International Cybercrime Prevention Act of 2021

Section by Section Analysis

Section 1: Short Title

Section 2: Predicate Offenses. This provision would make the use of illegal interception devices a money laundering predicate and make violations of the Computer Fraud and Abuse Act (CFAA) a RICO predicate. These important changes would give prosecutors new tools to fight sophisticated cyber criminals.

Section 3: Forfeiture. This provision would authorize the forfeiture of illegal interception devices, proceeds from the sale of spyware, and the property used to facilitate these crimes. While current law allows for prosecution of these crimes, these provisions would ensure that prosecutors can seize the tools used by criminals to violate victims' privacy and the proceeds resulting from these crimes.

Section 4: Giving Courts the Authority to Shut Down Botnets. This provision would enhance DOJ's ability to fight networks of compromised computers known as botnets. Under current law, DOJ's authority to obtain injunctive relief to shut down botnets is limited to those botnets engaged in fraud or illegal wiretapping. This provision would expand DOJ's authority and allows for injunctions against botnets engaged in a broader range of illegal activity, including destruction of data, denial of service attacks, and other violations of the CFAA.

Section 5: Aggravated Damage to a Critical Infrastructure Computer. This provision would create a new criminal violation targeting those who knowingly cause damage to computers that control critical infrastructure systems, such as dams, power plants, hospitals, and election infrastructure.

Section 6: Stopping Trafficking in Botnets and CFAA Forfeiture. This provision would prohibit selling the "means of access" to a compromised computer if the seller knows or has reason to know the buyer intends to cause damage to the computer, or use the means of access to commit wire fraud, or violate the criminal spam statute. It targets cybercriminals who sell access to the compromised computers within a botnet. Criminals purchase access to these computers for a variety of reasons, including to load additional malicious software, or to enlist the compromised computers in a denial of service attack. Under current law, it is difficult to prosecute sellers of access to compromised computers—especially when the seller is not the person who compromised the computer in the first place—because no current criminal law directly prohibits this conduct. This section closes this loophole.