PI magazine .com

professional investigator magazine

$8.95

November/December 2022

Investigating Above All

BIGAMY INVESTIGATIONS: A BRIEF INTRODUCTION

RISK MANAGEMENT, LIABILITY, AND THE PRIVATE INVESTIGATOR

THE VALUE OF A PRIVATE INVESTIGATOR ASSOCIATION

You've Encountered an IoT Device, Now What?!

BY **ROBERT B. FRIED,** SENIOR VICE PRESIDENT, FORENSICS & INVESTIGATIONS, SANDLINE GLOBAL

Like many others, I have joined the trend to create a connected home. In our home we have many Wi-Fi enabled devices, including a blood pressure monitor, a dehumidifier, a doorbell, a door lock, garage doors, light bulbs/switches, security cameras, smart speakers, smart TVs, smoke alarms, sprinklers, thermostats, a vacuum, virtual assistants, and a washer/dryer. Notifications are sent to our mobile devices alerting us of device activity, including when the sprinklers have watered a zone, or when the dryer finishes a cycle. Putting aside any security and privacy concerns, these devices offer everyday conveniences in the palm of our hands. However, from an investigator's standpoint, these devices may hold a treasure trove of information!

OUR CONNECTED WORLD

In simplest terms, an Internet of Things (IoT) device is one that is connected to and controlled by the Internet. Why are they important? Recent statistics indicate that there are now billions of IoT devices on the market, and households, on average, contain nearly two dozen of these devices.[1]

Personally, I interact with my IoT devices using my Android phone via an app, and occasionally using my computer via an app or website. If I am online - my phone or computer is connected to a cellular or Wi-Fi network - with a few taps on a screen or clicks of a mouse, I can take care of several chores.

The apps and websites associated with IoT devices, provide users with the ability to monitor device usage and activity, or trigger reminders / notifications (based on settings, these may appear in the app or are sent via email or text message). This data may be presented in a variety of formats, including lists, charts, or graphs. Device manufacturers are frequently updating features and functionality – it's constantly evolving. Many devices provide data to users for free, while others offer paid subscription plans, based on the needs and wants of users. Typically, subscription plans provide enhanced features, functions, or storage. For example, a basic subscription for a doorbell stores video recordings for the last 60 days, while a premium subscription allows recordings to be stored for 180 days.

WHERE'S THE DATA?

Users can interact with IoT devices via mobile devices or computers, but associated data may be stored elsewhere. IoT devices may utilize internal memory, removable media, or cloud storage. Depending on storage capacity and configuration, data may be overwritten after a certain amount of data is saved or a period has passed. How can this data be accessed? Via an app, website, or directly from the device (extracting its removable media or attaching a data cable). It is important to consult with a digital forensics practitioner if an IoT device may be relevant to an investigation.

ENGAGE A DIGITAL FORENSICS PRACTITIONER

A digital forensics practitioner will be able to provide guidance related to a IoT device, including its function, any associated apps that may be installed on devices used to interact with it, where its data may be stored, and any requirements to access and subsequently collect this data in the most defensible and efficient manner.

It may be possible for data from IoT devices to be saved locally to a mobile device or computer. A digital forensics practitioner, utilizing forensic tools, can generate a forensic collection of a mobile device or a forensic image of a computer. To forensically collect the mobile device, a digital forensics practitioner will need the passcode to unlock the device, and any backup password (if enabled). To forensically image the computer, the digital forensics practitioner will need the login credentials or decryption key (if encryption is enabled).

An IoT device's internal memory may be accessed in several ways. For example, it may be possible for a digital forensics practitioner to connect the IoT device to a forensic workstation via USB cable (this may require powering down the device), access its data, and subsequently generate a forensic image. Alternatively, the forensics practitioner may be able to connect to / access the data from the IoT device via a web browser,

using a specific IP address; this may require administrator-level account credentials (username and password).

Regarding an IoT device's removable media, a digital forensics practitioner can extract the media from the device and subsequently generate a forensic image; to perform this process, it may be necessary to power down the device.

To access and forensically collect cloud storage utilized by an IoT device, a digital forensics practitioner will need administrator-level account credentials (and a two-factor authentication code, if enabled) to login to the associated cloud storage service. Depending on the service – if forensic tools can connect to it – a digital forensics practitioner may be able to generate a forensic copy of the data within the account. If obtaining a forensic copy of the data is not possible, it may be necessary to generate exports or reports from the data that is available. In certain cases, generating screen shots of the available data may be the only option to collect the data.

Data from IoT devices can be accessed and collected in various ways. It is important to discuss the various options and considerations with the digital forensics practitioner, and the other parties involved in the investigation; everyone must be on the same page regarding the overall process that will be performed, and the data that may be available.

PREPARE FOR THE INEVITABLE

As the number of IoT devices on the market increases, it is inevitable that these devices will be encountered during an investigation.

Here are several important things to remember about IoT devices:

- They are connected to the Internet, and other devices can interact with them.
- They may store data internally, on removable media, or in the cloud.
- There are typically different subscription plans available that may impact what functions, features, and data may be available. **PI**

REFERENCES:

Source: https://techjury.net/blog/how-many-iot-devices-are-there/

Robert B. Fried is a seasoned expert and industry thought leader, with over twenty years of experience performing data collections and forensic investigations of electronic evidence. He is the Senior Vice President and Global Head of Sandline Global's Forensics and Investigations practice. In this role, Robert leads the day-to-day operations of the practice, overseeing the forensic services offered to the firm's clients, including data collections, forensic analysis, expert testimony, and forensic consultation. Previously, Robert held senior-level positions within the digital forensic practices at global professional services firms. Additionally, Robert was a Computer Crime Specialist at the National White Collar Crime Center (NW3C), where he developed and instructed computer forensic and investigative training courses for federal, state, and local law enforcement agencies. He attained a BS and MS in Forensic Science, and certificates in Law Enforcement Science, Computer Forensic Investigation, and Information Protection and Security from the University of New Haven. Robert serves on the Board of Advisors for the Masters in Investigations program at the University of New Haven. He holds and actively maintains the following industry certifications: Access Data Certified Examiner (ACE), Certified Forensic Computer Examiner (CFCE), EnCase Certified Examiner (EnCE), GIAC Certified Forensics Analyst (GCFA), Chainalysis Cryptocurrency Fundamentals Certification (CCFC), Chainalysis Reactor Certification (CRC), and C4 Certified Bitcoin Professional (CBP). Robert is a licensed Professional Investigator in Michigan and is a licensed Private Investigator in New York. He is a frequent speaker at industry events, has been a guest on industry podcasts, and has been published in several professional publications. Robert is the author of Forensic Data Collections 2.0: The Guide for Defensible & Efficient Processes. Additionally, he is the author of PI Magazine's CyberSleuthing Department, where he shares insightful content on topics relating to digital forensics, eDiscovery, data privacy, and cybersecurity.