

**Opening Remarks for a Panel
Royal United Services Institute
London, United Kingdom
October 22, 2009**

Good morning. My name is William Snyder. I am a law professor from Syracuse University in New York State, where I teach such things as computer crimes, counterterrorism law, national security law, following 15 years service with the United States Department of Justice. I have been asked to summarize for you the U. S. experience with regulating cyberspace, in three to five minutes or less.

First, I remind you that we have 51 sovereign legislatures in the United States, and that their approaches to any issue are about the same as a room full of cats following a crash of thunder -- each runs its own way. Still, some patterns have emerged. In the early 1970s when the enormous potential harm of computer misuse first became apparent, no legislature had enacted a computer crimes statute. When prosecutors first began to bring charges for computer misuse, we naturally turned to physical crimes such as trespass, burglary, and theft. The fit of physical world crimes to the virtual world proved surprisingly poor. Our courts struggled with identifying a property interest that had been taken when, after the usual data theft, the owners still possessed the property. Several state legislatures tried different approaches until finally in 1986 Congress passed the Computer Fraud and Abuse Act.

That act makes it a crime to access a protected computer without authorization or exceeding authorization and thereby obtain information. Unfortunately, Congress did not define "exceeding authorization," and some courts soon concluded that any violation of an Internet service provider's user agreement constituted "exceeding authorization." Most user agreements are thousands of words long and contain nebulous prohibitions against uses that anyone else might find offensive. Moreover, we were told that this federal law would play a very limited role in our national system, because it only applies to "protected computers" defined as those in or involving interstate commerce. That may have been a meaningful limitation in 1986 before the World Wide Web, but today that definition includes every computer connected to the Internet and every cellular telephone. The result is that today nearly every single American commits a felony every day.

This has been a pattern for our Congress in areas of rapid change. They create very broad, powerful statutes, and leave it to the discretion of prosecutors such as I was to decide whom to charge. Recent history has radically reduced the American public's trust in its prosecutors, however.

Procedural law in the cyber realm has proved even tougher. The very nature of Internet protocol communications divides them into packets of data that almost instantly cross jurisdictional boundaries. F.B.I. director Robert Mueller has decried the "patchwork of laws" his investigators face as making it nearly impossible to obtain digital evidence in a manner that will maintain its admissibility in our own courts.

But, this is a conference on cyber security not cyber crime. The topic of the times in the U.S. is *offensive* cyber security. That is, when can a U.S. corporation or government agency reach out

and strike a cyber attacker's computers? Just last month, a very distinguished panel generated a report by our National Academy of Sciences concluding that the traditional law of armed conflict and the United Nations Charter should govern offensive cyber security. That body of law applies when there has been an armed attack. According to the panel, the existence of an armed attack should be determined by the effects of a cyber attack, not by its perpetrator's intent. Again, physical world concepts do not apply well to the virtual world. By the National Academy of Sciences logic, had the Soviets shot an ICBM armed with a nuclear warhead into Washington in 1973 but the warhead failed to explode, no armed attack would have occurred and no U.S. response would have been justified. The public would hardly have stood for that.

The fundamental international law principles of necessity, proportionality, and discrimination between combatants and noncombatants are virtually impossible to apply to the Internet, whose attributes include anonymity, unpredictability of outcomes once a virus is released, and shared hosting and backbones. Thus, the U.S. experience demonstrates the title of this session, "The Limits of the Possible When Legislating in Cyberspace." The regulation of a realm that knows no national borders cries out for a global solution, while the American public generally recognizes a social contract with -- and therefore the legitimacy of -- only those institutions created by its own Constitution.

A person who has studied Internet law since its earliest days is our featured speaker this morning. Professor Lilian Edwards is Professor of Internet Law at Sheffield University. The details of her distinguished career are in your program, but I want to underscore that the third edition of her seminal work "Law and the Internet" was just released last month. Her presentation will be on the record, but the subsequent questions and answer period will be confidential. Welcome, Professor Edwards.

- William C. Snyder
www.williamsnyder.com