Nervous System: Florida Man, Joe Biden, and the Federal Computer Crimes Act

BY DAVID KALAT

With the aggressive pace of technological change and the onslaught of news regarding data breaches, cyber-attacks, and technological threats to privacy and security, it is easy to assume these are fundamentally new threats. The pace of technological change is slower than it feels, and many seemingly new categories of threats have been with us longer than we remember.

Nervous System *is a monthly series that approaches issues of data privacy and cyber security from the context of history—to look to the past for clues about how to interpret the present and prepare for the future.*

In 1978, Florida became the first state to pass a law specifically covering computer crimes. It was quickly hailed as a model for the types of legislation that would be needed in other states or even nationwide to deal with growing threats to information security. Nine states soon followed Florida's lead and passed similar legislation. The Florida bill's author, Representative Bill Nelson (D), turned his attention to proposing federal legislation that would define computerized information as property and make misuse of the data a federal offense. It turned out to be a rocky road.

As the nation's economy transitioned to being cashless, information focused, and computerized, Nelson recognized that criminal laws were woefully behind the times. His proposal sought to define electronic information as property and make misuse of electronic information a federal offense. He felt this was needed because, at the time, both the law and the public at large still struggled to recognize computer crime as "real," as compared to physical theft, even though in some cases the sums at issue in computer crimes vastly dwarfed those that a "real-life" burglar might steal.

As a politician, Nelson naturally was attracted to punchy turns of phrase to help sell his pet project. As he put it, there was an inherent problem when a thief could make off with a $5 million software program but only risk prosecution for the $5 cost of the cassette tape used to store it.

Although modern readers may find the reference to "cassette tapes" a little quaint, the problem was real.

For example, in *United States v. Kelly* (507 F. Supp. 495, E.D. Pa., 1981), the defendants misappropriated the resources and time of their employers' computers to conduct their own separate business. In the end, they were prosecuted only for having failed to disclose that theft on the brochures they mailed to prospective customers, thereby committing mail fraud. Had they admitted in those brochures that their business was using another company's computers to perform its services, there would have been no case against them. Or, in *United States v. Seidlitz* (589 F. 2d), the prosecution of a defendant charged with copying stolen software code fell apart when the district court concluded that nothing had been *transported* across state lines if the original data had remained in the victim's computer.

Nelson's proposal led to congressional hearings in 1978 and 1980 where then-Senator Joe Biden, chairman of the Senate Judiciary Subcommittee on Criminal Laws and Procedures, took a prominent role in shaping the debate.

Senator Biden requested industry comment on Nelson's proposed legislation. One area of focus for that testimony was on the importance of developing layers of remedies and punishments to ensure that more serious computer attacks, such as ones that threatened national security, would be treated differently from less serious ones, such as teenage misadventures exploring computer networks.

Biden's hearings found considerable resistance to categorizing the misuse of computers as a distinct form of federal crime. The organizations that maintained large computer systems were reluctant to admit to a problem, especially when the wider public did not even perceive there to be one. Speaking in 1981 and quoted in the Christian Science Monitor, L. John Rankine, IBM's data security director, said, "The actual, purposeful frontal attack on a computer from the information available to us is way down the scale of what can happen to a machine." The real threat to data security, according to Rankine and others, was poor administration, not hackers or malicious attacks from outsiders.

Other opponents argued that computer crime laws were not needed because few such incidents were reported. Along those lines, Milton Wessel, a lawyer and instructor of computer law at Columbia University, testified that no prosecutions had yet occurred under Florida's law.

Although the proposed law was not passed, the debate surrounding it helped shape the discussion around cybersecurity until the eventual passage of the Computer Fraud and Abuse Act in 1986. Nelson's law stalled out each time he proposed it—in 1978, 1980, 1982, and 1983. For several years, the only direct impact of the congressional testimony was to provide a model to individual states seeking to emulate Florida's law.

At the federal level, though, there was not enough support for a nationwide response to the issue of computer crime. That is, until a high-profile incident emerged in which the plot of the movie ***WarGames*** seemed to come true, and a teenage misadventure on a computer network actually did threaten national security. That event (described in an earlier installment of Nervous System) led to the passage of the Computer Fraud and Abuse Act, which—not coincidentally—contained much of Nelson's language.

Legaltech news