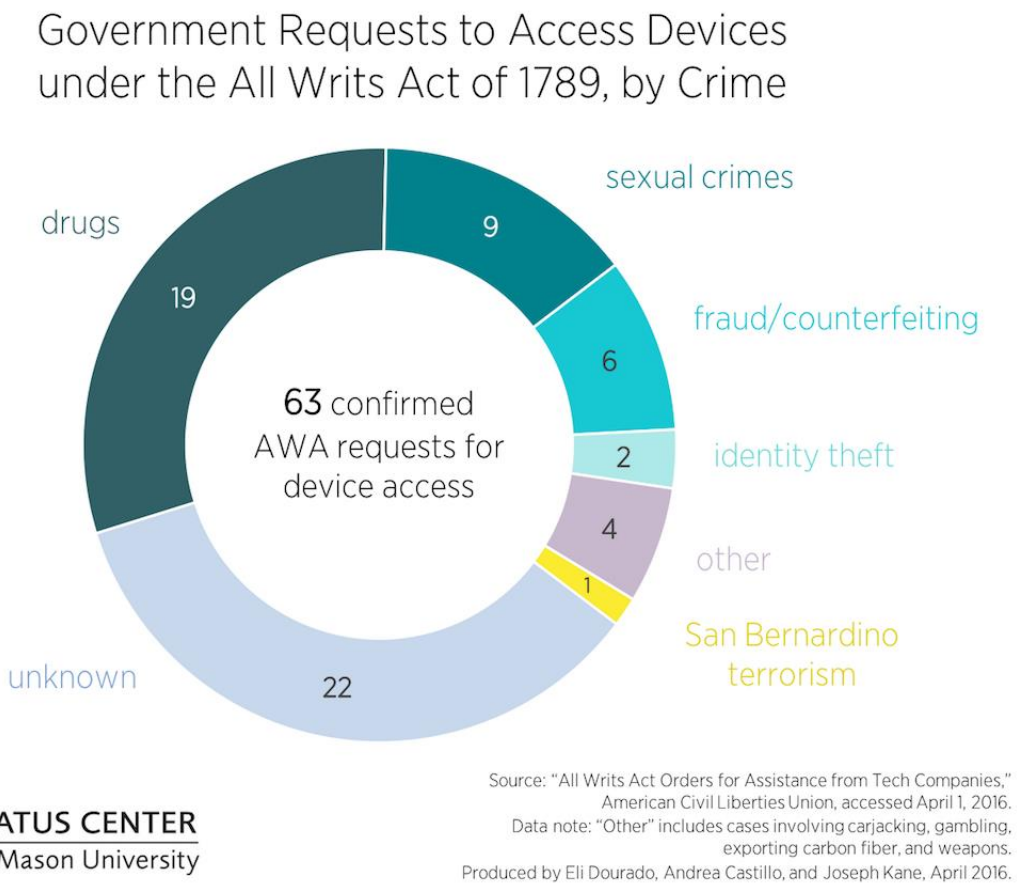
More Than “Just One iPhone”: Law Enforcement Cites All Writs Act to Access Many Devices

Eli Dourado, Joseph Kane, Andrea Castillo | Apr 27, 2016

The FBI’s recent conflict with Apple over accessing a locked iPhone in its investigation of the San Bernardino terrorist attack eventually settled out of court when an external party was able to unlock the device. Contrary to the government’s claims that this incident was about just one iPhone, this was far from the first time that law enforcement cited the All Writs Act of 1789 (AWA) to compel private companies to compromise secure devices. This week’s chart shows that law enforcement agencies have attempted to apply this law numerous times in recent years for a range of criminal offenses, particularly drug-related crimes.

The chart uses a dataset from the American Civil Liberties Union (ACLU) listing compiled court documents in cases where law enforcement bodies have appealed to the AWA to get access to devices with operating systems from Apple and Google. The data show that the AWA has been invoked to access data on devices in at least 63 other cases.



We further analyzed the data to discern the nature of the crimes involved in each case, and we were able to determine the crime involved in 41 of the cases. We categorized each case according to the primary nature of the crime: drug crimes, sexual crimes, fraud and counterfeiting, identity theft, and terrorism. The “other” category includes

four cases involving gambling, carjacking, exporting carbon fiber, and illegal possession of weapons. Each of these categories is displayed on the pie chart above. Our dataset contains links to each case and a description of the crime involved.

Of the 41 cases in which the associated crimes are known, 19 involve drugs, and only the San Bernardino attack involves terrorism. Overall, of the 41 cases for which an offense is known, two-thirds related to nonviolent crimes.

Public officials often justify the necessity of such practices as a necessary trade-off between privacy and public safety. For example, in his congressional testimony on the recent dispute with Apple, FBI Director James Comey framed the agency's application of the AWA as a question of "how to balance the privacy we so treasure . . . and also achieve public safety which we all very much treasure." However, the data suggest that many of these orders to compromise secure devices are not in fact related primarily with public safety.

Instead, these cases show that much of law enforcement's interest in accessing encrypted data on personal devices has more to do with pursuing the vexed social policy of the "war on drugs" than with combating terrorism or other literal threats to public safety. If law enforcement officials wish to discuss the tradeoffs raised by the widespread use of strong encryption, then it must be forthright about its policy goals.