

FBI'S CELL PHONE INVESTIGATIVE KIOSK WOULD ALLOW FOURTH AMENDMENT VIOLATIONS

Jim Comey wants to sacrifice individual security to ensure the FBI can access cell phones easily.

But in an audit of a forensic lab in Philadelphia, DOJ's Inspector General found that the FBI is not keeping adequate control of the kiosks that FBI uses to do initial reviews of data on cell phones.

As the report describes, cell phone kiosks serve as a "preview" tool of the contents of the data stored on a phone.

Cell Phone Investigative Kiosks (Kiosks) are available at select FBI field offices and RCFLs. A Kiosk is a preview tool that allows users to quickly and easily view data stored on a cell phone, extract the data to use as evidence, put it into a report, and copy the report to an electronic storage device such as a compact disk. Kiosks are not designed to take the place of full-scale cell phone examinations performed by certified Forensic Examiners; however, the evidence produced by a Kiosk is admissible in a court of law. Kiosk users are required to take a one-time hour-long training course and be familiar with computers. In addition, FBI policy requires Kiosk users to confirm they possess the proper legal authority for the search of data on cell phones or loose media.

The FBI only recently started tracking who had access to these kiosks. And when DOJ IG audited

this office's use of the kiosk, it found that 27% of the people who were accessing it hadn't filled out the requisite paperwork to ensure only appropriate people used it.

We found that the PHRCFL did not have adequate controls over the access and use of its Kiosks. FBI policy requires Kiosk users to confirm they possess the proper legal authority for the search of data on cell phones or loose media. During our fieldwork, the FBI did not provide any information to show that PHRCFL Kiosk users were required to sign-in, identify the case related to the evidence being examined, or, as required by FBI policy, confirm that they possessed the proper legal authority to search for evidence on the cell phone. In addition, the FBI did not provide us with any information regarding controls in place at the PHRCFL to ensure that users do not use the Kiosks for non-law enforcement matters.

[snip]

we conducted limited testing of 25 visits during FYs 2012 through 2014 to verify compliance with the procedures in place. When the PHRCFL began using the Acknowledgment Form in May 2012, its visitor's log contained a field for the purpose of each visitor's visit. We selected names from the visitor's log whose stated purpose for the visit was Kiosk usage and compared those names and dates to the corresponding Acknowledgment Forms. For the 17 visits we selected between May 2012 and January 2013, we found that approximately 24 percent of the PHRCFL Kiosk-related visitor log entries did not have corresponding Acknowledgment Forms.

[snip]

We believe that although the Kiosks are an efficient tool for law enforcement officers to use to examine digital evidence that may not require the extensive examination of a certified Forensic Examiner, Kiosks are vulnerable to potentially serious abuse. For example, without proper controls, it is possible that a Kiosk user could use this tool to view private cell phone information for non-law enforcement purposes. It also is possible for a user to use a Kiosk without proper legal authority, thereby engaging in a Fourth Amendment violation.

Later in the report, the IG noted that none of the centralized databases tracking other uses of the forensic office track use of the kiosk. That, combined with the paperwork failures, would sure permit FBI to do a whole lot of illegal cell phone searching that would not be tracked.

Which might explain why the numbers FBI shows for searching cell phones don't actually match Director Comey's stated concerns about iPhone encrypting its phone.