My computer is pleadin' the Fifth

Fifth Amendment case in Denver causes concerns

by Glen C. Davis

Recently, the Supreme Court ruled that GPS tracking devises violated the Constitutional Fourth Amendment guarantees because people have a reasonable right to privacy in their cars. As I understand the ruling, however, if you have *OnStar*® or one of the other government tracking devices already in your car, they can track you through that system.

On January 4th, the Denver Post reported on another example of the courts grappling with the Bill of Rights in the digital age. And the case is shaking up civil liberties groups.

The case involves Ramona Fricosu who was allegedly involved in a fraud scheme along with her husband. One of the items seized by the prosecutors was her laptop computer. The laptop, however, was encrypted and the prosecutor could not retrieve the contents. Fricosu refused to give the password citing her Fifth Amendment right against self-incrimination.

John Ingold of the Denver Post reported on the 24th, "In an order issued Monday, U.S. District Judge Robert Blackburn said requiring Ramona Fricosu to provide an unencrypted version of her laptop's hard drive to prosecutors does not violate her rights against self-incrimination. Instead, Blackburn ruled that providing the unlocked laptop wouldn't be self-incriminatory because it wouldn't prove anything that the government doesn't already know."

Hanni Fakhoury, an attorney with the Electronic Frontier Foundation, still thinks the Fifth Amendment applies in this case, according to the article. The case is going to the 10th Circuit Court of Appeals.

This is actually a compelling case and one likely to make it to the Supreme Court. On the one hand, you do have a right not to provide incriminating evidence in the Fifth Amendment. That is why signing anything "under penalty of perjury" is quite frankly unconstitutional. You cannot be compelled to sign away your rights.

On the other hand, the Fourth Amendment guarantees, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures shall not be violated,…" While the police today have pretty much the same power that the "Redcoats" had prior to the revolution—which was among the chief complaints of the colonists—they still must obtain a warrant from a judge. In this case, they did that and the seized computer was among the evidence for their case. Whether or not the computer and the location of the computer was specified on the warrant as is REQUIRED by the Fourth Amendment is another topic.

In this case, I would have to agree with District Judge Blackburn. Apparently the laptop was just another piece of evidence in the pieces of evidence that they already had.

Let us set another scenario, however. Let us say that a person is sitting and using a wireless laptop at a coffee shop. A police officer wanders over and the person presses a button and locks the computer. Does the officer have a "probable cause" to order the person to unlock the laptop? No. This would violate both the Fourth and Fifth Amendment. If the officer "sees" something that the person is doing and knows that it is illegal, he may then have probable cause to arrest and cause the person to unlock the computer. He already sees it and knows it is there. If the coffee shop owner, however,

sees actual evidence that the person is using the computer for illegal purposes and reports it, then the police have enough for a warrant and to cause the person to unlock.

Granted, in the case of Fricosu, the prosecutors and police have not “seen” the contents so they do not “know” there is anything related to the case on the computer at all. That may be an “out” in this case. Still, I believe there is enough “probable cause” that this does not represent a violation of either the Fourth or Fifth Amendment. Does the lock on your front door, for example, give you a Fifth Amendment right to keep officers from performing their duty after they have complied with the Fourth Amendment?

One question that might come up, however, is what about online storage sites? If a person stores the data at an online site that is not listed on the search warrant, can the police access it or use it as evidence? I would think not until they obtained another warrant for the evidence. Of course, that would be served to the provider of the service, not the defendant.