VB2020
localhost

30 September - 2 October, 2020 / vblocalhost.com

WHY THE SECURITY WORLD SHOULD TAKE STALKERWARE SERIOUSLY

David Ruiz
Malwarebytes, USA

davidalruiz@gmail.com

ABSTRACT

Last year, cybersecurity vendors, nonprofit organizations and digital rights activists bandied together to present a multifaceted front against a shadowy digital threat that can be used to inflict harassment, harm and violence against domestic abuse survivors. That threat is stalkerware. These types of apps, which proliferate online and at times sneak into the *Google Play* store, can pry into a person's private life, revealing GPS location history, web browsing behaviour, text messages, emails, phone calls, photos and videos, all without consent and hidden from view. The information that can be wrongfully accessed by these apps can be used to reveal a domestic abuse survivor's hidden location, dismantle plans to find safety through a domestic abuse support network, and undo attempts to find help through domestic abuse hotlines.

The numbers on this threat are limited, but staggering. In the first nine months of 2019, *Kaspersky* reported more than 518,000 detections of either stalkerware installations or installation attempts on *Android* phones [1]. From 1 March 2019 to 1 March 2020, *Malwarebytes* detected apps with these capabilities more than 55,000 times on *Android* devices [2]. Though we have no numbers on the prevalence of these types of apps within domestic abuse situations, we do know from conversations with domestic abuse advocates, university researchers in intimate partner violence, and local law enforcement, that stalkerware-type apps have been used in many situations of domestic violence.

Some of us in the cybersecurity community are already working together to better stop this threat, having helped build the Coalition Against Stalkerware, but more help is needed.

INTRODUCTION

For years, *Malwarebytes* has detected and warned users about the potentially dangerous capabilities of stalkerware, an invasive threat that can rob individuals of their expectation of, and right to, privacy. Just like the domestic abuse it can enable, stalkerware proliferates away from public view, leaving its victims and survivors in isolation, unheard and unhelped.

These types of apps can pry into a person's private life, revealing GPS location history, web browsing behaviour, text messages, emails, phone calls, photos and videos, all without consent and hidden from view. The information accessed by these apps can be used to reveal a domestic abuse survivor's hidden location, dismantle plans to find safety through a domestic abuse support network, and undo attempts to find help through domestic abuse hotlines.

Last year, we proposed an internal experiment to better understand what these types of apps can reveal, along with the level of tech proficiency required to use them.

This paper explores the results of a two-week experiment in which we installed a mobile application which revealed sensitive, private information on a test device – a *Google Pixel* – that we had purchased and factory reset.

The experiment ran from 1 – 14 June, with six participants who consented to the activity and risks. On 7 June, we told the participants to no longer send SMS messages or make phone calls to the *Google Pixel* unless explicitly asked to do so. From 8 – 14 June, we followed up with a select number of participants, separately from the *Google Pixel*, to try to recreate experiment results.

On 15 June, we uninstalled the application from the *Google Pixel* and informed the participants about the end of the experiment.

The application retrieved current location, location history, Wi-Fi network name, battery percentage, SMS messages, notifications, photos, deleted photos, videos, call logs and call recordings. It also provided the capability to live-stream footage from the *Google Pixel*'s front and rear cameras, and the capability to stream audio from the *Google Pixel*'s microphone.

The application *did not* retrieve social media interactions on the *Google Pixel*, including comments, likes, shares, or direct messages across platforms including *Facebook*, *Instagram* and *Twitter*. Though we created test accounts with these platforms for this experiment, the test accounts proved to be of little value. Further, we did obtain consent from more participants than those included in this paper to engage in social media interactions with our test accounts, but these efforts are not included in the paper.

The results of our experiment show the clear potential for danger. But the response to these threats must be multifaceted. In the final portion of our paper we explore why downloading and running an anti-malware scanner is not a comprehensive solution for survivors of domestic abuse who are facing tech-enabled abuse.

WHAT STALKERWARE IS AND WHAT IT LOOKS LIKE WHEN USED

In our research and advocacy to protect users from the capabilities of stalkerware-type apps, we learned that what these apps look like – how they present themselves to their actual users – demanded further scrutiny.

How these types of applications present themselves to users is important because, contrary to what some may think, these types of applications can be exceedingly easy to use and understand. They often require no advanced training or high-tech proficiency in writing or understanding code. They are often consumer-ready tools that, in under 10 minutes, can be deployed against a person's mobile device without their knowledge.

This year, *Malwarebytes* developed several sample images that represent what the 'average' user experience resembles for a stalkerware-type application. We worked with images from public demos for five stalkerware-type applications.

In comparing the user interfaces for the applications, we learned that many apps share the same user interface. Stalkerware-type applications often present an online web portal that users can log into and where they will find a type of universal 'dashboard'. The dashboard often includes a left rail on its user interface with tabs that lead the user to the desired information. Some of these tabs, for example, can direct users to call logs, call recordings, contacts, SMS messages, current location, location history, browser history, photos, videos, calendars, app usage and keylogger data.

Figure 1 shows a representation, developed by *Malwarebytes*, of what these types of apps can look like for those who use them and deploy them onto separate mobile devices.

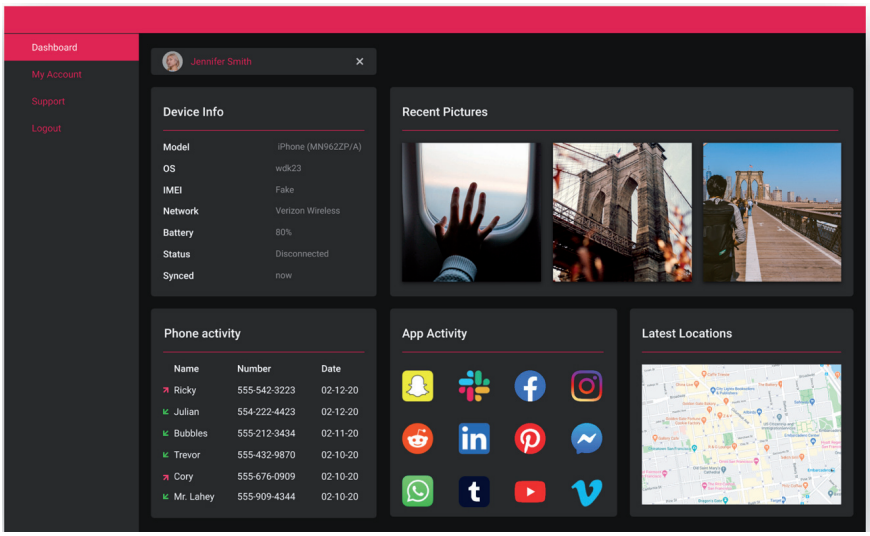

Figure 1: Visual mockup of a stalkerware-type application dashboard.

The dashboards for several stalkerware-type applications also borrow liberally from the 'card'-inspired design of many mobile apps today. 'Cards' refer to single panels of information that focus on one topic. A type of this design can be seen in *Google*'s newsfeed on *Android* devices (see Figure 2).

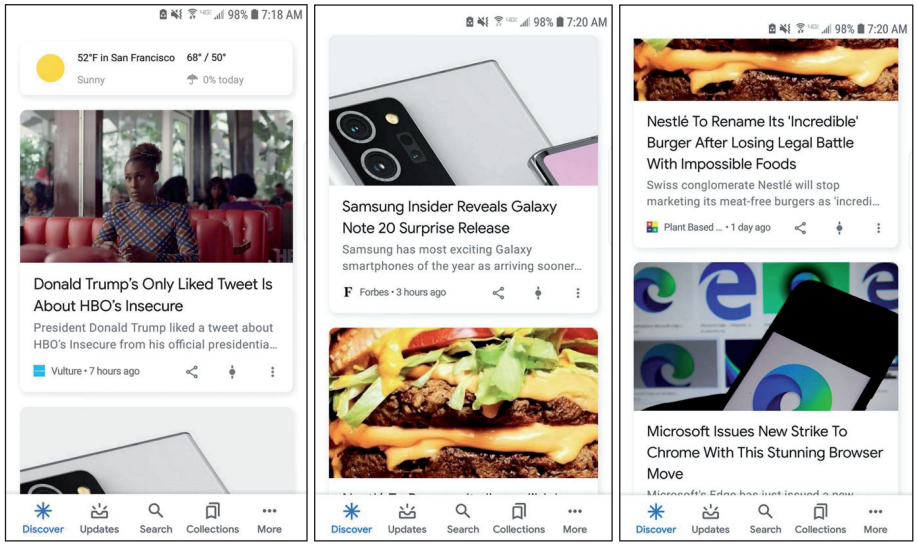

Figure 2: Google 'card' designs.

We make these comparisons to show that stalkerware-type applications do not have to be complicated, difficult products to use. Instead, they can be familiar and easy to navigate for most users today, simply because of their design and user interface.

When users click tabs within the dashboard of a stalkerware-type application, they can be shown a separate screen with desired results. For example, when a user click on the item on the left rail that says 'Photos', they can then be led to a more devoted screen that reveals the photos stored and taken on the device on which the stalkerware-type application is installed. Figure 3 is a representation of what that looks like.

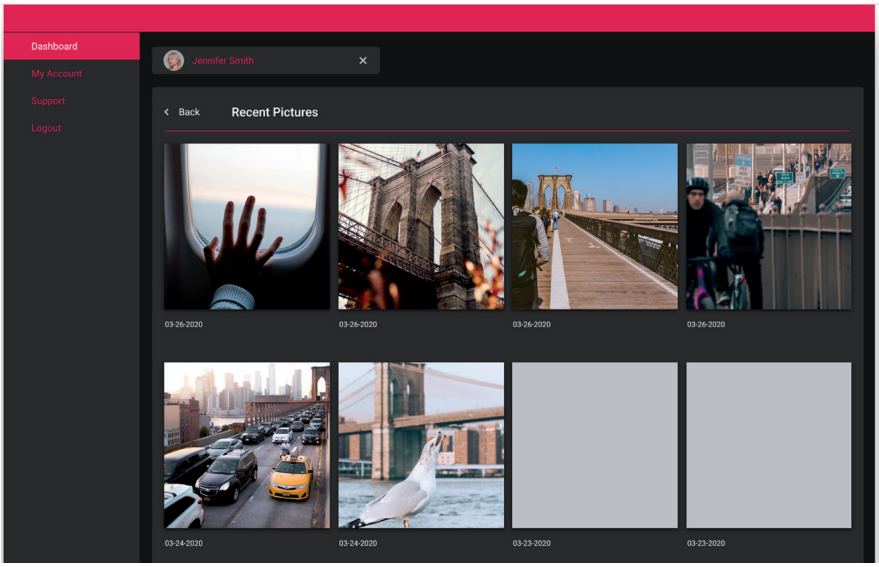

Figure 3: Visual mockup of a photo dashboard from a stalkerware-type application.

Figure 4 is a representation of what a user could be shown when, for example, clicking on the call logs and call recordings feature offered by a stalkerware-type application that is installed on a separate device.

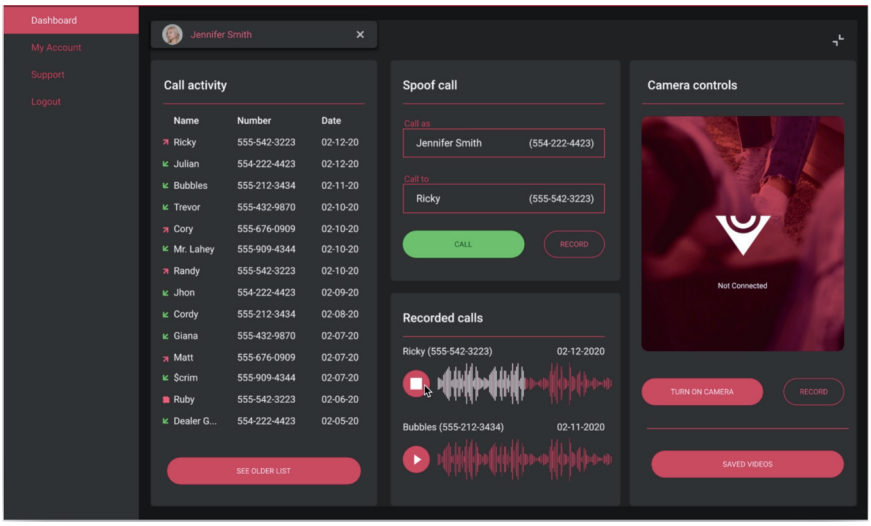

Figure 4: Visual mockup of a call log and recording dashboard from a stalkerware-type application.

These visual mockups represent both the familiar navigation of these apps and their broad, claimed capabilities. Many of these types of apps advertise the ability not just to reveal call logs, for example, but to record incoming and outgoing calls, and to take over a device's camera controls, providing the opportunity either to take a photo or to live-stream a device camera's view. Some of these types of apps also claim to provide users with the capability to 'spoof' a message from the device that has the stalkerware-type application installed on it, in effect granting a non-device owner the power to potentially send an SMS message from the device's phone number.

But these visual representations can only show so much.

INSTALLING A MONITORING APP ON A TEST DEVICE – CONSIDERATIONS

In 2019, in trying to increase education about the threats posed by stalkerware, the paper author proposed an experiment: implant such an app on his own device for a limited time frame.

Months later, the paper's author worked with a mobile malware researcher at *Malwarebytes* to refine the experiment and preserve the security and privacy both of himself and of the individuals he interacted with during the experiment.

Together, we took into account multiple considerations:

- The cybersecurity protections of apps with these types of capabilities:

  - The risk of a data breach of whatever company developed the monitoring application we chose to deploy in the experiment.
  - The privacy risks to other individuals who interacted with the paper author during the experiment period.

- The level of tech proficiency required to install the selected monitoring application:
  - Whether such an application would require rooting a device for successful installation.
  - Whether the monitoring application was available on the *Google Play Store.*
  - Whether the monitoring application was only available from a separate website.

- The time required to install the monitoring application on a device:
  - Whether a successful installation could be performed in under 10 minutes.
  - Whether a successful installation could be performed without a device owner's knowledge or consent.
  - Whether a successful installation required physical access to a device.
  - Whether a successful installation required knowledge of a device passcode to unlock the device.

- The ethics of payment:
  - Whether we could, as committed members in the fight against stalkerware-type applications, pay for a potentially invasive application.
  - Whether any monitoring application was entirely free.
  - Whether any monitoring application offered a free trial.
  - Whether we could install a stalkerware-type application without payment, and whether we could access the necessary web portal to use the stalkerware-type application without creating a paid account with the application's developer.

Following these considerations, we performed the following actions:

- Purchased a refurbished, unlocked 2016 *Google Pixel* test device solely for this experiment, which we factory reset before the experiment began
- Purchased a three-month prepaid phone contract and SIM card solely for this experiment, to use with the 2016 *Google Pixel*
- Created a new *Google* account to register the *Google Pixel*
  - The new *Google* account came with a *Gmail* account and other *Google* services
- Created a new *Signal* account by using the *Google Pixel*'s real phone number.

In selecting participants for the study, and in warning them of the risks involved in the planned experiment, we did the following:

- Emailed a list of individuals from the paper author's personal *Gmail* address.
- Informed potential participants about the risks involved in the experiment, including a potential data breach of the developer of whatever stalkerware-type application we would eventually choose. If the individuals participated, we warned that such a data breach could reveal:
  - Phone numbers entered into the *Google Pixel*'s 'Contacts'
  - SMS messages traded with the *Google Pixel*
  - Call logs between their devices and the *Google Pixel*, including the time, duration, and date of the call
  - Recordings of calls made between their devices and the *Google Pixel*, depending on the capabilities of the stalkerware-type application we would eventually select.

After learning of potential participants' interest, we followed up in a separate email and asked for consent to:

- Add phone numbers to the *Google Pixel* device's 'Contacts'
- Send and receive SMS messages with the *Google Pixel*
- Send and receive phone calls with the *Google Pixel*
  - (If called by the *Google Pixel*, we asked for consent to record the conversation)
- Send and receive messages through the end-to-end encrypted app *Signal.*

Following receipt of consent, we added participants' phone numbers into the *Google Pixel*, and we obscured their real names by running their initials through an undisclosed cipher. The resulting initials were the only 'names' to show up in the *Google Pixel*'s list of contacts.

We also refrained from email communication using the experimental *Gmail* account because we did not have a safe method to obscure participants' real names from their email addresses. Should the stalkerware-type application suffer a breach in the future, we did not want to take that risk of private information being released.

We informed participants on 24 May 2020 that we planned to begin the experiment on 31 May, with a planned end date of 7 June. On 30 May, the night before the experiment began, we emailed a second reminder about the planned start date.

On 7 June, we emailed the participants telling them that the experiment had largely ended, but that we needed an additional week to test whether our results could be recreated. We told participants that the safest option for the second week would be not to engage with the *Google Pixel* in any way, and that, should we need a more targeted test, we would contact the participants from a separate device and obtain consent for those targeted tests on the *Google Pixel* when necessary.

The participants

Participants A, B, C, D and **E** all consented to:

- Having their actual phone numbers entered into the *Google Pixel*'s 'Contacts' under obscured initials
- Accepting phone calls from the *Google Pixel* that could be recorded by the monitoring software
- Trading SMS messages from the *Google Pixel* that could be retrieved by the monitoring software
- Trading messages on the end-to-end encrypted app *Signal.*

Participant F consented to all of the above, with the exception of accepting phone calls from the *Google Pixel* that could be recorded by the monitoring software.

CHOOSING AN APPLICATION TO INSTALL ON THE GOOGLE PIXEL

In selecting a stalkerware-type application, we tried to recreate conditions of a hypothetical stalkerware user: we searched on *Google*. We entered several search terms, including:

- 'How to spy on my girlfriend's phone'
- 'How to spy on my girlfriend's location'
- 'How to track my girlfriend's phone'

(While separate *Google* search results may exist based on gender, we did not take into account that intersectionality when working on this paper, thus we did not immediately look up how to track a boyfriend's phone or a boyfriend's location.)

From these search results, we found websites advertising their own stalkerware-type applications. We also found a number of blogs and 'review' articles that compared the capabilities of multiple stalkerware-type applications.

We compiled a list of six stalkerware-type applications that provided capabilities that would prove useful for our experiment. We knew that whatever application we chose, we wanted it to be able to see, at minimum, our current location and location history, call logs, contacts, SMS message logs, SMS message content, photos, videos and notifications received by the *Google Pixel*.

Additional, favourable features to test would have included the monitoring of social media activity, a keylogger, camera and microphone control, and the ability to hide the app from view in the *Google Pixel*'s app drawer.

We also wanted to choose an app that did not require jailbreaking or rooting a device, so as to not focus our experiment on conditions that required strong technical knowledge. As we showed in the first section of the paper, these can be consumer-ready applications. It would betray the experiment to choose an application that requires high-tech proficiency to install.

The six apps we found provided the same barrier each time – high cost. We instead looked for a free stalkerware-type app that *Malwarebytes* detected. But we took two steps in getting to our final app choice.

First, we installed an application – that has some of the above, desired features – that is available for free on the *Google Play Store*. Then, after granting the application permissions, we connected to the application's web portal. Through that web portal, we downloaded a *second*, similar app, advertised by the same company but *not* available on the *Google Play Store*.

The second application was nearly identical to the first one, but it had one extra feature: the ability to hide itself from view. **During our experiment, however, this feature did not work**. The second application claimed to have the following capabilities:

- GPS location viewing
- Location history tracking
- Call log viewing
- Call recording with limited functionality
- SMS message content viewing
- Notification viewing
- Photo viewing
- Deleted photo viewing
- Video viewing
- Contact viewing
- Installed app viewing
- App usage statistics
- Camera control to take a photo with the front and back cameras on a device
- Camera control to allow live streaming from the front and back cameras on a device
- Microphone control to allow live streaming of ambient sound from the device
- Device screen sharing, showing what the device user is doing in real time.

We will call this second application, not listed on the *Google Play Store*, the 'Monitoring Application'. We also subsequently uninstalled the first application we had downloaded.

INSTALLING THE MONITORING APPLICATION

After downloading the Monitoring Application to a separate laptop, we plugged the *Google Pixel* into the laptop using a USB cable and transferred the application to the *Google Pixel*.

During setup, the Monitoring Application first presented a screen of text that resembled a 'Terms and Conditions' agreement. It explained how the Monitoring Application's developer would use data gathered from the device. **It also explained that certain data, including location, contacts, SMS messages and notifications, call logs, saved and removed photos, and browser history, would all be sent to the developer unless the user explicitly opted out**.

After agreeing to the initial data-sharing agreement, the Monitoring Application led us through several screens to grant it various permissions. There was one screen each to grant access to:

- Contacts
- Phone calls
- Calendar
- Call logs
- Taking pictures and recording video
- Location
- Photos, media and files
- Recording audio
- Sending and viewing SMS messages.

Further setup screens requested administrator access, accessibility permission (for call recording), access to read notifications, and access to allow screen mirroring.

The setup process required physical access to the *Google Pixel*, plus knowledge of the device's passcode. Despite the many agreement screens, the entire process took under 10 minutes. Following setup, the *Google Pixel* showed no immediate signs that its permissions had been changed.

We then connected the *Google Pixel* to the Monitoring Application's web portal by using the *Pixel* to scan a QR code that was visible on our laptop.

We then obtained a free 'pro' trial of the Monitoring Application, and subsequently paid $11 to maintain the 'pro' capabilities. (After the experiment, we asked for a refund.)

The Monitoring Application web portal presented a central dashboard that showed us:

- The *Google Pixel*'s battery percentage
- The Wi-Fi network that the *Google Pixel* was connected to, **with the capability to turn off the *Google Pixel*'s Wi-Fi connection**
- The name of the *Google Pixel*'s cell service provider
- The *Android* OS version
- The *Google Pixel*'s phone number
- The last app used by the *Google Pixel*
- The *Google Pixel*'s screen status (on or off)
- The *Google Pixel*'s available memory
- The *Google Pixel*'s current location.

THE RESULTS OF THE EXPERIMENT

Once installed, the Monitoring Application tracked activity that occurred on the *Google Pixel* for 14 days, including call logs, current locations, location history, and SMS message content in conversations with participants A, B, C, D, E and F. The Monitoring Application also retrieved photos, as well as deleted photos, videos and call recordings.

The Monitoring Application retrieved notifications received by the *Google Pixel*, including updates from *Gmail*, the *Google Play Store*, *Maps* and *Google*'s weather service.

The capability to retrieve notifications had the potential to directly interfere with the security of end-to-end encrypted messaging apps. We tested messages and notification settings on the end-to-end encrypted app *Signal*. When we allowed the content of a *Signal* message to be displayed in the *Google Pixel*'s notifications, the Monitoring Application recorded the content of that *Signal* message through the notification. But when we chose to hide the content and sender of a *Signal* message – through *Signal*'s notification settings – the Monitoring Application only pulled a notification that said 'New Message', as shown below:

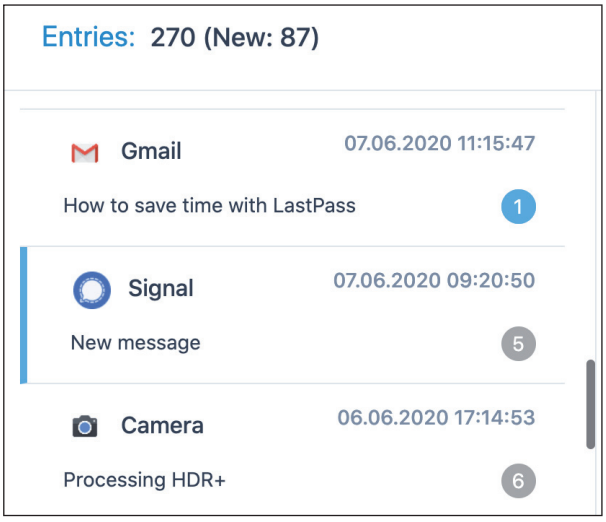

Figure 5: A screenshot of the notifications pulled by the Monitoring Application, including an obscured message on Signal.

The following sub-sections present a breakdown of some of the Monitoring Application's capabilities and retrievals.

Current location and location history

The Monitoring Application retrieved the *Google Pixel*'s current location whenever we logged into the web portal. Though the locations would shift and change by about 250 feet, a look at the *Google Pixel*'s historical location data easily revealed the actual cross-streets of the paper author.

The Monitoring Application also tracked the *Google Pixel*'s location over time, with often impossible 'routes' that cut through buildings and street blocks lacking any pedestrian or car access.

Further, locations tracked by the Monitoring Application were sometimes imprecise.

For example, on 6 June, the paper's author visited San Francisco's North Beach district to purchase takeout from two restaurants: Mario's Bohemian Cigar Store Café on the corner of Union Street and Columbus, and Da Flora on the corner of Filbert Street and Columbus. When looking at the Monitoring Application's location history tab, it appears as though the

paper author travelled directly to North Beach's Washington Square State Park, and then left the area. The paper author in fact never entered Washington Square State Park.

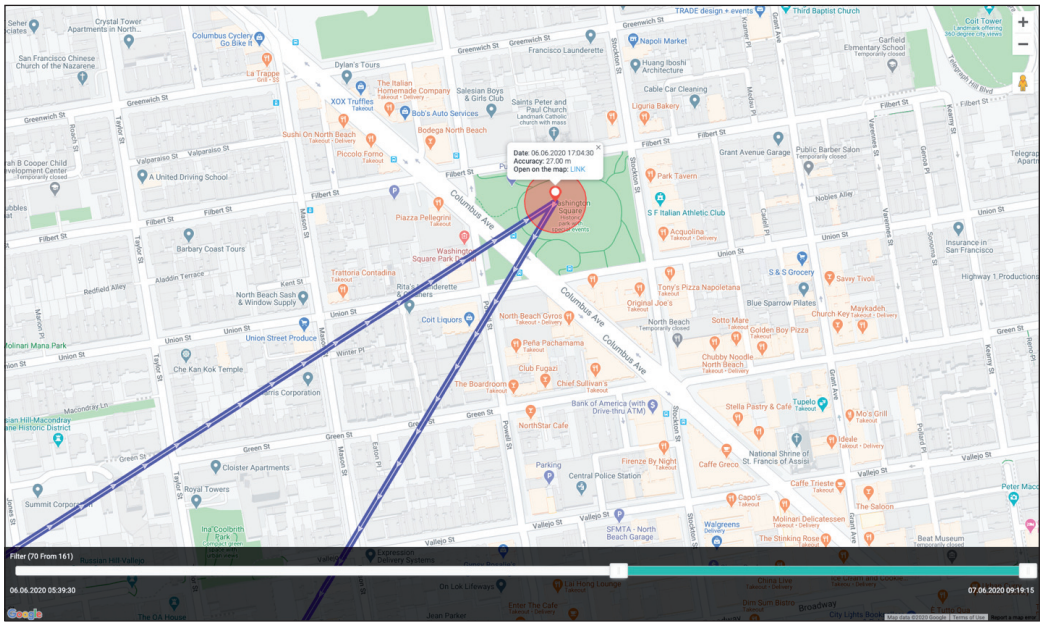

Figure 6: A screenshot of the Monitoring Application's location history feature, showing imprecise location of our actual route.

Zooming in, we can see that Mario's Bohemian Cigar Store is directly across the street from Washington Square State Park, as shown in a green circle in Figure 7. Though unmarked on the *Google Map*, La Flora is also marked in a green circle in Figure 7.

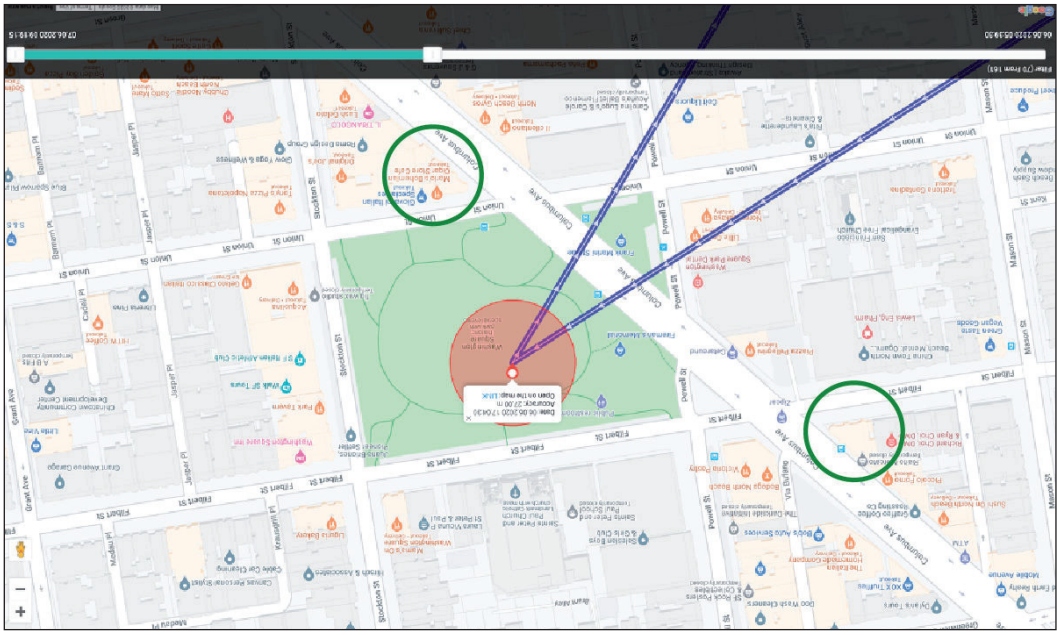

Figure 7: A screenshot of the Google Pixel's tracked location, with the two restaurants we visited circled in green.

At another point in the experiment, the Monitoring Application revealed that the paper author visited a shopping centre on 5 June.

The tracked locations were sometimes wrong – the paper author did visit this shopping centre, but he did not stand at all those exact locations. However, because the experiment ran while coronavirus precautions were in place, purchasing groceries at *Trader Joe*'s required standing in a line outside the store. This line wrapped around to the south, and then further west of the store. This line sometimes extended to the space in front of the *Bank of America* location. The Monitoring Application retrieved this accurately.

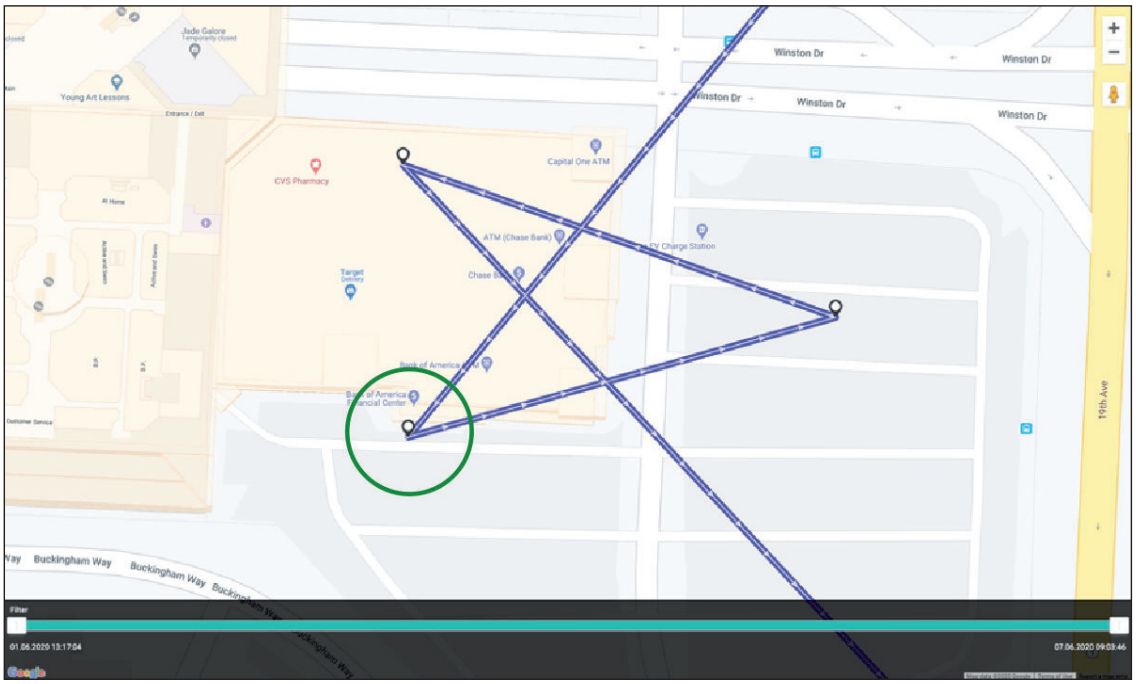

Figure 8: A screenshot of the Monitoring Application tracking the paper author's location on 5 June, with his accurate position circled in green.

Photos taken and deleted by the Google Pixel

The Monitoring Application retrieved every photo taken with the *Google Pixel*'s Camera app, including those that were stored on the *Google Pixel* before the installation of the Monitoring Application. This same functionality applied to screenshots taken with the *Google Pixel*. The Monitoring Application's web portal provided time stamps for every photo.

The Monitoring Application also retrieved 'deleted' photos, which included photos that were removed from the *Google Pixel* on the *Google* 'Photos' app user interface.

Below, we show the steps we took to remove a specific photo from *Google Photos* and its later retrieval by the Monitoring Application.

We first looked at the photos available in the *Google Pixel*'s photo roll, in the *Google Photos* app. We then selected the third available photo for a closer view.

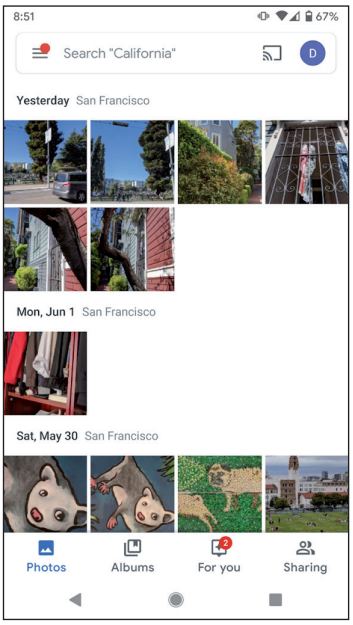

Figure 9: Screenshot of the Google Pixel's photo roll.

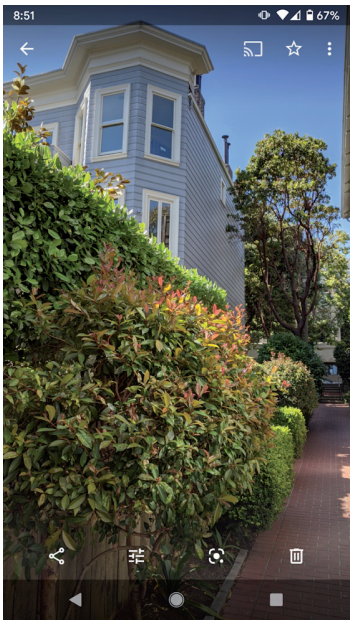

Figure 10: Screenshot of a photo in full view on the Google Pixel, showing the trash can icon to delete.

We then pressed the 'trash can' symbol in the lower right portion of the frame, which brought up the dialog box that asked if we wanted to delete the photo. We then saw the dialog box show up, asking if we wanted to 'Remove from Google account and synced devices' (Figure 11).

When we pressed 'Move to trash' we took a screenshot showing the notification that the photo had successfully been moved to the trash, as we see in Figure 12, circled in green.

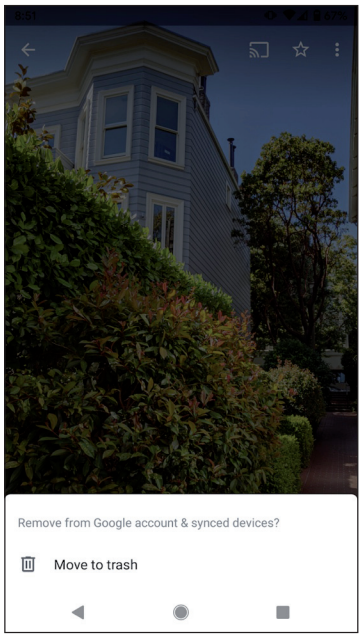

Figure 11: Screenshot of the dialog box to move a photo to the trash on the Google Pixel.

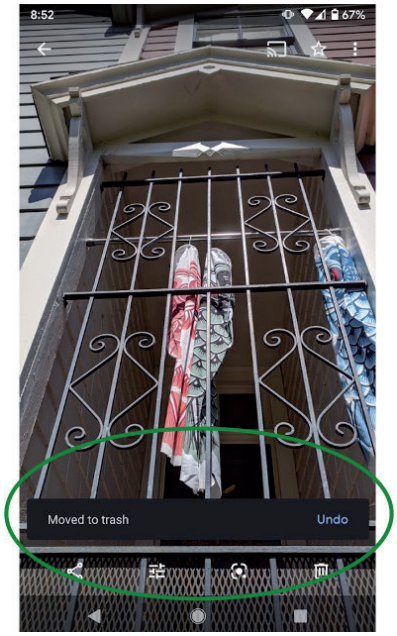

Figure 12: Screenshot that shows our most recent action to remove a photo from the Google Pixel.

After these steps were taken, we retrieved the 'deleted' photo using the Monitoring Application, as shown in Figure 13. The time stamp from the Monitoring Application shows that we did accurately delete the photo at 08:52 PM PT, as shown in Figure 12.

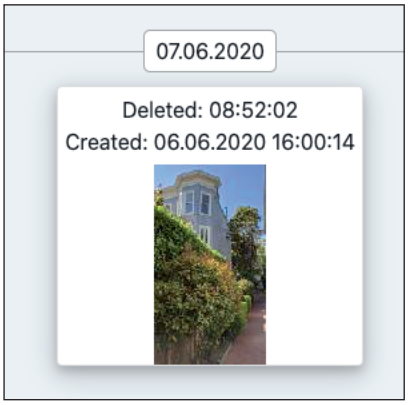

Figure 13: A screenshot showing the Monitoring Application's retrieval of the just-deleted photo.

SMS conversations using the Google Pixel

The Monitoring Application retrieved all of the SMS conversations exchanged on the *Google Pixel*. The web portal grouped these SMS conversations by contact name, as shown in Figure 14.

(The *Google Pixel*'s phone number was mistakenly routed to take delivery orders for a restaurant. This behaviour was present before the installation of the Monitoring Application. We have obscured the relevant number above.)

Interestingly, messages *sent* by the *Google Pixel* were, according to the Monitoring Application, sent twice. The first send would be blocked, and the second send would connect. This happened with every SMS message sent by the *Google Pixel* during the experiment period.

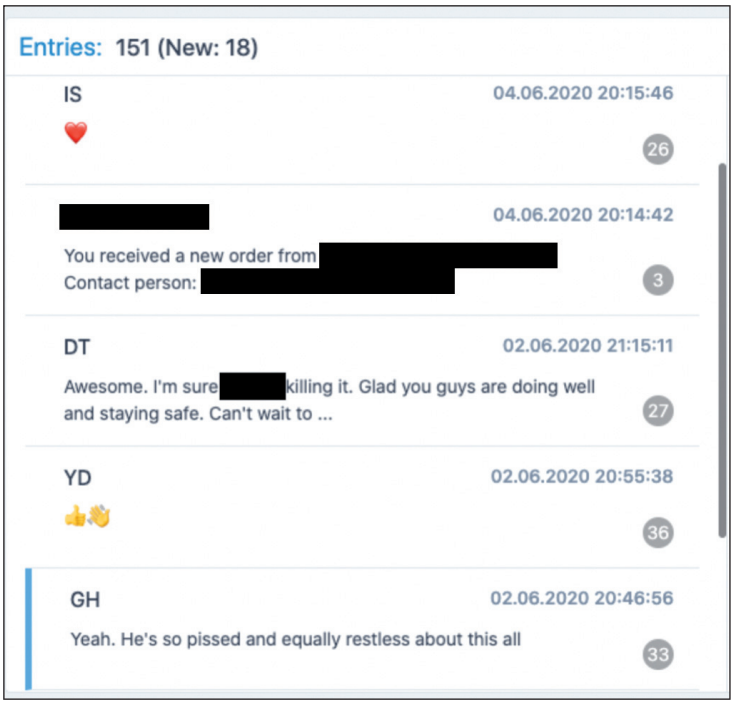

Figure 14: A screenshot of the SMS conversation 'tabs' available on the Monitoring Application's web portal.

When a conversation is selected, the Monitoring Applications presents the relevant SMS messages to the right of the menu shown in the screenshot above. **The Monitoring Application can retrieve SMS messages that were exchanged prior to the Monitoring Application's installation**.

We have recreated portions of some of the conversations and redacted the names to protect privacy.

SMS conversation with Participant A, 2 June 2020

08:24:03 PM PT Paper Author:
How are y'all doing down in [**REDACTED LOCATION**]? Are you still curfewed?

08:28:55 PM PT Participant A:
Hey [**REDACTED NAME**] We're good. Yes, still curfewed. [**REDACTED NAME**] just went back to work for the first time yesterday but they've sent him home at lunch both yesterday and today because no one is coming in. Crazy times. What about you? How are things in your neck of the woods?

08:29:07 PM PT Paper Author:
Oh damn, that's crazy about [**REDACTED NAME**]. I can't say I wouldn't do the same honestly. Like, if my eyes were a bit blurry, I'm just running with it for a bit. Things are alright here. [**REDACTED NAME**] and I are far from actual protest. Nothing smashed in the [**REDACTED LOCATION**] from what we can tell. We have a curfew, too. Honestly just f*cking brain fried from the news and from high police brutality.

I'm a moron at work this week

Are you able to work from home? Things as normal as they can be there?

08:32:01 PM PT Participant A:
Same. It's hard to focus on work when there's so much other stuff going on. Being quarantined for 3 months has a frying effect on the brain 🙃

08:33:58 PM PT Paper Author:
🔥
🦁

Has your house gone insane? Were you just managing young, impressionable men like [**REDACTED NAME**] as they watched every show on Netflix?

20:40:32 PM PT Participant A:
Yeah I had to quarantine myself from their quarantine

It was a lot of drinking and McDonald's chicken tenders

SMS conversation with Participant C, 2 June 2020

08:37:37 PM PT Participant C:
Tonight I decided is a martini night because I just can't sleep well the past couple of nights with all of this going on

And I'm forced to work everyday on menial stuff that doesn't matter in the scheme of things

08:41:13 Paper Author:
Dude yeah. It's been like f*cking impossible to focus on anything and pretend like we aren't facing an existential crisis

We got a message from [**REDACTED NAME**] supporting the protests and being like "hey, right now is tough, take care of yourselves"

08:45:03 Participant C:
That's actually really reassuring

My roommate had been telling me about his work and how they refuse to talk about anything during their meetings about what's going on in our country

It's crazy

08:46:03 Paper Author:
That feels low key irresponsible

08:46:46 Participant C:
Yeah. He's so pissed and equally restless about this all

Call logs and call recordings

The Monitoring Application retrieved call logs from the *Google Pixel*. The application's web portal presented the paper author with a list of calls both sent and received by the *Google Pixel*. The call log list included the following information for each listed call:

- Type (missed, outgoing, incoming)
- Name
- Date
- Duration
- Number (the number dialled or the number reaching the *Google Pixel*)
- SIM card slot

The Monitoring Application also recorded the content of phone conversations, despite warnings about the unreliability of this feature. According to the Monitoring Application, on *Android 10* devices, the call recording feature can only record the device owner's voice, and not the voice on the other end. This warning was presented through the Monitoring Application's web portal when selecting the 'Call recordings' tab. That notification read:

> 'In Android 10, only the voice of the device user can be recorded. This requires a current version of [the application] and the activation of the accessibility service.'

Despite this warning, the Monitoring Application retrieved two, separate phone calls with Participant B and Participant C that included both the paper author's voice and the participants' voices. This feature required no intervention from us. Instead, the Monitoring Application appears to automatically record call audio as it happens.

Both Participant B and Participant C were alerted before the phone call that the call could be recorded by the Monitoring Application, and, when starting the phone call, both consented to having their voices recorded.

Once both calls were completed, recordings were logged by the Monitoring Application. We accessed the call recording easily – a simple click and download. The entirety of the calls had been recorded. Though the voices of Participant B and Participant C were quiet, they could easily be heard simply by turning up the volume on our computer.

Streaming capabilities – camera, microphone and screen

The Monitoring App provided three streaming capabilities for the *Google Pixel*. It could provide, through its web portal, a live stream of the *Google Pixel* camera's field of view, a live stream of the *Google Pixel*'s microphone audio, and a live stream of the *Google Pixel*'s screen, operating as a screen share.

The camera and microphone streaming features did not require the *Google Pixel* to be awake. The features also did not present any notification to the *Google Pixel* about the use of the device's cameras or microphone. However, when we tried to use the microphone live streaming feature while also on a call with Participant B, the Monitoring Application could not turn the feature on, as the microphone was already in use by a separate app (the phone).

When turned on for the first time, the screen-sharing feature triggered a warning notification on the *Google Pixel*.

The full warning read:

> 'While recording or casting, [Monitoring Application] can capture any sensitive information that is displayed on your screen or played from your device, including sensitive information such as audio, passwords, payment info, photos, and messages.'

The warning then allowed the paper author to either cancel or allow the screen-sharing feature.

However, once the *Google Pixel* granted permission to allow screen sharing, the warning box was not presented again until after the phone was restarted.

Further, when the Monitoring Application's screen-sharing feature was turned on, it required a 'screen-share' icon to be present in the notification bar of the *Google Pixel*, as shown below:

Figure 15: A screenshot of the Google Pixel's home screen when the Monitoring Application's screen share feature was turned on.

When turned on, and when given permission to access the *Google Pixel*'s screen, the screen-sharing feature captured every engagement the paper author made with the various apps installed on the *Google Pixel*. This feature could, in effect, reveal sensitive details that the Monitoring Application itself could not retrieve, including messages viewed and written in real time on various social media platforms.

The feature could not be used or turned on when the *Google Pixel* was asleep.

While we understand that a screen-share feature relies on the a device being awake, for many survivors of domestic abuse, this is a far from unlikely scenario. For the survivor who lives with their abuser, their cell phone activity is difficult to hide.

Particularly during the recent pandemic and shelter-at-home orders, a screen share feature poses a great risk because many individuals are stuck inside and attached even more closely to their mobile devices. *Some users have reported their screen time increased by more than 100 per cent since the shelter-in-place orders began in their states*.

WHY AN ANTI-MALWARE SCANNER IS NOT A CATCH-CALL SOLUTION

Following the experiment, the paper author ran a *Malwarebytes* scan on the *Google Pixel*. The *Malwarebytes* scan found the Monitoring Application and gave the option to remove it. He did.

From one perspective, this appears to be a simple 'fix'.

But for many, the option to remove these types of apps can be far more inaccessible. In fact, for survivors of domestic abuse, downloading and using an anti-malware scanner depends on a multitude of variables that cannot be controlled for by any cybersecurity company alone. If cybersecurity vendors were to act without the input and collaboration from domestic abuse advocates, they might design a product that actually puts domestic abuse survivors at greater risk of harm.

Because these types of apps can see the very activity that is occurring on a mobile device, it must be recognized that the downloading of an anti-malware scanner would also be viewed by a stalkerware-type application.

Our Monitoring Application experiment proved this.

When we ran a *Malwarebytes* scan on the *Google Pixel*, the Monitoring Application's central dashboard showed us that *Malwarebytes* was the 'last used app'. The Monitoring Application also revealed what apps were installed on the *Google*

Pixel, including *Malwarebytes*, along with a time stamp of the installation of *Malwarebytes*, and a link to *Malwarebytes*' *Google Play Store* profile. This means that, even if an abuser were unaware of *Malwarebytes*, they could easily click the link to find out more.

In speaking with domestic abuse advocates and intimate partner violence researchers, we learned that abusers can interpret the downloading of an anti-malware tool as a potential act of trying to limit their control over the survivor. These actions can be met with further abuse. Further, these actions will likely have to be explained by the survivor to the angered abuser.

If anti-malware scanners automatically removed stalkerware-type apps once detected, such removals could then, in effect, put survivors at greater risk of harm, making them have to answer why an abuser's digital control was removed.

Further, for many survivors of domestic abuse, the very option to download an anti-malware scanner is not available. They may share a device with their abuser and may not have full control of the device. If a survivor owns and manages their own device, an abuser may still have the device passcode to access the survivor's phone, making individual attempts to maintain privacy and security far more difficult. Such non-private passcodes are not unusual. In fact, many non-abusive relationships exhibit this behaviour. We should not forget that it can occur in abusive relationships, too.

Finally, cybersecurity vendors should consider that downloading and using an anti-malware scanner is not a comprehensive solution to the broader problem of tech-enabled abuse.

In our research for this paper, and for several pieces that *Malwarebytes* has written and published online, we learned that abusers can still obtain a survivor's private information without the use of stalkerware-type apps. If the abuser and the survivor are on the same mobile plan for their cell service, for instance, the abuser could retrieve call logs that include the numbers dialled.

Further, the automatic cloud storage provided by some mobile devices could reveal sensitive information without a survivor's knowledge. For instance, in our experiment, when we set up the *Google Pixel*, we agreed to many of the features that the device automatically suggested – including cloud backups of photos taken by the device.

If an abuser had the password to those cloud backups, they could see photos taken by the device, with no stalkerware-type app necessary.

Because of the different types of potential privacy invasions that do not require stalkerware-type apps, cybersecurity vendors should recognize that an anti-malware scan may not provide immediate help to a domestic abuse survivor. In fact, it could even give a false sense of security if the survivor's abuser was tracking information not through a stalkerware-type app, but through other means.

CONCLUSION

From our two-week experiment, we learned about the powerful, potentially invasive capabilities of these types of applications. The Monitoring Application revealed where the paper author lived, who he spoke to, when, how often, and about what. It revealed the photos he took and deleted, and it opened a digital portal into his home, complete with streaming audio and video.

Even in a controlled environment, these revelations were deeply upsetting.

The cybersecurity community has the power to help address these issues, but it should not assume that it has all the answers. As we said, the use of an anti-malware scanner is not available to every survivor, and even for those who understand the capabilities of stalkerware and the anti-malware tools that detect it, such a scan could put their life in further danger.

This is an issue in which cybersecurity vendors can help. It should be our responsibility to understand why this threat deserves our attention, and why domestic abuse advocates and researchers must be involved.

REFERENCES

[1] The State of Stalkerware in 2019. Secure List. October 2019. https://securelist.com/the-state-of-stalkerware-in-2019/93634/.

[2] Ruiz, D. International Women's Day: awareness of stalkerware, monitoring, and spyware apps on the rise. Malwarebytes. March 2020. https://blog.malwarebytes.com/stalkerware/2020/03/international-womens-day-awareness-of-stalkerware-monitoring-and-spyware-apps-on-the-rise/.