October 2, 2003

Your Own Affair, More (VCR) or Less (MP3)
By SETH SCHIESEL

HE Internal Revenue Service is not used to hearing "no."

In 1998, it was investigating Kent Hovind, an evangelist and Internet radio host in Pensacola, Fla., and his wife, Jo Delia. Mr. Hovind said he had not filed a federal tax return since the early 1970's. Naturally, that got the agency's attention.

The I.R.S. was trying to figure out how much money the Hovinds were making by figuring out how much they were spending. The Hovinds were customers of Cox Cable, so the agency asked Cox to turn over the family's account records.

Federal law gives the I.R.S. extremely broad powers to obtain financial information when it is investigating a suspected tax dodge. That is why it rarely hears "no."

Cox said no.

It turns out that consumers' cable-television records enjoy more legal protection than just about any other sort of electronic media or communications records: more than satellite-television records, more than Internet logs, more than telephone records. The Cable Communications Policy Act of 1984 said that before the government could obtain cable television records, it had to go to court to show "clear and convincing evidence" that the subject of the request was reasonably suspected of criminal activity. Moreover, the customer was entitled to a hearing to contest the disclosure.

The I.R.S. took Cox to court, arguing that it was exempt from those requirements. A federal judge disagreed. The I.R.S. ultimately got the information it was after, but only because the judge ruled that it had satisfied the cable act's requirements.

This year, the recording industry has had things a lot easier than the I.R.S. Since July, the music industry's lobbying wing, the Recording Industry Association of America, has obtained the names, addresses, telephone numbers and e-mail addresses of more than 1,000 people around the nation whom the group suspects of Internet music piracy. The group has sued 261 of them so far, and promises that more suits are to come.

The Digital Millennium Copyright Act of 1998 says that copyright holders may issue subpoenas signed only by a court clerk - not a judge - that require Internet providers to turn over personal information about their subscribers. The law does not require the subscribers to be notified. Every major Internet provider except SBC has complied with the record industry's requests.

Between the stringent provisions of the cable law and the relatively wide-open provisions of the digital copyright act, a crazy quilt of laws - a product of decades of ad hoc legislation - govern what your phone company, cable company, Internet service provider or video store may be compelled to tell about you.

"Consumers are almost totally unaware that different modes of communication carry with them different expectations of privacy and have different rules," said Paul Glist, a communications lawyer with Cole, Raywid & Braverman in Washington who has represented major cable-

television companies. "Every line of business has a different set of regulations, and it really is a maze. There are many times when a company comes to me and they just want to do the right thing and they can't figure it out. You might have one law saying you have to disclose certain information to law enforcement and another law saying you can't disclose the information unless other conditions are met."

For instance, federal law says law enforcement agencies may monitor the phone numbers a citizen is dialing, as they are being dialed, after certifying only that the information is "relevant to an ongoing criminal investigation." Under that provision, the person under surveillance need not even be the person suspected of breaking the law. Generally the subject of that surveillance is not notified of the government's action.

By contrast, a separate law says that even when law enforcement agencies obtain a court order to gain access to a consumer's video rental records, the consumer must be notified before those records are turned over.

While the European Commission has recently issued regulations meant to harmonize privacy protections across different electronic media, the provisions protecting electronic privacy in the United States remain a mishmash, reflecting the vagaries of politics and culture at different moments in recent decades.

"This is a historical accident reflecting law's inability to comprehend the convergence of technologies," Susan P. Crawford, a professor at the Cardozo School of Law of Yeshiva University in New York, said in a telephone interview. "We are very slow to understand that one bit is very much like another and that each bit should probably be subject to uniform law. On the other hand, this slowness means there are speed bumps in the way of law enforcement's ability to get access to all possible information."

In fact, in some areas of digital media, consumers' privacy does not appear to be guaranteed by any specific federal laws. For example, while the cable act generally prohibits the disclosure of personal information to outside private parties without the consumer's consent, there appears to be no federal law of any kind that protects the equivalent information from satellite-television companies.

"I am not aware of any federal statutes that specifically cover satellite-television providers," Christopher A. Murphy, a lawyer for DirecTV, the No. 1 satellite-television provider, said in a telephone interview. "There is a patchwork of state statutes out there, but they run a pretty wide gamut."

Definitive numbers are difficult to come by, but executives at several large telecommunications and media companies said that they process hundreds of requests for customers' personal information each year. Since the enactment of the USA Patriot Act of 2001, which essentially removed many of the most stringent privacy protections, including those in the cable act that supported Cox's case with the I.R.S., those demands have increased significantly, they said.

"Let me put it this way: we have five people working full-time in our court order bureau," said Jim Russell, SBC's managing director for asset protection. "It certainly would make our lives a lot easier if all of these privacy rules were in one law."

The evolution of electronic privacy laws in the United States has taken a convoluted path. In 1928, shortly after the initial widespread adoption of the telephone, the Supreme Court essentially

ruled in Olmstead v. United States that law enforcement agencies could engage in unfettered wiretapping because listening in on a telephone conversation did not constitute a search or seizure subject to protection under the Fourth Amendment.

That decision was overturned in 1967, and a year later the Federal Wiretap Act became law. That act, which sets out the legal requirements for wiretapping, established that wiretaps should be an investigative measure of last resort.

For 30 years after the passage of the 1968 wiretap act, the basic framework for privacy in communications and media remained intact even as new laws established different legal privacy frameworks for national security investigations in 1978 and for the cable television industry in 1984. The basic principles of the 1968 wiretap system were extended to electronic data communications in 1986. The furor over the disclosure of Judge Robert Bork's video-rental history prompted a separate law for video-rental records in 1988.

For all the inconsistencies among these various laws, one of the more significant shifts in privacy protection came in 1998 with the Digital Millennium Copyright Act.

To many legal experts, the right that the digital copyright act granted to copyright holders to subpoena personal information about Internet users goes far beyond earlier legal frameworks. Verizon , the big phone company and Internet provider, challenged the subpoena provisions of the law but lost in court. That case is being appealed, and Verizon and other Internet providers are pushing Congress to change the law.

"The recording industry under this statute can get subpoenas that the Justice Department could not have," said Jessica Litman, a law professor at Wayne State University in Detroit and the author of "Digital Copyright" (Prometheus Books, 2001). "It is highly questionable whether Congress would have so lightly done something so constitutionally questionable, which is to subject millions of Americans to subpoenas for their personal information which are not reviewed or reviewable by any court."

The recording industry disagrees vigorously with that characterization. It argues that its expedited subpoena right under the copyright law reduces the load on judges and helps copyright holders and those accused of piracy work out solutions without lawsuits.

"The analogy is similar to a bank robber donning a ski mask to hide their identity as they rob the bank," said Matthew J. Oppenheim, senior vice president for business and legal affairs at the recording industry association. "A guard witnesses the robbery, and the question is: should the guard have the right to pull the mask off of the robber as he is running out of the bank? The answer obviously should be yes."

If the 1998 copyright law appeared to some experts to challenge elements of traditional privacy protection, the Patriot Act altered them wholesale. It superseded the stringent privacy provisions of the cable act, for example, by specifying that in many cases government agencies can use the more relaxed traditional wiretap process to get personal information.

Robin H. Sangston, Cox Communications' chief litigation lawyer, has seen the changes wrought by the Patriot Act firsthand. She oversaw the strategy that won the legal victory against the I.R.S. in Pensacola, and she has seen an explosion in requests for customer information from the government over the last two years.

"The government will take the position that they can now use a subpoena under the wiretap law to get any personal subscriber information except for the video selections," Ms. Sangston said. "We have to respond to a lot more of these requests now, with the USA Patriot Act. I mean a lot more. Obviously we do not want our customers to break the law, but we want to be able to know that the government is not using this information for a fishing expedition. But we are not able to do that because there is no review by a judge."

The range of laws largely reflects Congress's unwillingness to pass comprehensive digital privacy legislation, perhaps because of competing impulses: a fear that greater infringements on privacy could stifle the development of the Internet, for example, whereas broader privacy rights could stifle law enforcement agencies and copyright holders like the recording industry.

To the man in the middle of the Pensacola case, Ken Hovind, it does not seem to matter much. Mr. Hovind said in a telephone interview that he could not recall the case, partly because he has been at loggerheads with the I.R.S. for so long.

There is one bit of personal information he does not hesitate to share. "I haven't filed a tax return in 30 years," he said.

http://nytimes.com/2003/10/02/technology/circuits/02priv.html?pagewanted=1