" was actionable under the CFAA. *See AOL* at *10; *see also Shaw* at 931.[6]

The new sentence should not be read to suggest that the mere distribution (as opposed to design or manufacture) of a defective product could trigger CFAA liability. The substantive

[5] The combination of the words "and" and "only" indicate that the multiple act to multiple computer approach applies only in proceedings brought by the U.S. government. This means that in all other proceedings, courts must follow the single act to single computer approach.

[6] These decisions were denials of motions to dismiss for failure to state a claim. In both cases, the defendants properly focused on legal issues, such as whether the sale of a product was a "transmission," and not fact issues, such as the cause of the defect (e.g., negligence or intent to harm the system). Thus, the courts did not specifically rule that negligent design could lead to CFAA liability. However, *dicta* in both decisions could be read to imply that negligent design and manufacture could violate the CFAA.

offense remains "knowingly caus[ing] the transmission of a program ... and as a result of such conduct, intentionally caus[ing] damage...." The distributor could intentionally cause damage only if it distributed the product knowing that it was defective. So long as the distributor did not know that the product was defective, it could not intentionally cause damage, and thus no CFAA liability could attach.

In sum, the USA PATRIOT Act makes several important amendments to the CFAA. These amendments eliminate ambiguities in the underlying statute by codifying well reasoned interpretations of the CFAA, such as those in the *DoubleClick* decision. Taken together, these amendments should provide greater certainty and predictability to CFAA actions, which in the long run should benefit all legitimate players in the Information economy.

IV. Impact of USA PATROIT Act on Civil Liberties

The USA PATRIOT Act has been attacked as a threat to privacy and civil liberties. Although some of those criticisms are exaggerated, certain provisions of the statute clearly result in a lower level of legal protection against governmental surveillance and seizure of stored communications and records.

The relaxation of the procedure for access to stored voice communications, for example, represents a substantial erosion of earlier safeguards. In 1986, when the ECPA was enacted, the Congress made a policy decision that communications containing the human voice warranted especially stringent protection from interception. Notably, ECPA provided that even when a law enforcement agency sought only to obtain an existing tape recording of a conversation, rather than authority to intercept a conversation in progress, the agency still would be required to meet the rigorous requirements for a wiretap order rather than the lesser requirements for a search warrant. Stored e-mails and other stored non-voice communications, however, still were obtainable through service of a warrant.

In the years since ECPA was enacted, civil libertarians have criticized the statute for not extending the highest level of protection to e-mail and other non-voice communications, and have urged amendment of ECPA to require wiretap orders -- rather than mere warrants -- for governmental access to *all* stored communications. The USA PATRIOT Act not only declines to make this change, but takes the opposite approach by downgrading recordings of voice conversations to the level of protection afforded to stored e-mail.

Privacy safeguards also are reduced by the provisions affecting Internet and telephone service provided over cable television networks. Under previous law, cable systems could disclose information concerning their customers' use of the cable providers' services only after giving notice to the customers. Under the new statute, if a law enforcement demand involves information concerning a customer's use of a telephone or Internet service offered by the cable provider (as opposed to the customer's choice of video programming) no notice to the customer will be required before the customer information is disclosed.

The new provisions concerning service providers' voluntary disclosure of customer account information also threaten user privacy. As noted earlier, the 1986 version of ECPA prohibited service providers from disclosing customer information to any governmental agency except pursuant to warrant or other process. The new provisions, which permit a service provider to disclose such information whenever the service provider reasonably believes that such disclosure is necessary to prevent death or serious physical injury, can easily be manipulated by police agencies. So long as a law enforcement representative tells the service provider -- however implausibly -- that disclosure is needed to prevent death or serious injury, the service provider's reliance on that representation will furnish the "reasonable belief" that the statute requires. Under this standard, exaggerated claims of imminent threat may prove to be an attractive substitute for the trouble of obtaining a warrant.

Although the concerns posed by these innovations are substantial, some of the USA PATRIOT provisions that have been the subject of the strongest complaints from civil libertarians do not give investigators unprecedented powers, but merely extend or confirm powers that already are available. For example, roving wiretaps have been available under ECPA for years, but now will be permitted in Foreign Intelligence Surveillance Act ("FISA") investigations as well. Similarly, although USA PATRIOT makes FISA pen register and trap-and-trace orders easier to obtain, the new FISA standard for such orders is not novel but resembles the longstanding requirements for obtaining such orders under ECPA. Also, although USA PATRIOT amends the pen register/trap-and-trace statute in a way that makes it plainly applicable to e-mail as well as telephone conversations, the absence of that amendment did not prevent police agencies from obtaining pen register and trap-and-trace orders on e-mails.

V. Conclusion

As the Act moved swiftly through the Congress, civil liberties groups on the left and conservative political organizations on the right argued that the Act's provisions circumscribed privacy and personal freedoms more than necessary. Congress inserted the sunset provisions in response to these concerns. In four years, Congress will be forced to determine whether it struck the right balance between security and privacy with several parts of the Act. Hopefully Congress at that time will also review the impact of the provisions not subject to the sunset.

Other provisions, such as the amendments to the CFAA, are less controversial. These amendments should eliminate some of the ambiguities which led to abuse of this important statute.

Jonathan Band is a partner in the Washington, D.C. office of Morrison & Foerster LLP and an adjunct professor at the Georgetown University Law Center. He is co-author of *Interfaces On Trial: Intellectual Property and Interoperability in the Global Software Industry*. Mr. Band can be reached at jband@mofo.com.

Charles H. Kennedy is a partner with the Washington, D.C. and Northern Virginia offices of Morrison & Foerster LLP and teaches communications law and computer law at The Catholic

University of America Law School. He also is the author or co-author of four books, including *Modern Communications Law*, a treatise published by West Group. Mr. Kennedy can be reached at ckennedy@mofo.com.