Researchers uncover privacy risks in cellphones purchased at police auctions

July 17 2023

(From left) University of Maryland computer science Ph.D. students Richard Roberts and Julio Poveda are shown with their adviser, Associate Professor Dave Levin. The trio recently concluded a study that uncovered significant privacy concerns with cellphones purchased from police property room auctions. Credit: University of Maryland

Law enforcement agencies nationwide regularly sell items that are seized in criminal investigations or are unclaimed from lost-and-found inventories. Many of these items—vehicles, jewelry, watches and electronic devices like cellphones—end up at online auction houses.

People looking for a bargain can bid on cellphones in bulk, snatching up dozens at rock bottom prices for parts or other uses. This ultimately provides revenue for the police agencies, making for a good deal for everyone involved. Or is it?

A recent study by University of Maryland security experts found that many of the phones sold at police property auction houses are not properly wiped of personal data. The study, conducted over two years with cellphones bought from the largest police auction house in the U.S., uncovered troves of personal information from previous owners that was easily accessible.

Of the 228 phones that the UMD team successfully bid on, 61 (27%) contained personal data like social security numbers, credit card and banking information, passport data, pictures of driver's licenses, and more.

"We were actually surprised at the level of personal information we found, and the ease by which we could access it," said Dave Levin, an associate professor of computer science who led the UMD team.

Levin, a core faculty member in the Maryland Cybersecurity Center, first became interested in this topic through a casual conversation with a colleague. After determining there was a security breakdown—whether through police not wiping the phones, or auction houses not taking proper safeguards before shipping items to the highest bidder—Levin and several of his graduate students set out to explore the scale of the problem

The first step was to work closely with the university's legal counsel and institutional research review board to determine the appropriate protocols needed to view any personal data.

"There were stringent guidelines in place—how each phone we received was catalogued, the processes we used to access the phones, and most importantly, what we would be legally required to do if we found any evidence of child abuse," said Julio Poveda, a second-year computer science Ph.D. student who was part of the research team.

The UMD team did not come across any evidence of child abuse, but did uncover other information that was unsuitable for public dissemination, such as depictions of adult nudity and drug use.

Some of the phones they accessed had been used in criminal activities like identity theft, a discovery Levin found particularly troubling.

"It's as if people that were victims of identity theft were being 're-victimized' by having their personal information available again for anyone to see," he explained.

The UMD team determined that some of the phones had been used by sex workers, with text messages between the workers and their clients still intact.

"It's important to remember that your phone does not just have your data, it has data from anyone who has communicated with you," said Richard Roberts, a sixth-year computer science Ph.D. student and lead author of the study.

Roberts, who presented the team's academic work at the IEEE Symposium on Security and Privacy earlier this year, said that out of the 61 phones the

researchers accessed, they determined that there had been some form of digital contact with more than 7,000 people.

Levin, Poveda and Roberts are all security experts, but decided against using using any type of sophisticated digital forensics for their study. "We wanted to attempt to gain access to any cellphone data using techniques that someone on the street might use," Roberts said.

The researchers were shocked at how easy it was. One of the phones arrived with a sticky note attached with the phone's passcode in plain view, a leftover from the originating police agency that had already legally hacked the phone. Multiple other phones had PINs or passcode patterns that were easy to guess.

"Sadly, passcodes like 1-2-3-4 are still in common use today," Levin said.

Last October, the researchers reached out to the auction house where they purchased the phones. The company—PropertyRoom.com, which bills itself as the largest police auction house in the U.S. working with more than 4,400 law enforcement agencies—promised to investigate the problem. Shortly after that, the company stopped selling bulk lots of phones altogether for a short period, then started again, prompting the researchers to purchase another batch.

"We found that PropertyRoom had started wiping the phones but failed to wipe the phones' [Secure Digital] cards, which in several cases had partial backups of the phones' contents," Levin said.

After pinging the company again to inform it of this oversight, the UMD researchers received no further response.

A subsequent investigative report by a local television station prodded

the company to publish a message on its website stating it was aware of the security concerns and was taking corrective measures.

From a security standpoint, Levin said, police agencies should avoid auctioning used cellphones. "Just destroy them," he said. "[The police agencies] don't get that much money in return, and the potential damage far outweighs any financial incentives."

He also suggested that people take better precautions in the event their phone is lost or stolen and ends up being resold.

"Use your phone under the assumption that somebody else might later become its legal owner," Levin said. "Set a passcode that is hard to guess, minimize the private information that's easy to access, and remotely wipe your phone if it is lost or stolen. Otherwise, our study shows just how easy it is for someone to gain an incredible amount of access to your private information."

More information: Richard Roberts et al, Blue Is the New Black (Market): Privacy Leaks and Re-Victimization from Police-Auctioned Cellphones (2023). DOI: 10.1109/SP46215.2023.00167

Provided by University of Maryland