APPLICATIONS OF THE PRIVACY PROTECTION ACT

Mark Eckenwiler, Esq.

What I would like to talk about today is not purely an issue of constitutional law. It's neither a federal statute, but the reason I think that it's relevant is what we're talking about on this symposium, constitutional law and the Internet, is that it lies at the intersection of some court issues, at least the First Amendment people have been talking about a lot here today. It also implicates the Fourth Amendment. It's called the Privacy Protection Act and it has very, very practical concerns, raises some particular issues for law enforcement as the statute is currently to be applied around the world.

In order to understand what the statute is about, you have to go back to April 1971, Palo Alto, California. There was a demonstration there at Stanford University Hospital. A number of demonstrators took over the offices at the hospital. Santa Clara and Palo Alto Police Departments dispatched officers. There were nine officers there stationed at one location in the building who were confronted by some demonstrators. There was a violent clash which ensued. Demonstrators escaped. They were not identified and the police officers were injured.

Two days after this happened the *Stanford Daily*, the student newspaper for the university, published a series of photographs of the clash, and it turned out they have a staff photographer who was there taking pictures as these police officers and demonstrators were going at it. Naturally, this was of profound interest to law enforcement, and so what the chief of police decided to do was get a search warrant. What he wanted to do was go search the *Stanford Daily*. So he applied for and was granted a search warrant to go to the offices of the newspaper and seize material which might constitute evidence of this criminal activity which was under investigation.

That's what they did, they went to the *Stanford Daily*. They searched the waste baskets, through photographic negatives, did not open, according to testimony in the case, did not open any locked containers, locked drawers, but nevertheless rummaged around enough in the offices that the proprietors of the *Stanford Daily* were, I think one can euphemistically describe it as displeased. They felt that their rights had been violated, and so they did what any red-blooded American does when he or she feels their rights have been violated, they filed an action under 42 U.S.C. § 1983. They went to federal dis-

trict court and claimed that the First Amendment barred the use of a search warrant under those circumstances, specifically circumstances where the entity in question is a news gathering organization not implicated in the criminal conduct.

They said they should have asked us, asked us to voluntarily produced it. We would have said no. They could have sent a subpoena and we would have talked to our lawyers and probably said no, but they could not force their way in, they could not search or seize. They could not compel in that way.

The district court agreed with this position. So did the Ninth Circuit. The Supreme Court held otherwise, though, in a decision *Zercher v. Stanford Daily* issued seven years after the fact, 1978. The Supreme Court said that the First Amendment was not a bar to the use of a search warrant under those facts. The Court decided on the longstanding precedent holding that law enforcement may use a search warrant to obtain mere evidence. You're not looking for instrumentalities of crime or contraband by means of a search warrant. You can go after mere evidence, and even if that mere evidence is in the possession of a party who is not suspected of the commission of the offense. So the court found that *Zercher* and the other police officers who obtained this warrant and conducted the search had not violated the constitutional rights of the *Stanford Daily*.

As you may imagine, this was not well received in certain quarters, and as a result there was a hew and cry over *Zercher*. In 1980, Congress passed a law, the Privacy Protection Act, which is somewhat of a misnomer. What it really is more of is a protection of expressive activity in utero, if you will. It's not so much about private facts but rather protection of things which are intended to become public. The P.P.A. is, in effect, a legislative overrule of *Zercher*. The statute in effect prohibits the use of a search warrant in certain cases, and *Zercher* is the model fact pattern in which it would be permissible to use a search warrant.

Okay, so the P.P.A.—we find this at Title 32 of U.S. Code, Section 2000 AA. This was enacted two years after *Zercher* and established a general rule which bars—it doesn't specifically say on its face "use of search warrant" because that would be too narrow. It says it is a bar against search or seizure of certain kinds of materials, and before we get to what the bar itself says, I would like to talk about the two categories of protected materials.

The first one is called work product. To lawyers and law students it may have a familiar ring. Let's see how familiar it is. First of all, what it's not. It excludes contraband, fruits or instrumentalities of crime. What it is is material which satisfies a three-part test. It's material which was prepared or created to be communicated to the public. For instance, an article that I might be writing which I intend to publish somewhere, on the web site or local newsletter. Note that under the statute it need not be in the possession of, to borrow Bob Hamilton's terms, the author. For instance, if the material in question is in the pos-

session of an editor, a typographer, anybody who is in the chain of preparing that material to be disseminated to the public, the material can have statutory protection. It must be for the purpose of public communication. It must be in the chain of public communication. And, third, in order to qualify as work product which receives more protection under the category it must include mental impressions, opinions or theories. That is drawn very closely from the standard for attorney work product.

The second category is what's called documentary materials, and you might think of this as the everything-else category or raw materials category. Again, there's exclusion for contraband, fruits or instrumentalities of crime. It is defined very, very broadly in the statute as materials upon which information is recorded. Again, it's explicit. It may be written or printed photographs, film, videotape. It may be electronic. It says it may be magnetically recorded, but I don't think they're talking about things that are purple. It's a typo for things that are magnetic. Photographs, at issue in the *Zercher* case. Things like copying of a corporate report, basically anything but which does not include mental impressions. Sort of the raw materials on which news reporting or communicative activities might be based.

So now we know what the two categories of materials are. What does the statute say about those categories? What it says literally is it shall be unlawful to search for or seize, so either one of those qualifies, any work product, materials, and again there's a similar cast of documentary materials, possessed by a person reasonably believed to have a purpose to disseminate to the public. So if the agent or law enforcement officer who would be conducting the seizure has a reasonable belief for thinking that the possessor intends to communicate this stuff to the public, then the statute would apply. So long as the means of public communication is, quote, is newspaper, book, broadcast or similar form of public communication. And I'll counter that last term in a moment.

Again, there's a similar general rule for documentary materials. It's materials which are possessed in connection with an intent to—generally, it's the work product itself, the things that contain opinions, theories and impressions which is to be communicated, raw materials. The same general rule, thou shalt not use a search warrant. You may not go to the *New York Times* or city paper or the New York press or name publication and use a search warrant to seize. You cannot search for or seize under any circumstances except—exceptions. As with all good statutes, there's some exceptions. Death or serious bodily injury, if that's a threat, then you may search or seize. Very, very narrow.

For documentary materials only, the test is a little relaxed. If you try to use a subpoena and you didn't get the goods or if by giving the notice that is inherent in the subpoena process there would be a risk that the evidence in question would be destroyed or altered or concealed, then you may also search or seize. That's a fairly exacting test. And then there is really the key to the statute and the thing I would like to focus on is the suspect exception which is what occu-

pied most of the attention of Congress in trying to crack the very convoluted statute. You'll see how convoluted it is here.

First of all, it applies to both kinds of materials. What I mean by the suspect exception, well, simply put, it's the case that you didn't have in *Zercher v. Stanford Daily*. Search or seizure is permitted under the statute. General rule, no search or seizure for the two categories. Now we have an exception. It says if there is a probable cause to believe that the possessor committed the offense or will be committing the offense to which the materials relate. So if you have somebody publishing a newsletter which is a stock scam, then it is okay to use a search warrant, go to the premises and seize the intended future publications because there's your suspect. The materials intended for public dissemination relate to the suspect. So suspect exception.

Pretty clear, right? No. Because there is an exception to the exception. You may not use a search warrant, you may not search or seize where the offense is a mere possessory offense. I've gone to great lengths to understand why they created the subsubexception. The reason was something like this: Suppose you have a reporter who has obtained a document that was stolen from a corporation. Say a corporation makes women's shoes and the document says—it's an internal study that actually competes with their most popular product is causing serious physical harm to the customers who buy and wear this particular line of shoes. Well, if the document is then stolen, then arguably the newspaper reporter, the investigative journalist who receives that document has in some jurisdictions, maybe all jurisdictions, violated the receipt of stolen property statute. We don't want law enforcement ginning up these kind of charges, so you go into the newsroom and use search warrants for those kind of mere possessory offenses. So you can't do it if it's a mere possessory offense.

And just to make it all the more confusing, there is a subsubsubexception. If the possessory offense relates to a national offense clearly, classified information or child pornographer as of , then you can search or seize. I hope all of your heads hurt a little right now because it makes my head hurt every time I think about this statute, which is about ten times a week. Just to review very briefly, the rule is if you got an innocent third party, *Stanford Daily* holding on to these protected materials, you should not search or seize, and so instead of using a search warrant, you want a subpoena instead. If you have a suspect who is committing something more than a mere possessory offense, you may search or seize. And then you have these other exceedingly rare kind of exceptions. But keep in mind the general rule, the suspect exception.

Let's talk about something simpler, the remedies for violations. Any party who's aggrieved by a search or seizure, damages $1,000 floor, counsel fees, costs, all the usual kinds of things. In addition, if the prospective defendants or state officers, you may sue them individually if the state has not raised sovereign immunity. What Congress said is states can decide. They can pay;

their police officers can pay. We'll let them make the call.

Interestingly, the statutes do not mention a so-called good faith defense. It specifically bars good faith defense. The police officer knows that the entity he's about to search is a publisher, call it that for shorthand, some entity intended to disseminate materials to the public. He knows—he's never heard of the Privacy Protection Act. He's heard of the Fourth Amendment and his state analog and he's complied exactly with those federal and state constitutional requirements and got his warrant, did the seizure in total good faith that what he was doing was legally processed. Liable. So there's no good faith defense. On the other hand, statutory violations are not grounds for supervision in a criminal proceeding. Again, that's explicit on the face of the statute.

Now, there's very little . . . surprisingly little case law in the PPA considering it's a statute that's more than seventeen years old. One case that is interesting in this context and sort of leads to what I would like to talk about today in a sort of computer online context is Steve Jackson Games against the United States Secret Service. I would like to give you a few of the facts. In 1990, the secret service suspected an employee in Austin, Texas has been engaging in political activity and got the search warrant and went to the premises of the business where they were told that Steve Jackson Games was a publisher and published games. The secret service seized a number of items. They seized a game that was in graph. Under the professional publication. They also seized a BBS, a bulletin board system, containing all kinds of private information including private electronic mail. I'm not going to go into that. That's another statutory thing I would be happy to talk about at some other symposium.

Steve Jackson sued the P.P.A., and district court found that secret service had violated the statute by means of its seizure of this game, the game *Cyberpunk*, that there was no reason to have—there was no reason that Steve Jackson Games was suspected of any offense, so it didn't fit the suspect exception so the seizure was improper.

The court did not explicitly reach the question of the extent to which stuff on the BBS would be protected under the P.P.A. Most of the matter—I have this on authority from Steve Jackson who told me this in Austin three weeks ago. Most of the stuff that went into the game was actually paper form. So the court hadn't really reached the question of whether or not BBS stuff—whether or not material on a BBS were to qualify for P.P.A. protection.

Why are we talking about the statute? Why did I come here today? Because the statute, it's sort of an interesting example of law of unintended consequences. The world today is very different from the world in 1980. Congress could not and obviously did not see the explosive growing of the computer world. Remember, in 1980 there was no such thing as an IBM PC. There were Tandy closed computers and some TI 994As which now are basically used as doorstops.

Why does the world of today, 1998, make a difference? There are two

complications, one which you should be a mile off because it's what Ed Cavazos was talking about. The Internet makes everyone potentially an individual who is in possession of material and has a purpose to disseminate that material to the public. There's no case law yet saying you can publish online, you can publish on Usenet, put something up on a web site that you're covered by the P.P.A., but I think it's worth noting that in legislative history of the P.P.A., Congress said form of public communication, there was a catchall, newspapers, books, magazines and broadcast form of public communication that tag on at the very end of that phrase "is designed to have a broad meaning." So I think it is likely that the court would reach the result that such matters are equally protected under the statute.

The second issue that we have today that didn't really exist in the way it exists today is computers now store vast, vast quantities of data, and because they do, they store all kinds of different information often in one place. It's a problem known as commingling. Well, why does that matter? The reason it matters is, at least from law enforcement's perspective, what happens if the suspect—you're investigating a crime. What happens if your suspect possesses P.P.A. material that is unrelated to the suspected offense. He's got a hard drive and there's all sorts of stuff on it, and law enforcement has a reasonable basis so there's knowledge to know that he is a potential publisher, he's got a web page, whatever. What should be the result?

Let me just clarify why that sometimes arises. In factual scenarios it's often impossible to effect a search and seizure to search computers. Sometimes, I happily concede that this is not in a majority of cases, you have what I would call forensic issues. Somebody's got a weird operating system. It's configured kind of strangely, and it's not possible to tell how it works.

More commonly, there is a very serious problem with the fact that you have vast amounts of data and it's too time-consuming to conduct a search on site. Law enforcement agents go to somewhere, they cannot camp out there for days and days searching through all the records. And that is equally true of paper documents. The computer is often an instrumentality of an offense. Sometimes it contained contraband.

It's not always necessary to seize the computer, take away the box, the machine itself. You can do what's called here roring the drive. Imagine matching the media. Even if you can't search through all of it to find the particular stuff that you're interested in, you can make a copy. Of course, that's still a seizure. The fact that you left the machine there doesn't mean you didn't seize something when you took away a copy of what was on the media. And even if the search is on site, you have to at the very least prohibit noninvestigative agents who are present or not necessarily present but anyone who formerly had a right of access to that computer, you have to prohibit their access to the machine. You cannot conduct a search on the computer while other people are logged into it either locally or remotely because, for all you know, they're de-

stroying or altering the data. And by excluding people from access to information on a computer, if you're excluding them from access to PPA protected materials, that is arguably, I think a court could conclude that is a seizure, a technical violation of the P.P.A.

Let me give you a couple of scenarios how this might play out. Suppose you have a web page designer. He's got a client. Please design. And they have a falling out over money. The consultant feels he's not being paid the money he's entitled to, so what he does is he logs onto the web server and being disgruntled he puts a picture of a naked women on the page, bad words instead of the company's product list. Let's say that law enforcement has a reason to think he did this from home. Telephone records, for instance, Internet transaction logs consistent with his being logged on from home at the time that the files were changed.

We also know this is somebody's stock and trade is designing web pages. We have every reason to think on his computer at home he's going to have a draft web page, maybe his own, for which he is preparing materials. When you go to his house you may find some voluminous quantity of data. I think you can reasonably believe he will have material intended to be disseminated to the public, but you also have probable cause to go there and search for evidence of the crime. So I guess my point here is that the P.P.A. as literally applied today, excuse me, as it could be potentially interpreted literally would create a situation in which law enforcement would have a legitimate reason to go and investigate a suspect for suspect exception materials to seize information that relate to your crime and the investigation might also be found to be in violation of the statute. I think that's a potentially troubling result. It has not happened yet. I know that when I get calls from people out in the field, I have to counsel on the scope of their seizure. We try to be very careful. But law enforcement has a need in these kinds of cases to conduct searches and conduct seizures, and I think the P.P.A. creates a risk of deterring certain legitimate law enforcement activity.

I got a call last week from an assistant district attorney on the West Coast who had a police officer who was familiar with the Steve Jackson Games case and was worried sick to seize the home computer of a suspect in a murder case. I think that's nuts. I think that that's the kind of crime you do want to investigate, and my counsel was do the search. But it is deterring some law enforcement activities that I think should not be deterred. To just make one final point here, for more information on computer search and seizure, you can get the federal guidelines for searching and seizing computers. It's a voluminous document. Some Fourth Amendment considerations and other statutory considerations. And you can find that on my section's home page on the DOJ web server www.usdoj.gov, governor/criminal/cybercrime. Thank you very much for your time.