Statement of

Robert Richardson
Dirctor, Computer Security Institute
Robert.Richardson@ubm.com

Before the
United States Senate
Committee on the Judiciary
Subcommittee on Crime and Drugs

Chairman Specter, Ranking Member Graham and members of the Crime and Drugs Subcommittee, thank you for inviting my written statement and for this opportunity to speak to the issue of video surveillance, particularly as it relates to surveillance using common consumer mobile computing devices such as notebooks, cell phones, and personal digital assistants. These devices, because of their ubiquity, clearly present opportunities for enhanced communication, but they also challenge our notions of security practices as they relate to privacy and surveillance. As Director of the Computer Security Institute, I am engaged daily with these issues as they relate to organizations that maintain large computer and network infrastructures.

The instigation for our discussion today was the desire of one such organization to protect its computer assets. As one would probably expect, concern that mobile assets may be lost or stolen is completely well founded.

One project undertaken by the Computer Security Institute over the past fourteen years is an annual survey of our information security professional community, specifically within the United States. In the most recent survey, 42% of 443 respondents said that their organizations had suffered the theft of laptops or mobile devices in the previous year. Only infection by malicious software, or *malware*, reported by 64% of respondents, was more prevalent.

Perhaps ironically, the modus operandi of today's sophisticated malware is not at all unlike that of the software deployed by some organizations to monitor their notebook computer assets. Both with tracking software and malware, a fundamental level of direct control of the device is transferred to a third party at a distance. This transfer is achieved in both cases because both malware and tracking software have gained or been granted access to the most extensive level of control of the computer, so-called "root" control. Most issues of privacy and access within the confines of a computer have, at their root, the issue of root access.

When the owner and the primary user of a device are one and the same, control and responsibility is easily understood and it is the user who has control of the root account. But in the instance of, say, an employer that loans a notebook to an employee, the employer may well withhold root privileges from the employee. This gives the employer more control over the device than the user, and indeed more control than the user may be aware of, such as the ability to remotely operate a built-in camera.

Root control may be abused in many ways, including by surreptitious spying. But this notion of root control is a necessary one and, extended only slightly, gives us an opening to separate and

protect different categories of use within a device. There can be a category of "workplace" use, for example, that is entirely walled off from "personal" use.

There are multiple ways to achieve this that it would be too lengthy and technical a discussion to delve into here, but in fact most Americans are already familiar with one such division of control. Ninety-five percent of cell phones sold each year within the US are "locked" phones, meaning that their use is controlled and restricted by the carrier that originally sold the phone and that is providing service to it. Using the phone for conversation or texting is understood to be a context where the user is in control. That same user, however, cannot update the core software that runs the phone. The service provider can and does because the service provider has what is in effect root control of the phone.

It is possible, in short, to "lock down" part of a system so that the locked down elements function as a complete computer system unto themselves, with separate software applications and separate storage for files. That this locked down environment is truly separate from the rest of the computer can be rigorously demonstrated using well understood techniques based on advanced forms of encryption as well as a computing framework known as "trusted computing."

Almost all notebook computers sold since 2004 include a Trusted Platform Module housed in a sealed, tamper-proof component within the computer. This provides a reliable foundation for a protected, high-control partition of the computer. In the vast majority of cases, however, this TPM functionality is not enabled and it would be disingenuous not to note that trusted computer systems have raised a great deal of controversy within the information security

community. This controversy, however, stems precisely from a fear that third parties such as Microsoft will have overreaching control over consumer-owned PC's. This is not of concern when we are speaking of an organizational owner extending control over its own PCs.

Within this locked down system, a third party such as a school or employer has an oasis of control. If they don't want to allow chat programs, chat programs can be barred. If they don't want pornography stored, they can scan for it and monitor employee use at will. And the user of that system will know that whenever they are using this system in this workplace context, they may well be monitored.

On the same system, however, it is possible to use what effectively is a second computer that is not locked down, or that is locked down in a less restrictive way. That we can create clear technical boundaries means that we can, by extension, create clear legal boundaries.

We have the option to legislate in a way that recognizes the possibility of such boundaries. By doing so, we can establish that the context in which any kind of surveillance occurs is either clearly within or outside of legal bounds. I appreciate the opportunity to discuss this important issue and will be happy to answer any questions from the Subcommittee.