Blue Is the New Black (Market): Privacy Leaks and Re-Victimization from Police-Auctioned Cellphones

Richard Roberts, Julio Poveda, Raley Roberts, Dave Levin
University of Maryland

***Abstract*—In the United States, items in police possession are often sold at auction if they are not claimed. This includes cellphones that the police obtained through civil asset forfeiture, that were stolen, or that were turned in to lost-and-found. Thousands of US police departments partner with a website, PropertyRoom, to auction their items. Over the course of several months, we purchased 228 cellphones from PropertyRoom to ascertain whether they contained personal information. Our results show that a shocking amount of sensitive, personal information is easily accessible, even to a "low-effort" adversary with no forensics expertise: 21.5% of the phones we purchased were not locked at all, another 4.8% used top-40 most common PINs and patterns, and one phone had a sticky-note from the police with the PIN on it. We analyze the content on the 61 phones we could access, finding sensitive information about not only the phones' previous owners, but also about their personal contacts, and in some cases, about victims of those persons' crimes. Additionally, we analyze approximately two years of PropertyRoom cellphone auctions, finding multiple instances of identifying information in photos of the items being auctioned, including sticky-notes with PINs, owners' names and phone numbers, and evidence stickers that reveal how the phones were obtained and the names of the officers who obtained them. Our work shows that police procedures and phone auctions can be a significant source of personal information leakage and re-victimization. We hope that our work is a call to arms to enforce new policies that either prohibit the selling of computing devices containing user information, or at the very least impose requirements to wipe phones in a manner that the US federal government already employs.**

I. Introduction

Police play a critical role in ensuring the safety and protection of society. Through the course of these efforts, police commonly come into the possession of various items through civil asset forfeiture, seizure of stolen items, or even simply through lost-and-found. Police departments often auction off any items of value that remain unclaimed for a period of time, including cars, jewelry, or the central focus of this paper: cellphones.

It is well-known from seminal work by Garfinkel and Shelat [12] that secondhand computing devices bought from online auctions and pawn shops often contain data from their previous owners. However, cellphones sold via police auctions represent a unique set of risks when compared to other retail outlets: Phones in police custody are more likely to contain evidence of criminal activity. Moreover, if a phone was stolen or lost-and-found, then it may be sold without their previous owners' knowledge or consent. Finally, through the course of criminal investigations, police sometimes use advanced forensics tools to grant them access to sensitive information. As we will show, heightened access is sometimes extended to those who win the phones at police auction.

In this paper, we seek to understand the potential threats posed by police auctions of secondhand cellphones. Over several months, we purchased 228 cellphones from PropertyRoom[1], an auction website that partners with thousands of law enforcement agencies and municipalities across the United States. Following a strict protocol (§III) agreed upon by our institution's Institutional Review Board (IRB), Division of IT, and legal counsel, we analyzed the content of these phones to understand the extent to which private and sensitive information is leaked.

In addition to being the first thorough study of phones purchased from police auctions, there are three key aspects that differentiate our work from prior analyses of data on secondhand devices:

Re-victimization of identity theft victims. Phones may end up in police custody because their owners were arrested for committing a crime, such as identity theft. In some cases, the phone *itself* was used as a tool to commit that crime. We initially expected that police would never auction these phones, as they would enable the buyer to re-commit the same crimes as the previous owner. Unfortunately, that expectation has proven false in practice. This work shows the extent to which police sold phones with victims' social security numbers, credit cards, and credit histories. Even worse, in one case, the police cracked a phone's PIN and wrote it on a sticky-note that was attached to the phone; this phone was used in identity theft and contained extensive amounts of victim data.

Weakened threat model. Tools like Cellebrite[2] and GrayKey[3] are used by law enforcement agencies and researchers alike for forensic analysis and to gain access to restricted devices. However, licenses cost thousands of US dollars and are out of reach for most users.

In this work, we assume a far weaker adversarial model requiring no sophisticated forensics whatsoever. We were able to access 21.49% of the phones merely by turning them on; they arrived completely unlocked. We were able to unlock another 4.82% of the phones in just a few hours by manually guessing the 100 most popular PINs and patterns. Looking back at the past two years of PropertyRoom auctions, we found 6 instances where police sold phones with sticky-notes

[1]https://www.propertyroom.com/
[2]https://cellebrite.com/
[3]https://www.grayshift.com/graykey/

containing the phones' PINs or patterns. Our results show that virtually anyone can gain access to a substantial amount of sensitive information from cellphones sold via police auction, without any special training, device, or software.

A longitudinal view of the auction ecosystem. In addition to our deep-dive analysis into the 228 phones we purchased, we also perform a longitudinal analysis of the cellphone police auction ecosystem. We crawled the PropertyRoom website to obtain approximately two years' worth of auction data. Our analysis shows that, over these two years, police departments across the US have collectively auctioned off over 33,594 phones at an average price of $16.55 per phone. Moreover, by manually analyzing thousands of photos included in PropertyRoom's auction listings, we find many instances of sensitive information readily available on the website for free, without having to win an auction. PINs, patterns, names and phone numbers of prior owners, evidence tags describing how the phones were obtained, and the names of law enforcement agents who collected or processed the phones, are all visible on stickers or sticky-notes attached to phones. Our measurements show that the leaking of sensitive information via police auction is widespread, longstanding, and sometimes lacks safeguards as basic as removing a sticker.

Contributions. We make the following contributions:

- We perform the first study of phones sold at police auction by purchasing and analyzing 228 phones from PropertyRoom.
- We show that an adversary with no forensics experience can gain access to 26.8% of phones by merely turning them on or trying the most common PINs or patterns.
- We thoroughly analyze the content of these phones, finding many instances of private and sensitive data, evidence of criminal activity, and data that would enable purchasers to re-victimize previous victims of identity theft.
- We perform what is, to the best of our knowledge, the first longitudinal analysis of police phone auctions, characterizing the economy and showing how longstanding practices divulge sensitive details about the phones' original owners and the police who processed them.
- We have disclosed our findings to PropertyRoom and other stakeholders and, at least at the time of this writing, PropertyRoom ensures that the phones they sell no longer contain personal information.
- We discuss potential mitigation measures that various stakeholders could take.[4]

Roadmap. The rest of this paper is structured as follows. Section II presents background and related work on police auctions, PropertyRoom, and prior forensics efforts. Section III describes our methods, including our phone collection and analysis protocols, and the legal and ethical concerns we addressed. Section IV provides an overview of the phones we obtained, and Section V gives an overview of the content stored on them. In Section VI, we dig deeper into the phones' contents and report on the criminal activity we were able to infer. Section VII presents our longitudinal analysis of two years' worth of phone auctions on PropertyRoom. In Section VIII, we discuss potential countermeasures, and we conclude in Section IX.

[4]Additional resources and contact information can be found on our project webpage: https://policeauctions.cs.umd.edu

II. Background and Related Work

In this section, we give an overview of police auctions, describe how PropertyRoom operates, discuss legal considerations of police auctions, and review related work.

A. Police Auctions

In the United States, police come into possession of various items throughout the course of their work.[5] After a criminal investigation concludes or when lost or stolen property is discovered, police are typically required to inform the rightful owner directly or via public posting (e.g., in a newspaper) that their item is available to be claimed. If the original owner does not claim it after some amount of time, the finder may claim the item if it was lost-and-found; otherwise, items become the property of the state or local government. For instance, New York state law [10] gives owners six months to claim property valued between $100–$499.99 and three years to claim property worth more than $5,000; finders then get three months to claim it. Once that window expires, the property may—and in some instances *must* [9], [40]—be put up for sale at public auction. The proceeds from these auctions tend to go to the respective local government or the police department that obtained them. These so-called police auctions are a common occurrence in the US; thousands of departments now partner with third party auction houses in order to reduce their logistical overhead. Chief among them is PropertyRoom.

B. PropertyRoom

PropertyRoom.com partners with over 4,300 police departments in the US to reduce the logistical burden of managing their own secure auction website. According to their website and a news article from 2009 [41], PropertyRoom operates as follows: PropertyRoom periodically visits partnered police departments and takes items for sale back to one of five processing centers [31]. PropertyRoom organizes the items into batches to auction, takes photos of them, and lists the auctions under one of the categories on their website, such as Jewelry, Boats & Planes, or the central focus of our paper: "Bulk Lots of Cell Phones"[6]. Each category is processed differently; for instance, most valuable jewelry is appraised. At the time we purchased phones from them, PropertyRoom asserted that each bulk lot of cellphones contained untested items sold as-is for parts. On learning this, we wondered: is

[5]Police auctions are not unique to the US; for instance, some UK police departments auction items on eBay (https://www.ebay.co.uk/str/sussexpoliceauctions). We focus on the US in this paper.

[6]https://www.propertyroom.com/c/electronics_cell-phones_bulk-lots

anyone verifying that these phones are wiped before they are sold?

The PropertyRoom website handles user accounts and online bidding using an ascending first-price auction with bid increments (thereby approximating a second-price auction). PropertyRoom also handles shipping and customer service with the bidders. Finally, PropertyRoom shares the proceeds of the auctions with the police departments whose items were auctioned off; in 2007, Bovid and Sparks reported that PropertyRoom kept 50% of the revenues [4].

Other police auction websites. We are aware of only one other auction website in common use by US police: GovDeals.com. Like PropertyRoom, GovDeals handles hosting, bidding, and payment processing of the auctions. Unlike PropertyRoom, GovDeals lists the identity of the department or agency selling the items. We crawled the GovDeals website to compare the number of agencies using GovDeals to those using PropertyRoom. In total, we identified 998 police departments, prisons, correctional facilities, and the like that had sellers' accounts on GovDeals. By comparison, PropertyRoom claims to have over 4,300 such partners. Also, we manually searched for auctions of bulk lots of cellphones sold by police departments on GovDeals and consistently found few, unlike PropertyRoom's steady supply shown in §VII. From this, we conclude that PropertyRoom is, at the time of our study, the most popular website in use for US police auctions.[7]

C. Legal Considerations of Police Phone Auctions

Before embarking on our study, we wondered: who is the rightful owner of the data on the phones? Are winners of the auctions legally allowed to look at the data? Do the original owners have a right to retain ownership? To answer these questions, we spoke with members of the Electronic Frontier Foundation who in turn discussed it with some of their lawyers. We summarize their analysis here.

Various state and local laws outline the attempts that must be made to return seized, stolen, or lost-and-found items to their original owners (or those who found them) and the time limits that owners have to do so. When this time expires, the items usually become the property of the state or local government, at which point the original owner is no longer entitled to redeem the property. Thus, when the police auction off an item, they transfer their ownership to the purchaser. Note that, normally, purchasing stolen property does not transfer ownership rights—even if the buyer did not know it was stolen. However, in the case of police auctions, ownership is transferred regardless of how the phone was obtained. Put another way: ownership is effectively laundered through the police.

As a result, the winners of the auction own the phones and all of the data on the phones. As an analogy, suppose one were to purchase a painting and later discover that inside the painting was a collection of handwritten letters from the original owner. *Ethically*, one might argue that the letters belonged to the original owner of the painting, but *legally* they belong to the purchaser.

However, ownership of the data ends within the confines of the phone. The Computer Fraud and Abuse Act (CFAA) still prohibits the new purchaser from accessing a remote service that they are not authorized to—and merely possessing cookies or passwords does not confer authorization. Continuing the analogy: if the letters contained detailed instructions on how to access a person's safe deposit box, then those instructions would belong to the purchaser but they would not be allowed to *use* them to actually access the box. In the case of a secondhand digital phone, if the new owner were to open a banking app that automatically logged into the previous owner's account, they would be legally obligated to log out.

Finally, there is one form of data that is *always* illegal to possess, no matter how one obtains it: Child Sexual Abuse Material (CSAM). We consulted with our institution's legal counsel, who informed us that we were legally obligated to immediately report any such material to law enforcement, if found.

What this analysis meant for our study was that, *legally*, we were allowed to possess and analyze the materials on the phones, so long as we followed strict methods ensuring that we did not violate the CFAA and that we identified and reported any CSAM we found (though we did not find any). We detail these methods in §III-A.

D. Related Work

Prior work showed that it is possible to obtain data from secondhand electronic devices by using sophisticated forensics toolkits. In their seminal work from 2003, Garfinkel and Shelat purchased 158 secondhand hard disk drives and developed various forensics techniques to extract and analyze 75GB from them [12]. Since then, forensics toolkits have become more advanced, with third-party companies developing zero-days to gain access to phones [45]. In 2016, Glisson et al. compared three such forensics toolkits to retrieve more than 11,000 data artifacts from 49 secondhand mobile devices sold on eBay and a pawn shop [15]. Similar forensics toolkits have been used to get data from USB storage devices [23], [1], memory cards [44], [47], hard disk drives [22], handheld devices [24], and smartphones [13]. In comparison with these prior efforts, our work shows that even an adversary with no sophisticated forensics tools can still gain access to a significant amount of data from phones sold via police auction.

Many studies acquired secondhand devices from diverse sources like eBay [15], [23], [5], computer stores [12], pawn shops [42], a Forbes 500 company [13], and various resellers [25], [46], [21]. Our work extends these efforts into the previously unstudied but critically important space of police auctions. Unlike these other sources of secondhand devices, phones from police auctions are more likely to have been involved in a crime, and are thus more likely to contain

[7]Conversely, GovDeals appears to be more popular for *federal* agencies auctioning off used equipment. A cursory look at these auctions indicated they more consistently wipe hard drives.

sensitive information that could be used for blackmail or re-victimization. Police auctions also introduce a third party not present in other studies' sources: the police and forensics teams who, as we will show, attach sticky-notes and stickers to phones that divulge PINs, patterns, and information about the phones' original owners.

We are aware of only one other cursory study of PropertyRoom, performed by Mosieur in 2016 [20], in which they purchased 10 phones and reported on how many were accessible and contained text messages, photos, and pornography. We perform a more thorough evaluation, detailing precisely the sensitive nature of the data on the phones, as well as a two-year longitudinal analysis of PropertyRoom auctions. As a result, we believe our work shows more fully the risks that police auctions pose to society.

III. Methods

In this section, we describe how we obtained phones, gained access to them, and extracted and analyzed the data stored on them. We begin by discussing how the legal and ethical considerations from Section II guided our approach.

A. Legal and Ethical Guidelines

Our study was approved by our Institutional Review Board (IRB) as a secondary data analysis study, as the data on the devices we obtained existed without our intervention. The IRB was primarily concerned with potential harm that could come to researchers, and how sensitive/identifying data would be handled and stored. Seeking IRB approval is a necessary, but not always sufficient, step to conducting ethical research. Our IRB team felt that they alone were not capable of addressing all potential concerns related to this project, and helpfully referred us to both our institution's legal counsel and our division of IT for further guidance.

Based on discussions with our institution's legal counsel, division of IT, and the lawyers' analysis discussed in Section II, we instituted the following rules:

No network access. Phones were not allowed to connect to any network, and could only directly connect to air-gapped machines. This ensured that we were not in violation of the CFAA, and mitigated IT's concerns that the phones may have had malware.

Automated checks for CSAM. Before researchers were allowed to manually look at any photos on a given phone, all of that phone's photos had to be automatically tested and cleared against a database of known child sexual abuse material (CSAM). Also, all researchers had to familiarize themselves with mandatory reporting guidelines for evidence of child abuse or neglect. This mitigated the risk of exposing the researchers to psychological harm, and ensured we knew the correct legal recourse if we did find such material.

By bidding on auctions and giving money to PropertyRoom and police departments, we are directly participating in the same ecosystem that this paper outlines the harms of. Establishing the severity and scale of this problem is a necessary step to resolving it, and we believe that the benefits from this research outweigh the marginal cost of our financial participation. In a similar vein, our analysis of the phones' data is done without the original owners' informed consent—the very act we are concerned that malicious actors might perform. This, too, is necessary in understanding and mitigating future data leaks. Our data management protocols were designed to ensure that our intervention caused no additional data leakage; in fact, our intervention effectively *removed* their data from circulation.

B. Obtaining and Processing Phones

We limited bidding to the "Cell Phones: Bulk Lots" category of phones on PropertyRoom. For these auctions, PropertyRoom bundled together multiple phones in the same auction lot. We actively bid on auctions during two periods of time: auctions that closed between November 11–13 2021, and auctions that closed between February 6–11 2022. We won almost all of the bulk lots of cellphones during these times.[8] Based on our analysis of the PropertyRoom auctions (§VII), we believe that concurrent lots often come from the same police department. Thus, by winning all of the auctions in a short period of time, it increases the chances of obtaining phones that may have been part of the same criminal investigation (indeed, this was the case; see §VI). However, *only* buying phones in a single batch risks biasing the results towards a small number of police departments; to reduce this bias, we purchased phones in two groups, separated by months. Collectively, we won 40 auctions, with winning bids totalling $4,245 USD (this excludes shipping costs and additional fees). From these auctions we received 228 phones (including two Android tablets), along with miscellaneous accessories. Apple iPhones make up 29.4% of our dataset (67 phones).

After receiving the phones but before turning them on, we took pictures of the fronts and backs of the phones, then cleaned them with a disinfecting wipe. We prevented the phones from connecting to a network by removing the SIM cards and, after turning the phones on, immediately enabling airplane mode and disabling location tracking.

C. Gaining Access to Phones

Some phones arrived locked by PINs, pattern locks, text passwords, knock codes, or a combination thereof. Sophisticated forensics tools can extract content from locked phones. Low-power attackers have a different tool at their disposal: guessing common credentials. For each locked phone, we manually iterated through a list of frequently used credentials [3], [29], [43], [28] (again locally, not via network connection) until we were locked out, the phone wiped itself, timeouts became infeasibly long to guess, or we exhausted 100 guesses of the credential type. We successfully guessed the credentials for 11 phones; see §IV for more detail.

[8]There was one auction in which we were outbid shortly before the auction closed.

D. Extracting and Analyzing Phones' Data

We conducted both automated data analysis of the phones' digital backups, and manual data analysis on the phones themselves.

Digital backups. To extract and analyze digital backups of *some of* the data from the phones, we used several open-source tools, including Android's `adb` [16], the libimobiledevice suite [26], and the Mobile Verification Toolkit (MVT) [2]. More sophisticated mechanisms exist; bootloaders and expensive tools like Cellebrite, for instance, are often able to reliably get digital copies of a phone's entire contents. Conversely, the techniques we used were limited; they tended to get each photo, text message, and contact from each phone, but they mostly failed at obtaining non-native application data. We chose to use these less-capable tools because they adhere to our "low-effort" adversarial model: they are easy, free, and require no training. Some locked or broken phones had SD cards, and others allowed us to mount the device and manually create copies of some files.

To mitigate potential leakage of the phones' data, we extracted all data onto an encrypted hard drive connected to an air-gapped laptop, on which we also performed our data analysis.

PhotoDNA. To automatically detect CSAM, we used Microsoft's PhotoDNA [27] service, which allows researchers and qualified organizations to check images against a database of known images of child exploitation. We created a PhotoDNA hash locally for each image, and sent that hash to Microsoft's servers for comparison to known images. PhotoDNA was able to hash 52,245 images (86%).[9] None of these images were flagged by PhotoDNA as known images of child exploitation. Only after checking each image against PhotoDNA did we allow the researchers to perform manual analysis of the phones.

Manual analysis. We complemented our automated analysis with manual analysis of data on the devices themselves; this is within our threat model of a low-effort attacker. This included navigating applications, reviewing communications, and investigating account settings. We stress once more that we only analyzed content stored or cached locally on the device; some applications such as email indicated that more content would have been available were the phone to connect to a network.

E. Disclosure

We disclosed our findings to PropertyRoom with a three-month embargo to allow them time to address the concerns raised in this paper. PropertyRoom acknowledged our disclosure and said they would review their policies and procedures, but did not engage further. Shortly thereafter, they paused selling new bulk lots of cellphones for approximately a month. When new auctions of bulk lots resumed, we successfully won all of them for one week and analyzed the phones, finding that they had been restored to factory settings. However, four phones had SD cards that had not been erased and contained photos and partial backups of the phones. We disclosed these additional findings to PropertyRoom, who did not reply. As of the time of this writing, descriptions for new bulk lot auctions of cellphones on PropertyRoom include: "Devices presented for auction have gone through our internal process to ensure personal information has been removed."

We also disclosed our findings to multiple organizations with ties to law enforcement in the US: National Sheriffs' Association, International Association of Chiefs of Police, Police Executive Research Forum, Major Cities Chiefs Association, DHS's Office for State and Local Law Enforcement, and National Computer Forensics Institute.

We have chosen *not* to try to reach out to the previous owners of the phones—nor to try to return the phones to them—for two key reasons: First, we cannot determine with certainty whether the person we believe used the phone most recently had rightfully owned it, or if they stole it from someone else; returning the phone to a thief risks re-victimizing its true owner. Second, some of the phones showed clear signs of violent criminal activity (see §VI); in the interest of the researchers' safety, we did not try to communicate with the previous owners at all. Instead, we destroyed each phone (and deleted copies of its non-aggregate data) after we completed analyzing it.

[9]The rest were malformed, unsupported image types, or too small.

Category	# Phones	% of Phones
All Phones	**228**	**100**
Accessible with User Data	**61**	**26.8**
Arrived Unlocked	49	21.5
Guessed Credentials	11	4.8
Credentials Given	1	0.4
Functional, Inaccessible Data	**107**	**46.9**
Locked Out	45	19.7
Wiped	12	5.3
Minimal Access	1	0.4
Exhausted Guess Space	9	3.9
Unreasonable Guess Timeout	40	17.5
Arrived Nonfunctional	**60**	**26.3**
Locked Out	2	0.9
Wiped	19	8.3
No Battery	5	2.2
Cannot Power On	21	9.2
Screen Broken	12	5.3
Requires SIM	1	0.4

TABLE I: Overview of the phone functionality and data accessibility for phones in our dataset

IV. Phone Dataset

In this section, we provide an overview of the phones in our dataset and their functionality (summarized in Table I).

Arrived nonfunctional. Of the 228 phones we purchased, 60 (26.3%) of them were not functional due to hardware issues. This includes phones that could not turn on due to hardware fault (21), phones that could power on but had broken screens (12), phones that neither included a battery nor was there a battery of the same size in our whole dataset (5), and phones

that would not operate without a SIM card (1). Also, 21 phones arrived wiped or locked and unusable without some intervention that was beyond the bounds of our methodology (connecting to WiFi, logging into an account, etc.).

Functional, but inaccessible data. Of the 168 phones that arrived in a functional state, we were unable to get full access to 107 of them using our limited means. 45 phones locked themselves down after too many incorrect guesses, requiring the phone to connect to a network to become functional again. 12 phones wiped themselves after we exceeded their guess threshold. 40 phones allowed us to continue guessing, but we stopped due to long timeouts between guesses. For 9 phones, we exhausted our list of popular credentials without finding a match. 1 phone had additional security settings that did not allow us to access anything on the device, despite it not having a screen lock.

Accessible with user data. The remaining 61 phones (26.8% of all phones we purchased) were functional and we were able to access the previous owners' data. 49 phones (29.2% of the 168 phones that arrived in a functional state) arrived with no lock screen protection whatsoever; merely turning these phones on gave us unfettered access to their data. This percentage largely agrees with a 2016 study that found that 35.4% of Android users in the US do not use lock screens [18].

Using a list of the most popular PINs and patterns (§III), we successfully guessed the login credentials of another 11 devices (10 phones and 1 Android tablet). Of these, we unlocked 2 on our first guess, 5 within 10 guesses, 9 in fewer than 20 guesses, and 2 in fewer than 40 guesses.

Finally, one phone was protected by an unpopular PIN, but stuck to the back of the phone was a sticky-note on which the PIN was written, along with a message indicating that the PIN had been obtained by GrayKey (see Phone 1 in §VI). Recall that the GrayKey forensics tool is commonly used by law enforcement. As such, we conclude that law enforcement gained—and unintentionally granted us—access to this device.

Collectively, these results show that an attacker can unlock a substantial number of phones without sophisticated forensics, or even many manual guesses.

Partial information. We were unable to fully analyze 167 phones: 107 due to their security setups, and 60 due to hardware issues. While we could not investigate these phones fully, 29 had some identifying information accessible by us for partial analysis. 9 of these phones had external SD cards (2 unlocked phones also had removable memory cards). 18 phones were locked, but had identifying information present on their lock screen in the form of notifications or emergency information. 1 phone allowed us to copy files from shared file system locations, despite the phone having a broken screen. Finally, 1 phone had the name of its former owner, their attorney, and the trial district on a sticker pasted on the back of the phone. Our analysis in the following sections includes these phones, as well.

V. Phone Content

In this section, we investigate the communications, activities, behaviors, and sensitive content present on the phones we purchased from PropertyRoom, to better understand what information police are selling to the public.

A. Communications

Communication is a two-way street. The phones we bought contain more than the private communications of one person; they have information from *everyone else* the device communicated *with*. Our digital backups included text message and call histories for 58 unlocked Android and Apple devices.

Text messages. SMS and MMS messages are the most private communications in our dataset, as we can see *what* is being communicated with *whom*, and *when*. In addition to text, we can also see any attachment sent via MMS. In total, we extracted 100,075 individual text messages: over 10,000 text messages from each of five phones, between 1,000–10,000 messages from 12 phones, 100–1,000 from 14 phones, and 1–100 from 17 phones.

Phone calls. Our phone call records include the date, time, duration, and the phone number of the other party for each call. Apple devices also included a history of video calls. One phone had over 9,000 call records, while two phones had exactly[10] 2000 each. Fourteen phones had 500–1,000 records, eight of which kept 500 exactly. Sixteen phones had records for 100–499 calls, and another sixteen had fewer than 100. Collectively, these backups contain records of 25,365 phone calls. Six phones have records of calling 911, notable as the phones themselves were obtained via the police.

Emails. Emails are another rich source of communication. Even though we did not allow the phones to connect to the email servers, we were able to view cached emails on most unlocked devices. These emails included receipts, medical records, and communications with lawyers about the owners' open legal cases. We were also able to extract email metadata from 2,818 emails across 21 Android phones. The emails were dated between May 2015 and August 2020, and the metadata includes 997 unique email addresses: 44 in the email's `To` field, 574 in the `From` field, and 622 in the `Reply-To` field.

Additional communications. The data presented here only scratches the surface of communications accessible in our dataset. One phone had 460 calls in its backup, but elsewhere on the phone saved a 39-page phone bill with a record of an additional 1,441 phone calls. Others had locally stored voicemail messages. Many phones had third-party messaging apps with even more visible content, including WhatsApp, Facebook Messenger, TextFree, TextNow, and Telegram. Our backup tools did not allow us to extract these messages, but we were able to manually view them on the phones.

[10]We believe phones with exactly 2000 and 500 records stored only the most recent calls up to that number.

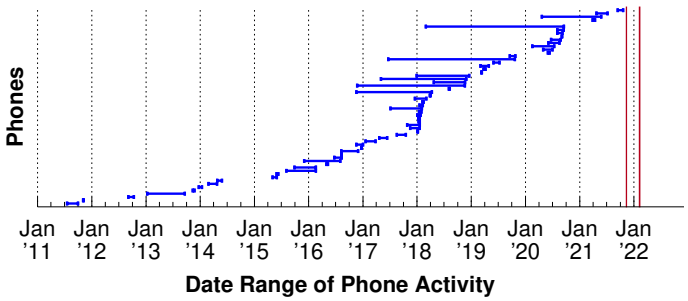

Fig. 1: Ranges of time for when each phone was in active use. The red lines represent our two bidding periods.

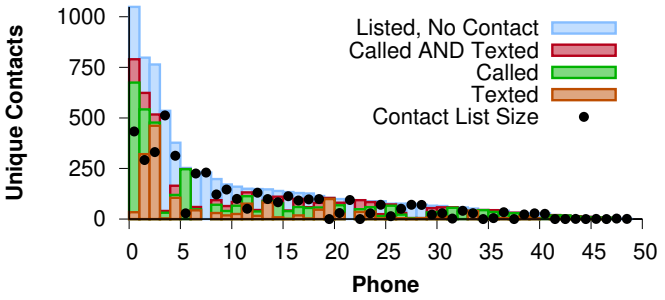

Fig. 2: Stacked histogram for the expanded contact set of each phone. The difference between the black dot (all phone numbers in the "Contacts" app) and the height of each bar is the number of phones contacted that would be missed by only looking at the "Contacts" application.

B. When Were These Phones Used?

After leaving possession of their previous owners, the phones had to pass through the police, PropertyRoom, and shipping, before arriving in our physical possession. Communication timestamps establish a window of time when each phone was actively in use, and allow us to estimate how much time elapsed between the previous owner losing possession of the phone and us gaining it. To this end, we use text and call histories when available, as they are unlikely to contain events synced from other devices; we use other time indicators from the phone when necessary.

Figure 1 shows the active time ranges established for the phones we collected. The two solid vertical lines on the right represent our bidding periods in Nov. 2021 and Feb. 2022. Phones are sorted vertically by the most recent timestamp in their activity range, allowing us to see the distribution of time-of-use to time-of-sale. The phones in our dataset were used between 2011 and 2021, with the largest clusters in early 2018 and mid 2020. This shows that phones released from police departments contain information ranging from months to a decade before being sold: wide-ranging data that a malicious purchaser could mine.

C. Phone Contacts

Next, we measure the number of contacts on each phone to better capture the number of people whose data is being sold by the police. We start by looking at the distribution of the 5,484 contacts explicitly listed in "Contacts" applications on the phones. Two phones had over 600 contacts; seven phones had 200–300; six phones had 100–200, ten had 50–100, fourteen had between 10–50, and seven phones had fewer than 10 contacts.

We find that "Contacts" applications under-represent the number of *other* phones each of the phones we purchased have communicated with; many phones call and text numbers that are not tied to a named contact. We calculate a more representative contact list by taking the union of all phone numbers from call histories, text messages, and "Contacts" apps[11]. Figure 2 visualizes our expanded contact lists. Each phone has a stacked histogram representing the number of unique phone numbers only called, only texted, both called and texted, and numbers present in the "Contacts" app that were neither called nor texted. The black dot on each bar represents the total size of the "Contacts" app list for that phone. A greater difference between a black dot and the top of its histogram implies more under-representation were one to ignore unlisted phone numbers. Overall, we found 7,151 unique phone numbers in our expanded contacts lists. For 21 phones, the expanded list more than doubled the number of known phone contacts, and eight of those phones had expanded contacts but zero phone numbers in their "Contacts" app.

In summary, the phones we purchased at police auction leak communication data for an *order of magnitude* more individuals than the number of phones purchased.

D. Images

Here, we demonstrate the scope and severity of sensitive photos sold on police-auctioned phones. We manually analyzed all images stored in gallery applications and MMS attachments, and classified sensitive ones into the categories shown in Table II. The table shows how many *phones* had images of each type. Many phones had photos depicting drugs and drug use, conversations of screenshots, and photos of young children or family members. We identified 19 phones with *residual* images, that the previous owners attempted to delete but were still visible in settings or trash folders. Finally, we identified 18 phones with nude images.

Glisson et al. [14] similarly found instances of sensitive photos on phones they purchased from eBay and pawn shops. Our findings show that phones purchased from police auctions are especially sensitive, as they are evidently more likely to contain pictures pertaining to criminal activity. We return to this in §VI.

E. Browsing History

Browsing history can reveal a wide array of information on activities that the user may wish to keep private. Browsing

[11]For consistency, in this comparison we consider only contacts with phone numbers that are 10+ digits long.

Image Category	# Phones
Sexually Suggestive	26
Explicit Nudity	18
Drugs	16
Drug Use	6
Weapons	8
Piles of Money	9
Children	28
Communications	20
Marked for Deletion	12

TABLE II: Image categories of interest, and how many phones had at least one image including that content.

Website Category	# Phones
Ecommerce	35
Pornography	31
Adult Themes	18
File Sharing	8
Drugs	3
Questionable Activities	3
Deceptive Ads	1

TABLE III: Number of phones in our dataset with web histories that show the browsing of sensitive websites, according to Cloudflare's domain categories [6]. The three "Questionable Activities" websites comprised (1) black market financial statistics, (2) pornography, and (3) a cult-like organization.

histories also contain page titles, paths, and parameters that can reveal even more specific information about page interactions.

We extracted 2,511 unique domains browsed from 51 devices. We used Cloudflare's website categorization [6] to classify each domain name, and counted the number of phones that browsed at least one site in those categories. Table III shows the results for the seven categories we identified as being particularly sensitive. We observed Ecommerce activity for 35 of the 51 phones. The phones in our dataset track pornographic consumption habits for 31 individuals, and 18 phones browsed other websites that Cloudflare considers to have "Adult Themes," which include websites advertising escort services. Finally, we saw phones browsing file sharing websites (8), websites about drugs (3), sites that Cloudflare considers as having "Questionable Activities" (3), and one phone browsing a website associated with deceptive advertising.

F. Locations

While our sample was purchased during two short windows of time and may not be representative of all phones sold through PropertyRoom, we can still gain insight into which states are participating in this ecosystem. Table IV summarizes where the phones in our sample came from, using three tiers of confidence.

We identified 40 phones with high-confidence location information, such as: home or work locations saved in maps applications, addresses in the browser's auto-fill settings, documents or IDs with the primary user's home address on them, or evidence stickers on their exterior saying what state the police department resided. An additional 33 had other, more loose

US State	Phones, Strict	Phones, Strict + Loose	Phones, Projected (# Auctions)
California	2	8	25 (5)
Florida	3	7	23 (3)
Georgia	2	5	16 (3)
Kentucky	4	7	27 (3)
Maryland	1	2	6 (1)
Michigan	1	1	5 (1)
New York	4	14	35 (7)
Ohio	1	4	11 (2)
Oregon	1	1	5 (1)
Washington	21	24	48 (9)
Ambiguous			27 (5)

TABLE IV: States where the phones in our dataset were primarily used and collected. We classify the phones into two tiers based on the specificity of available location data. We then project the location of known phones onto phones with no known location sold together via the same auction.

indicators of location, including: maps and internet search histories, weather applications, text messages and emails, location-specific phone applications (e.g., local transit apps), and public records for the suspected primary user. We also incorporated geographic metadata present in 2,621 images across 30 phones in this category. In total, 73 phones provided some degree location information about themselves.

The majority of phones had no visible indicators of where they came from. However, to the best of our knowledge, phones bundled together in the same auction are sold from the same police department. We can use the 73 phones with known locations to infer the locations of unknown phones that were sold alongside them. This accounted for 35 of our 40 auctions, and 88.1% of all of the phones we bought.

G. Sensitive Data

We close this section by analyzing the most severe examples of sensitive data found on the phones, bringing together data from communications, photos, documents, settings, and applications. We identified 31 phones in our sample that had some kind of severe information leakage, defined as the leakage of social security numbers, credit/debit cards, bank account numbers, government-issued identification, passwords, and other authentication information. We break down each of those categories below, and summarize our results in Table V.

Social Security Numbers. A Social Security Number (SSN) is a nine-digit identification number, often used for authentication in financial contexts. They are highly sought after by identity thieves, enabling them to steal money or open fraudulent financial accounts. Two phones had an SSN belonging to their respective owners: one on a photo of a bank form, and the other on a handwritten note card. Three phones had SSNs we believe belong to victims of identity fraud. More information on those phones and their victims can be found in §VI.

Identification. We identified 12 phones with photographs of government-issued IDs. Five unique passports were present across 4 phones: 2 from Germany, 2 from El Salvador, and

Sensitive Data	# Instances	# Phones
Social Security Number	34	5
Identity Theft (Credit History)	30	2
Identity Theft (Telegram Chatroom)	1	1
W2 (USA Tax Form)	1	1
Other Documents	2	2
Credit/Debit Card #	25	11
Stolen (Fraud Website)	11	1
Stolen (Telegram Chatroom)	1	1
Photo/Document	8	6
Browser Autofill	3	3
Text Message	2	2
Bank Account/Routing #	20	8
On Check	15	6
Photo/Document	4	4
Phone Application	1	1
Identification	29	12
Passport	5	4
Driver License	14	6
Firearm Permit	2	2
Other Govt. Issued ID	8	5
Username & Password	194	16
Browser Autofill	189	16
Photo/Document	5	2
Safe Combination	1	1
Security Question Answers	1	1
Total	304	31

TABLE V: Types of sensitive data, the number of unique instances of that data, and the number of unique phones that contained at least one instance of that data.

1 from Romania. Six phones had a total of 14 unique US Driver's Licenses. Two phones included permits allowing their owners to carry a firearm. Five phones had 8 other government-issued identification cards: 5 US state-issued ID cards (equivalent ID to a driver license without enabling its owner to drive), 2 German ID cards matching two of the passports, and 1 USA employment authorization card.

Financial data. While most applications and documents masked credit/debit card numbers to show only the last 4 digits of the card, there were 25 unique 16-digit card numbers present on 10 phones. Eight card numbers were visible in photos, 2 cards shared via text, and 3 cards were visible in browser auto-fill settings. Full details on twelve stolen credit cards were also present on two phones; see §VI for greater detail.

We counted the number of bank accounts for which we could see the bank routing and account numbers in full. We identified 15 account numbers visible on photos of checks, which also often included the names of the payer and recipient. There were also four photos of documents with bank account and routing numbers, and one pair visible from a phone application.

Security credentials. Finally, we recorded examples of username/password pairs, or other authenticating information. Five account pairs were visible on handwritten notes or photos. 189 pairs were visible on sixteen phones via the phones' system and browsers' auto-fill settings. One phone had a photo of an account's recovery questions and answers. Finally, one phone had a photo of a note with a safe combination at a retail store.

Collectively, these results show that the phones available on police auctions contain highly sensitive information that an adversary—even one without any forensics expertise—can use for intelligence gathering, identity theft, blackmail, and so on. Next, we investigate whether the data also shows evidence of criminal activity.

VI. Criminal Activity

Phones purchased from police auctions are more likely to have been involved in a crime than secondhand phones purchased from other retailers. It follows that police-auctioned phones are also more likely to have data related to crime itself: data that risks re-victimizing victims, exposing police procedures, and creating opportunities to blackmail the criminals or people they knew.

We analyzed all communications and content on each phone to determine if there was any evidence of criminal activity, and in this section we present 15 phones that showcase the breadth of our findings. Table VI contains an overview of the phones discussed in this section.

As we are not lawyers, we do not claim to know the specific crimes, nor whether this data would constitute admissible evidence. However, some signs of criminal activity were obvious; several phones, for instance, had court documents with explicit charges stored as PDFs. Other phones expose highly sensitive data about victims of crimes, indicating that police auctions pose the risk of re-victimization. We also searched for each phone's serial number and inferred owner in court record databases such as PACER, LexisNexis, and state and local databases. This search was successful for some phones (some of which we discuss in this section), but we were not able to find public records for most phones.

Identity theft and credit card fraud. Phone 1 arrived to us with a note taped to its back. The note had a numerical identifier, the phrase "Gry keyed" followed by a date, and a 4 digit number. GrayKey is a forensics tool used by law enforcement that is capable of cracking a phone's PIN. The 4 digit number unlocked the device, which would have otherwise remained locked as the number was not in our list of 100 frequently used PINs.

This phone contained photos of two credit cards, nine bank account and routing numbers, a photo of a computer screen (with a username and password) detailing a medical encounter, three drivers licenses, and one state-issued ID card with a photo and address. A text message thread on the phone was more concerning: the owner sent pictures of 3 money transfer receipts to another individual. In return, the other person sent the owner screenshots, PDFs, and HTML files of 24 Experian and TransUnion credit histories. These documents listed names, employment histories, addresses, phone numbers, family members, bank accounts[12], loans, and credit cards. We believe these were 24 victims of identity theft at the hands of the owner of this phone. Finally, 23 of the documents listed full, unmasked SSNs.

[12]The last 4 digits of the bank account numbers were masked.

Phone(s)	Criminal Activity
1, 2	Phone owners knew each other and their phones contained stolen Experian and TransUnion credit histories for 24 and 8 victims of identity fraud, respectively. All but one victim had their Social Security Number exposed, and another victim's information was present on both devices, which sold in different auctions. Phone 1 was initially locked, but broken into by police using the GrayKey forensics tool, and a note was left on the back of the phone giving us the 4 digit number needed to unlock the phone and access the stolen credit histories ourselves.
3	Contains 11 stolen credit cards, info on their owners, and evidence of stolen cards being used to buy goods and travel.
4	Owner was a member of a Telegram group chat that offers paid tutorials for committing fraud. One victim's SSN, credit card, and personal information were distributed for free to advertise the tutorials' effectiveness.
5	Owner was convicted for "commercial sex abuse with a minor." We believe they were caught in a sting operation, and the phone we possess shows the procedure that law enforcement agents used to catch them.
6, 7, 8	All three phones belonged to sex workers operating in the same city for the same brief period of time. The phones contain passports for the individuals, and communications with clients.
9, 10	These phones were owned by the same individual. Court documents on one phone show an associate was arrested for vehicle violations, and the owner was arrested for possessing a stolen modified firearm, methamphetamine, and heroin. A witness statement included in one document says the owner was a drug dealer.
11	Has court documents showing two individuals arrested for possessing methamphetamine and drug paraphernalia.
12	The owner of this phone was a member of a prominent violent gang in the United States. One text conversation includes details of a gang-related murder, and a photo on the phone shows an associate was arrested for murder. Public records show that the owner of the phone themself was a victim of homicide by someone in their contact list, some time after this phone was used.
13	Contains no evidence of violence itself, but after its use the owner and an associate were both convicted of murder.
14	Has multiple applications installed that imply a pattern of stalking and/or harassment.
15	Latest voicemails and SMS messages on this phone indicate that it was stolen, and threatened the thief to return it.

TABLE VI: An overview of notable criminal or suspicious activity found on the phones in our dataset, on court documents present on the phones, or in publicly available records. More details on each phone can be found in Section VI.

Phone 2 also had SSNs, names, addresses, and phone numbers for 8 victims stored in the phone's note-taking application. Signs indicate the owners of phones 1 and 2 were working together: one victim was shared between both phones, they had mutual contacts, and phone 1 called a number used as a Facebook login ID on phone 2. Phone 1 also had a text message arranging travel to meet with the owner of phone 2.

Phone 3 had a photo of a website marketplace for stolen credit card numbers. The page showed a username and a purchase of 90 credit cards, 11 of which were visible on the page and included full 16 digit card numbers, names and addresses, and security codes. Ten of the credit cards had not yet expired when we received the phones from PropertyRoom (though we did not attempt to verify whether they had been frozen). Emails on the phone show a wide array of credit cards being used to purchase expensive goods and travel.

Phone 4 was a member of a group chat on Telegram that sold tutorials for committing: USPS insurance fraud, physical credit card cloning, abusing financial mobile apps, COVID-19 small business loan assurance fraud, and tax return fraud, among others. Screenshots of payouts with sensitive information redacted were used to advertise the tutorials. One victim's SSN, credit card info, name, phone address, Apple username/password, IP address, and browser user agent string were provided unredacted by the group manager, as a show of goodwill to entice group members to pay for more.

Originally, we had hypothesized that police departments were wiping (or at least not selling) phones they knew to contain victims' data. Surprisingly, not only do they sell such phones, but in some cases they make it *easier* to access the data on them. The PIN for phone 1 was written on a note that stayed on the phone when it left police custody, when PropertyRoom took pictures of it for the website (see §VII), and even when it arrived to us after winning the auction. In effect, the police broke into the phone for us, giving us easy and *legal* access to credit histories of 24 people who had already been victims of identity theft.

Police procedure. Public records show that phone 5's previous owner was arrested for "Commercial Sex Abuse with a Minor" on the same day and in the same location as the activity on the phone, and was later found guilty. The phone has a text message thread where the owner knowingly solicited sex from someone claiming to be a minor, arrived at a predetermined location, and ended with a text from the other party saying only "Test." Due to the timing of the messages and arrest, we believe this may be evidence of a sting operation where law enforcement agents posed as a minor. If so, this phone contains the procedures those agents used to persuade and catch a criminal, details that could diminish the effectiveness of those techniques in the future if they were made public.

Sex workers. Phones 6, 7, and 8 belonged to three sex workers operating for a brief time in the same city. All three phones shared contacts, communicated with each other, and shared photos between them. The phones contained nude photos, as well as three passports and two state ID cards for their prior owners: two German and one Romanian. Emails show advertisements purchased on escort websites. The three

phones called and texted with 223 unique phone numbers, with even more conversations with clients visible on third party messaging apps. These phones' content not only poses a risk to the three owners, but the conversations and contact information of their clients could have been used for extortion or blackmail.

Court documents, public records, and drugs. Some phones had explicit proof of crimes that their owners were accused of in the form of court document PDFs downloaded to the phone. Phones 9 and 10 were owned by the same individual, and have documents for them and their associate. The associate was already incarcerated and facing additional charges for improperly driving a vehicle. The other document was a determination of probable cause summoning the owner to court, facing charges of possessing a stolen and modified firearm, and of possessing methamphetamine and heroin. A witness statement included in the document claimed that this person was a drug dealer. Phone 11 similarly had legal documents explicitly spelling out charges related to drug possession, and many other phones had evidence of drug dealing but lacked court documents alleging explicit charges. One final phone ended activity with the owner checking into a drug rehabilitation program. Public arrest records later show that the owner and an associate they contacted were arrested in a fentanyl bust years later.

Violent crime. The owner of phone 12 was a member of a large violent gang in the US. The phone had a photo of a booking for an associate who was convicted of murder, and a conversation discussing details about another victim of gang violence. Public records show that some time after the phone was in active use, the owner was murdered by a named contact in their phone. Phone 13 has no discussion of violence on the phone itself, but the owner and an associate named on the phone were both arrested years later for second-degree murder.

Harassment and stalking. Phone 14 had multiple applications installed indicating a pattern of harassment or stalking. These included apps for enhancing photos and audio collected from a distance, a "lie detector," an app for detecting hidden cameras, and an app for detecting or preventing wiretapping of phone calls. The phone's web history also had searches for location and other personal information about one individual, and searches for tools that enable SMS bombing.

We compared the lists of installed (and in one case, deleted) applications from the phones we purchased to lists of known stalkerware [7] and spyware [19], [11] applications. No phones had known stalkerware, and three phones each had one spyware app.

Stolen or lost phones. The arrest of an owner is not the only means by which police can gain possession of a cellphone. The phone may have been submitted as lost-and-found property, or the previous owner may have had their phone stolen by a third party who was later arrested. We witnessed evidence of the latter; the most recent two text and voicemail messages on phone 15 implied that it had been stolen, and were threatening the thief to return it.

At the time of our study, PropertyRoom auction descriptions warned that the devices purchased may be nonfunctional due to "identification of this item as stolen on a telecommunication carriers record." Each cellphone has a unique fingerprint in the form of an IMEI number (or equivalent). The Global System for Mobile Communications (GSMC) maintains a database of IMEI numbers for stolen or lost phones [17]. The US-based cellular trade organization CTIA provides a public interface for consumers to check if their IMEI was previously reported as lost or stolen [8]. Ten of the 207 phones in our dataset with legible IMEI numbers were reported as lost or stolen according to CTIA. Three were unlocked, and two were locked but had SD cards with data that we were able to extract. These phones stored resumes, images of full nudity, a credit card, bank account information, and documents describing former arrests. We conclude from this that users rarely report stolen IMEI numbers and, even when they do, they frequently lack protections from even a low-effort adversary.

VII. Longitudinal Measurement of Auctions

In this section, we analyze two years of auctions on the PropertyRoom website. Where our results in the rest of the paper take a deep dive into the lots of phones that we purchased from PropertyRoom, here we take a broad view over *all* auctions over a two-year period.

A. Methodology and Dataset

We crawled the PropertyRoom website to obtain information about each auction spanning approximately two years: March 5, 2020 [32] to February 28, 2022 [38]. We chose a two-year period somewhat arbitrarily; we wanted a long enough period to be broadly representative, but did not want to overburden the PropertyRoom websites with more crawling. The information on each auction webpage includes the auction's title, winning bid, category (e.g., "Electronics: Bulk Lots"), and the pseudonymous IDs of the sellers and winning bidders, In total, this comprised 560,020 auctions across all categories (not just cellphones) and all sellers (not just police).

From these, we filtered specifically for the seller ID for police[13] and the category ID for cellphone bulk lots.[14] There are multiple categories in which police sell phones, but we limit our analysis to bulk lots as we believe they are more likely to contain phones with previous users' data. This resulted in 5,241 auctions[15]. Each auction on PropertyRoom has one or more pictures of the items; we downloaded all of them for the police-sold cellphone bulk lots.

Next, we filtered out re-listed lots. Some lots are auctioned off multiple times, possibly because there were no bidders or the winning bidder did not pay. In such cases, PropertyRoom reuses the photos; we filter out redundant lots by comparing

[13]PropertyRoom uses a single seller ID (1) for all police sellers.

[14]Category ID 2029.

[15]Almost all of the bulk lots were sold by police; the remaining 39 ($<$1%) were sold by cellular accessory stores.

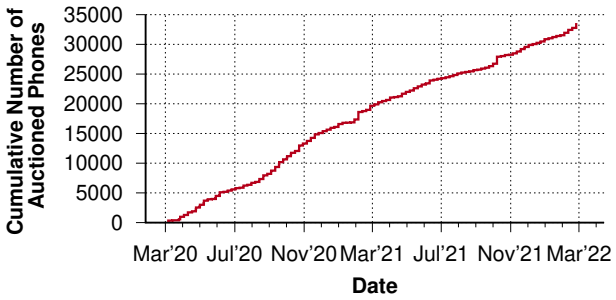

Fig. 3: Cumulative number of police-sold phones auctioned within bulk lots on PropertyRoom, March 2020–March 2022.

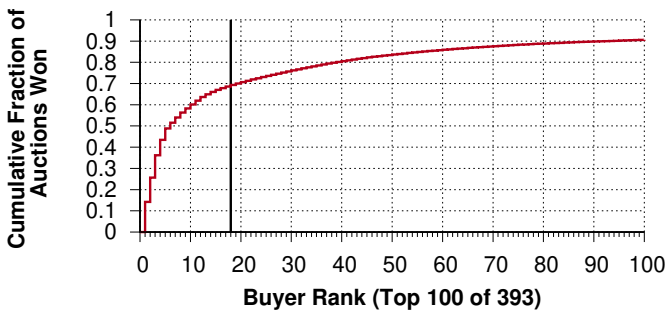

Fig. 4: Fraction of the 4,940 auctions won by the top 100 buyers. The top-six buyers collectively purchased 51.5% of all of the police-sold bulk lots of cellphones. (We were the 18th ranked buyer, indicated by the solid black line.)

hashes of the images and removing all but the final lot any images appear in. Collectively, this resulted in 4,940 unique bulk cellphone lots sold by police over this two-year period.

B. Phones Sold

First, we investigate the number of phones sold by police in bulk lots over this two-year period. Each auction title includes the precise (e.g., "6") or approximate (e.g., "10+") number of phones in each bulk lot. To estimate the number of phones, we parsed out this number, ignoring the "+". This gives us a lower bound on the number of phones sold; for instance, one auction [39] has 25 phones but only lists "10+" in its title. There are other potential sources of inaccuracies; for one of the lots we purchased, we received a phone that was not originally shown on the website.

In total, over these two years, we observed 33,594 phones that were once in police custody being auctioned on PropertyRoom. Each lot had on average 6.8 phones (median 6), with as few as 2 and as many as 30 [33]. Figure 3 shows the cumulative number of phones over time, indicating that there is a steady flow of phones. We speculate that PropertyRoom maintains a mostly fixed rate of phone sales so as not to allow the supply to exceed demand.

If the set of phones we purchased are representative of the broader population of phones, then we can estimate that over the two-year timespan: 7,219 phones would have arrived unlocked; 1,619 phones would have had easily guessable credentials; 4,569 would have had sensitive information (Table V); and 1,475 would have been blocklisted in the CTIA.

C. Money Spent

The total winning bid amounts over this two-year period was $556,008.92 (excluding the duplicated auctions), with an average of $112.55 per lot and $16.55 per phone.[16] The revenue per lot has remained roughly constant over the two-year window we studied.

This is a considerable sum, but the total revenue of *all* police-sold auctions on PropertyRoom during this time was $51,181,495; cellphone bulk lots constituted only 1.1% of this total.[17] In 2007, Bovid and Sparks reported that PropertyRoom receives 50% of auction revenues [4].

There are several other categories of note that also contain computing devices: Laptops (total police-sold revenue $909,324), iPhone & iPod ($689,572), Bulk Lots & Other Electronics ($435,511), Smartphones & Cell Phones ($424,789), and iPads & Tablets ($341,799)—representing a total revenue of $2,800,995. We did not investigate nor bid on any items from these categories, preferring instead to focus on the bulk lots of cellphones in particular. However, we believe these other categories also merit study to detect whether they have any sensitive materials.

D. Who Is Buying These?

The 4,940 unique auctions were won by 393 distinct buyers (including us: we bought all of our lots under a single buyer ID). Figure 4 shows the cumulative fraction of auctions won among the top 100 bidders. A small set of bidders won most of the auctions; the top buyer purchased 703 (14.2%) of the auctions for a total of $61,288.04, and the top six buyers collectively purchased 2,545 (51.5%) of the auctions.

PropertyRoom also provides information about the shipping city and state of the winning bidder. The 393 buyers we observed cover most of the US, spanning 40 states and Washington, DC. This shows that the dissemination of potentially private and sensitive data is not limited to any one region.

E. Photos of Auction items

Recall that one of the phones we purchased had a sticky-note attached to it with the phone's PIN. We sought to understand whether this was a one-off, or if divulging of information about the phone or its owner occurred in other auctions, as well. To answer this, we manually inspected each of the 15,760 unique photos from our two-year window of police-sold, bulk cellphone auctions. Specifically, we looked for any leaks of the private information stored on the phone. These pictures would have been available to bidders at the time of auction.

[16]The median price per lot was $100.02 and the median price per phone was $15.50.

[17]The two categories with the highest revenue—"Cars, Trucks, Vans" and "Heavy equipment and trailers"—constituted 42.0% and 25.8% respectively.

1) PINs and Patterns: We identified six auctions (including the one we won) that had information that unambiguously showed how to access the phone. These comprised four 4-digit PINs (including the one we purchased), one 6-digit PIN, and one 6-digit swipe pattern drawn onto a sticky-note attached to the phone. It was clear these were PINs, as most of them were clearly labeled "Passcode".

2) Information about Phone Owners: Beyond access information, other personal information was also included on many phones. We observed 40 phones with messages attached to them comprising a phone number. Typically, these appeared to have been placed there by the owner. We also saw 14 phones with messages containing what appeared to be the name of the owner. Finally, we saw one phone that had two pictures taped to the back of a family of two adults and three children. These are cause for concern as they each potentially identify the owner of the phone.

One phone [34] had a sticker indicating that it was the property of Harbor Regional Center in California, a care facility for those with developmental disabilities. We did not purchase that lot, but if the phone had data on it, it could potentially risk exposing patient data.

3) How Phones Were Obtained: The pictures of the phones also demonstrate the broad ways in which police can come into possession of cellphones that they auction. We identified multiple phones that had been turned in to lost-and-found. One such phone [35] had a sticker indicating that it had been found at LAX airport; LAX's policy[18] is to hold lost materials for 90 days and, if unclaimed, to auction them on PropertyRoom. We also identified phones with stickers noting that they had been stolen from a mall [36].

4) Phones Booting: PropertyRoom made a point to note that the items are only sold for parts, that the items are untested, and that the activation status has not been tested. However, we found 16 phones that were turned on or in the process of booting while the photos were being taken.

5) Insight into Police Practice: A large number of phones had stickers or writing on them from police. Many of these appeared to be innocuous, comprising barcodes or "item numbers" that do not obviously tie them back to any particular case or person. However, others had evidence stickers that provided more detailed information, including the name of the officer who entered the item into evidence. Many phones had stickers and notes from the forensics teams, indicating who processed the phone and the status of the forensics efforts. For example, in one lot [37], one phone had a note saying "SIM dumped. Phone in lock. Unable to defeat", and another had a note saying "Phone & Sim dumped". Finally, we note that some photos showed sound police practice. We found dozens of lots—all apparently from the same department—with sticky-notes noting which phones had been "Wiped".

VIII. Possible Mitigations

Here, we discuss steps various stakeholders could take to mitigate the risks posed by police auctions of cellphones.

[18]https://www.flylax.com/lost-n-found

Police departments. Police departments could wipe phones before selling them or, better yet, destroy them and not sell them at all. The loss of revenue would be small (in §VII-C, we estimate bulk lots of cellphones to constitute only 1.1% of police auction money), and the benefits to protecting citizens would, in our opinion, outweigh it. At the barest minimum, police should consider removing stickers and notes from the phones before releasing them to PropertyRoom, especially if those notes contain the PIN or pattern to unlock the phone as determined by sophisticated forensics tools beyond those available to the general public (as in §VI).

Legislatures. Governments must ultimately consider if the monetary benefit from selling phones in police possession outweighs the risks to everyone involved, especially if it enables victims of crimes like identity theft to have their stolen information sold to another person who could abuse it. At the federal level, entities are already required to take reasonable measures to prevent unauthorized data access or use when disposing of devices that contain consumer information [30]. State legislatures should consider analogous regulations to prohibit the sale of devices in police possession that store personal data. While our paper only investigated auctions in the United States, our recommendations are applicable to anywhere in the world where unclaimed property is auctioned by police.

PropertyRoom and other auction houses. Arguably, sensitive information should never leave a police department's evidence room in the first place, but pragmatically speaking, auction houses like PropertyRoom are in a unique position to handle the wiping or destruction of phones from many police departments. After our disclosure and as of the time of this writing, PropertyRoom appears to agree that they are in a position to act: they have since adopted an "internal process to ensure personal information has been removed" from all cellphones sold in bulk lots (§III). It is not yet clear if this will be a permanent or universally adopted solution amongst other auction houses; it is possible that taking on the responsibility of wiping the phones' contents could increase their legal exposure, particularly if they were to wipe incorrectly.

Phone manufacturers and application developers. Certain phones and applications had defense mechanisms that complicated our analysis. Limiting the number of incorrect guesses made it more difficult to guess the credentials to many locked phones; blocklisting common PINs/patterns would have made it even more difficult. Some applications would not allow us investigate and change account settings from within the app itself, and instead required the user to re-authenticate in a web browser. This could help prevent an attacker with physical access to an unlocked phone from gaining all available account information. While these techniques may not thwart a more powerful adversary, they raise the bar enough to preclude a much larger population of potential attackers from gaining access to highly sensitive materials.

Phone auction winners. Looking through the contents of the phone in a non-controlled environment can risk violating the CFAA or exposing the user to psychologically harmful photographs. In §VI, we found that some phones belonged to people with histories of violence, and many phones offer location tracking features that could reveal the buyer's location to the phone's previous owner. We recommend not purchasing phones from police auctions, but if one decides to, it is safest and arguably most ethical to wipe the phones immediately upon receiving them.

Original owners of the phones. The original owners of the phones have several mitigation steps they can try to take. First, users should choose nontrivial PINs or patterns. If one's phone is stolen or lost, they would be well advised to check various online databases and newspapers for reports of unclaimed property (see §II). Barring that, more recent phones have the ability to remotely wipe a lost or stolen device; users should employ these, as well as report their phone's IMEI as stolen. While it is encouraging that some applications have the ability to require passwords before permitting access, it is also likely that an adversary with access to the phone would have other means by which to recover or guess the password. Users whose phones have been taken should consider changing all of the relevant passwords and freezing financial accounts.

IX. Conclusion

In this paper, we performed the first thorough analysis of the security and privacy risks involved in police auctions of cellphones. Our results collectively show that police auctions represent a unique point in the space of secondhand computing devices. Phones purchased off of police auctions are likely to contain sensitive personal information as well as criminal activity, which risks blackmail of the person who committed the crime as well as re-victimization of the original targets of the crime. Moreover, by analyzing two years of PropertyRoom auctions, we found many instances where information from the police themselves was included, including notes from forensics teams, cracked PINs and patterns, identifying information about the phone's original owner, and information about the police who collected the evidence.

In sum, we find that police auctions of cellphones represent a serious and unique threat to the privacy and safety of users. We discussed mitigations various stakeholders can take. Our disclosure appears to have prompted PropertyRoom to wipe cellphones before selling them, but there are still smaller auction houses that may be selling unwiped phones. We hope that this paper motivates legislatures and police departments to enact policies that halt the sale of unwiped secondhand phones.

Acknowledgments

We thank Jon Callas from the Electronic Frontier Foundation for providing the legal analysis that appears in Section II-C, and Tom Goldstein for first bringing these police auctions to our attention. We also thank Stefan Savage for his insightful comments. We also thank UMD's IRB office, legal counsel, and Division of IT for helping scope how to safely and ethically perform this work. We thank the students of the Breakerspace lab for their assistance guessing PINs and patterns. Finally, we thank the anonymous reviewers for their helpful comments. This work was supported in part by NSF grant CNS-1901325.

References

[1] A. Adam and N. Clarke, "Information Security Leakage: A Forensic Analysis of USB Storage Disks," *Advances in Communications, Computing, Networks and Security: Proceedings of the MSc/MRes programmes from the School of Computing, Communications and Electronics, 2007-2008*, vol. 6, pp. 171–178, 2009.

[2] Amnesty International Security Lab, "Mobile Verification Toolkit," https://docs.mvt.re/en/latest/, visited 2022-19-08.

[3] Andrew Horton, "Android-PIN-Bruteforce," https://github.com/urbanadventurer/Android-PIN-Bruteforce, visited 2022-19-08.

[4] K. A. Bovid and B. N. Sparks, "Going Once, Going Twice...: Are Local Governments Sold on Online Auctions?" *Popular Government*, vol. 73, no. 1, 2007.

[5] W. Chaerani, N. Clarke, and C. Bolan, "Information leakage through second hand USB flash drives within the United Kingdom," in *9th Australian Digital Forensics Conference*, 2011.

[6] Cloudflare, "Content categories," https://developers.cloudflare.com/cloudflare-one/policies/filtering/dns-policies/dns-categories/#content-categories, visited 2022-19-08.

[7] Coalition against Stalkerware, "Stalkerware Threat List," https://backend.stalkerware.org/, visited 2022-09-08.

[8] CTIA, "CTIA Stolen Phone Checker," https://stolenphonechecker.org/spc/index.jsp.

[9] Disposition of lost property, N.Y. PEP Law §254. 2014, https://www.nysenate.gov/legislation/laws/PEP/254.

[10] Duties of Police, N.Y. PEP Law §253. 2014, https://www.nysenate.gov/legislation/laws/PEP/253.

[11] Echap, "Stalkerware indicators of compromise," https://github.com/AssoEchap/stalkerware-indicators, visited 2022-11-08.

[12] S. L. Garfinkel and A. Shelat, "Remembrance of data passed: A study of disk sanitization practices," *IEEE Security & Privacy*, vol. 1, no. 1, pp. 17–27, 2003.

[13] W. B. Glisson and T. Storer, "Investigating Information Security Risks of Mobile Device Use within Organizations," *arXiv preprint arXiv:1309.0521*, 2013.

[14] W. B. Glisson, T. Storer, A. Blyth, G. Grispos, and M. Campbell, "In-The-Wild Residual Data Research and Privacy," *Journal of Digital Forensics, Security and Law*, vol. 11, no. 1, pp. 77–98, 2016.

[15] W. B. Glisson, T. Storer, G. Mayall, I. Moug, and G. Grispos, "Electronic retention: what does your mobile phone reveal about you?" *International Journal of Information Security*, vol. 10, no. 6, pp. 337–349, 2011.

[16] Google, "Android debug bridge (adb)," https://developer.android.com/studio/command-line/adb, visited 2022-15-08.

[17] GSMA, "GSMA Device Check," https://www.gsma.com/services/tac/about-device-check/.

[18] M. Harback, A. D. Luca, N. Malkin, and S. Egelman, "Keep on Lockin' in the Free World: A Multi-National Comparison of Smartphone Locking," in *ACM Conference on Human Factors in Computing Systems (CHI)*, 2016.

[19] IPV Tech Research, "ISDi's IPV spyware blocklist," https://github.com/stopipv/isdi/blob/main/static_data/app-info.db, visited 2022-10-08.

[20] James Mosieur, "Careless Electronics Disposal Practices Can Lead To Embarrassment," https://www.data-secure.org/post/2016/10/06/careless-electronics-disposal-practices-can-lead-to-embarrassment, visited 2022-20-08.

[21] A. Jones, O. Angelopoulou, and L. Noriega, "Survey of Data Remaining on Second Hand Memory Cards in the UK," *Computers & Security*, vol. 84, pp. 239–243, 2019.

[22] A. Jones, G. S. Dardick, G. Davies, and I. Sutherland, "The 2008 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market," *Journal of International Law and Technology*, vol. 4, no. 3, pp. 162–175, 2009.

[23] A. Jones, C. Valli, G. S. Dardick, I. Sutherland, G. Dabibi, and G. Davies, "The 2009 Analysis of Information Remaining on USB Storage Devices Offered for Sale on the Second Hand Market," in *7th Australian Digital Forensics Conference*, 2009.
[24] A. Jones, C. Valli, and I. Sutherland, "Analysis of Information Remaining on Hand Held Devices offered for Sale on the Second Hand Market," *The Journal of Digital Forensics, Security and Law*, vol. 3, no. 2, pp. 55–70, 2008.
[25] Josh Frantz, "Buy One Device, Get Data Free: Private Information Remains on Donated Tech," https://www.rapid7.com/blog/post/2019/03/19/buy-one-device-get-data-free-private-information-remains-on-donated-devices/, visited 2022-20-08.
[26] libimobiledevice, "libimobiledevice home page," https://libimobiledevice.org/, visited 2022-19-08.
[27] Microsoft, "PhotoDNA," https://www.microsoft.com/en-us/photodna, visited 2022-19-08.
[28] Miessler, Daniel and Haddix, Jason and g0tmi1k, "Seclists: The Pentester's Companion," https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/10-million-password-list-top-100.txt, visited 2022-19-07.
[29] C. W. Munyendo, M. Grant, P. Markert, T. J. Forman, and A. J. Aviv, "Using a blocklist to improve the security of user selection of android patterns," in *Symposium on Usable Privacy and Security (SOUPS)*, 2021.
[30] Proper disposal of consumer information, 16 CFR §682.3, https://www.ecfr.gov/current/title-16/chapter-I/subchapter-F/part-682/section-682.3.
[31] PropertyRoom, "PropertyRoom.com Full Press Kit," https://content.propertyroom.com/listings/banners/!WSImages/PDFdocuments/PropertyRoomcom_FullPressKit_January2017.pdf, 2017.
[32] ——, "10" Fantasy Dragon Dagger Blade Knife Sword," https://www.propertyroom.com/listing.aspx?l=13869632, 2020.
[33] ——, "Apple Cell Phone Lot, 30+ Pieces, Sold For Parts And More," https://www.propertyroom.com/listing.aspx?l=14442714, 2020.
[34] ——, "Apple IPhone Lot,8 Pieces Sold For Parts," https://www.propertyroom.com/listing.aspx?l=14259052, 2020.
[35] ——, "Cell Phone Lot, 10 Pieces, Sold For Parts," https://www.propertyroom.com/listing.aspx?l=14413748, 2020.
[36] ——, "Cell Phone Lot, 20+ Pieces, Sold For Parts," https://www.propertyroom.com/listing.aspx?l=14218129, 2020.
[37] ——, "Cell Phone Lot, 5+ Pieces, Sold For Parts," https://www.propertyroom.com/listing.aspx?l=15134449, 2021.
[38] ——, "14K Yellow Gold Crucifix Pendant - Suitable for Men & Women - 19 mm X 12 mm," https://www.propertyroom.com/listing.aspx?l=15275419, 2022.
[39] ——, "Cell Phone Lot, 10+ Pieces," https://www.propertyroom.com/listing.aspx?l=15268422, 2022.
[40] Public sale of abandoned property, Wash. Rev. Code §63-29-220. 2011, https://app.leg.wa.gov/RCW/default.aspx?cite=63.29.220.
[41] C. Richardson, "It's a steal of a deal at former cop's site: PropertyRoom.com," https://www.nydailynews.com/new-york/brooklyn/steal-deal-site-propertyroom-article-1.405324, 2017.
[42] D. Salmi, "Avast finds personal data on phones sold at pawn shops [Infographic]," 2016, https://blog.avast.com/2016/02/24/avast-finds-personal-data-on-phones-sold-at-pawn-shops/, visited 2022-20-08.
[43] R. Samuel, P. Markert, A. J. Aviv, and I. Neamtiu, "Knock, Knock. Who's There? On the Security of LG's Knock Codes," in *Symposium on Usable Privacy and Security (SOUPS)*, 2020.
[44] K. Sansurooah and P. Szewczyk, "A study of remnant data found on USB storage devices offered for sale on the Australian second hand market in 2011," in *10th Australian Information Security Management Conference*, 2012.
[45] S. Savage, "Lawful Device Access without Mass Surveillance Risk: A Technical Design Discussion," in *ACM Conference on Computer and Communications Security (CCS)*, 2018.
[46] Stellar, "Residual Data Study on Second Hand Devices: A study on the risk implication for people, businesses and economies," 2019, https://www.stellarinfo.com/pdf/Stellar-Residual-Data-Study-on-Second-Hand-Devices-Report-April-2019.pdf, visited 2022-20-08.
[47] P. Szewczyk, K. Sansurooah, and P. A. Williams, "An Australian Longitudinal Study into Remnant Data Recovered from Second-Hand Memory Cards," *International Journal of Information Security and Privacy (IJISP)*, vol. 12, no. 4, pp. 82–97, 2018.