FEDERAL BUREAU OF INVESTIGATION TECHNICAL ANALYSIS BULLETIN

(U//FOUO) Internet of Things Devices Likely Present Both Opportunities and Potential Challenges for Law Enforcement Investigators

(U) PREPARED BY CYBER DIVISION/
TECHNOLOGY CYBER INTELLIGENCE UNIT
CO-AUTHOR OPERATIONAL TECHNOLOGY
DIVISION/TECHNICAL INTELLIGENCE UNIT

7 NOVEMBER 2019
FBI TAB039 20191107

(U) This document is classified: Unclassified//Law Enforcement Sensitive
(U) Technical Analysis Bulletin template approved for fiscal year 2020, as of 1 October 2019.

(U) LAW ENFORCEMENT SENSITIVE: The information marked (U//LES) in this document is the property of the Federal Bureau of Investigation and may be distributed within the federal government (and its contractors), U.S. intelligence, law enforcement, public safety or protection officials, and individuals with a need to know. Distribution beyond these entities without FBI authorization is prohibited. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. Information bearing the LES caveat may not be used in legal proceedings without first receiving authorization from the originating agency. Recipients are prohibited from subsequently posting the information marked LES on a website on an unclassified network without first obtaining FBI approval.

(U//FOUO) The FBI assesses Internet of Things (IoT)[a] devices very likely[b] provide useful digital evidence to law enforcement (LE) investigators, as long as the evidence is preserved and collected by device manufacturers or is stored locally on the device. The FBI also assesses subjects likely use IoT devices to hinder LE investigations and possibly monitor LE activity. The FBI makes these assessments with medium confidence,[c] based on observations of court proceedings, the demonstrated impact of IoT devices in recent LE investigations, and the FBI's own analysis of IoT devices.

(U//FOUO) The FBI assumes IoT devices are becoming more prevalent in homes worldwide. The FBI assesses IoT devices will provide new opportunities and challenges for LE over the next two years, as LE adapts to new technologies, incorporates them into operations, and uses them to aid investigations. Additional FBI reporting on how IoT device data is used in FBI investigations and the devices' impact on operations would improve the FBI's confidence in these assessments.

[a] (U) An IoT device, or "smart" device, is a non-traditional computing device that communicates to the Internet to send or receive data.

[b] (U) See Appendix A: Expressions of Likelihood.

[c] (U) See Appendix B: Confidence in Assessments and Judgments Based on a Body of Information.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) Source Summary Statement

(U//FOUO) Reporting in this technical analysis bulletin was derived primarily from open sources, composed of established information technology (IT) companies, as well as local and national US news organizations, and FBI reporting. Collection for this product occurred from July 2017 until 1 October 2019. The reporting was current as of 1 October 2019. Open source reporting was critical to the assessments contained herein because many state and local LE organizations provide the most examples to date of IoT devices and their data informing LE investigations. An increase in FBI and LE reporting regarding the use of IoT devices in investigations for evidence collection and operational successes would affect the confidence levels herein.

(U//FOUO) IoT Devices Very Likely Assist LE by Acting as Digital Witnesses for Corroboration and Lead Generation

(U//FOUO) The FBI assesses IoT devices have the potential to provide valuable data regarding device owners' movements in real-time and on a historic basis, which can be used to, among other things, confirm or contradict subject alibis or statements. This data may be stored by the device's manufacturers on the device itself or in a cloud environment, as well as with third parties. Such data, which can assist in the generation of leads and improve collection for investigations, may be accessible through US legal process, similar to information produced through the use of computers and mobile devices.

- (U) According to reporting from a global news organization with indirect access, in September 2018, a man was arrested for murdering his stepdaughter. The man staged the death as a suicide and claimed to have been at her house for only 15 minutes; however, police used security camera footage to show the man was at the victim's house when the victim's fitness tracker recorded the user's heart rate spike and stopped beating. The data helped establish the victim's likely time of death and refuted the suspect's alibi.[1]

- (U) On 11 January 2018, a technology website with indirect access reported on a German case, in which information associated with the subject's smartwatch health application was used as evidence in a rape and murder investigation. The subject reportedly was wearing the watch during the crime and appeared to have dragged the victim's body down a river embankment and climbed back up. The health application associated with the smartwatch categorized this activity as the user climbing stairs.[2]

- (U) According to open source reporting from an IT news organization with indirect access, on 29 July 2017, data from a pacemaker was used in an arson investigation. The suspect claimed to be asleep when the fire started before he managed to escape with some of his belongings; however, the data from his pacemaker revealed his heart rate and cardiac rhythms before, during, and after the fire were inconsistent with his version of events. The suspect was arrested for arson.[3]

- (U) According to open source reporting from a local news organization with indirect access, on 23 February 2016, data from a smartphone and smart water and electrical meters were used to help justify the arrest of a homicide suspect. The water and electrical usage data showed the home's water usage spiked following the victim's death, when the suspect claimed he was asleep in bed, indicating the suspect attempted to clean up the crime scene before notifying authorities of the victim's death.[4]

(U//FOUO) Data Generated from IoT Devices Very Likely Provides Key Evidence Collection in LE Investigations

(U//FOUO) The FBI assesses IoT devices very likely can be used to identify subjects of LE investigations by providing a new digital trail of evidence leading to subjects, resulting in more timely arrests. IoT devices are embedded with sensors and cameras; they typically are paired with a mobile app that requires users to register contact information and other forms of personally identifiable information (PII).

- (U) According to an online newspaper with indirect access, on 1 October 2019, a Colorado man released footage from his smart car's nine on-board motion-detecting cameras of an unknown woman keying his car. The man shared the footage with local LE and on social media to identify the woman and use the video of the incident as evidence of the crime.[5]

- (U) According to open source reporting from a news organization with indirect access, on 18 July 2019, a police department in Georgia worked with neighborhood residents to assist in an investigation of identity fraud and mail theft. One resident was able to capture an image of the subject's vehicle and tag number using Flock Safety license plate reader cameras. A different Flock camera was used to locate the vehicle in real-time and the information led police to the subject.[6]

- (U) According to open source reporting from a local news organization with indirect access, as of 17 September 2018, a South Florida police department was using automated license plate readers (ALPRs)[d] installed across the city and on patrol cars to help catch criminals. The ALPRs could run thousands of license plates at once, aid in catching unpaid parking ticket offenders, locate stolen vehicles, or catch wanted felons.[7]

- (U) According to open source reporting from an IT news organization with indirect access, on 29 November 2017, police worked with an IoT company to deploy mobile high-definition security cameras to assist in the investigation of a suspected serial shooter. The cameras were linked to a wireless, solar-powered gunshot detection system, which allowed LE to identify the vehicle used during the shootings and make an arrest.[8]

[d] (U) ALPRs are high-speed, computer-controlled camera systems that are typically mounted on street poles, streetlights, highway overpasses, mobile trailers, or attached to police cars. ALPRs capture all license plate numbers in view; photos; and location, date, and time data. All data are immediately uploaded to a central server.

(U//FOUO) Subject Use of IoT Devices Likely Pose Challenges to LE Personnel's Safety, Investigations, and Evidence Collection

(U//FOUO) The FBI assesses IoT devices likely pose new challenges to LE personnel, negatively affecting LE effectiveness and pose security challenges for LE personnel. Most IoT devices contain sensors and cameras, which generate an alert or can be remotely accessed by the owner to identify activity in and around an owner's property. If used during the execution of a search, potential subjects could learn of LE's presence nearby, and LE personnel could have their images captured, thereby presenting a risk to their present and future safety. Additionally, in some instances IoT device data may be stored only locally on a device, which can hinder LE access to key evidence if subjects or victims of crimes are unwilling to cooperate with LE.

- (U) According to open source reporting from a local news organization with indirect access, as of 24 August 2018, home security systems posed issues for LE, as the owners of the systems posted images and messages about possible crimes on social media before contacting the police for a proper investigation. This allowed individuals to post and accuse others of crimes publicly before any formal inquiry.[9]

- (U//FOUO) On 18 April 2018, the FBI released a report warning of the threat posed to LE from the use of panoramic camera bulbs by subjects under investigation due to the bulb's ability to surreptitiously record when motion is detected. The report addressed concerns that the bulbs could alert subjects of LE presence prior to entering a residence, provide the location of LE officers in a standoff situation, and surreptitiously record LE-executed searches.[10]

- (U) According to open source reporting in January 2018 from a news organization with indirect access, data from a smartphone's health-tracking application was only saved locally on the device and encrypted cloud backups. Because of this, the phone maker could not provide the data if served with a warrant. In a recent German murder case, police were forced to hire a Munich firm to break into the subject's phone because the subject refused to provide investigators with a password.[11]

- (U//LES) According to FBI employees with direct access, on 25 July 2017, FBI personnel approached a residential home to serve a search warrant and detected a video doorbell. Through the Wi-Fi doorbell system, the subject of the warrant remotely viewed the activity at his residence from another location and contacted his neighbor and landlord regarding the FBI's presence there.[12]

(U) Perspective

(U//FOUO) The use of IoT devices has increased exponentially the size and scope of data held by technology companies and other third parties. This data includes geo-location, personal health, and behavioral information. While some data may reside on an IoT device, much of the data is maintained in the cloud. LE organizations seeking evidentiary information collected through IoT devices need to consider where information is stored, whether data can be obtained through legal process, and, if so, whether that data is available in an unencrypted format.

(U//FOUO) Over the past couple of years, technology companies have fought LE search warrants for IoT device data because they argue such requests can violate the device users' Fourth Amendment, and in some cases First Amendment, rights as the lawfully requested data may not be easily segregated from other IoT data that reflects expressive activity, which they argue may fall outside the request's scope. Because companies that collect IoT data sets rely upon users' trust, they often claim additional responsibilities to protect user information. A 2018 law review article from a US university characterized the role of technology companies as "surveillance intermediaries" finding themselves situated between LE requests and the public's personal data. As a result, the article's authors argue companies are uniquely positioned to decide whether LE requests constitute potential government overreach. They may elect to challenge these requests through appropriate legal channels or, alternatively, have been observed taking an unusually extended time to process requests. Beyond these affirmative steps such providers might take to limit LE acquisition of IoT information, strict data retention policies and providers' inability to decrypt encrypted communications serve as additional inhibitors to using this information to advance LE investigations.

UNCLASSIFIED

(U) IoT Companies Partnering with LE Likely Causing Additional Privacy Concerns for US Citizens

(U) Beginning in July 2019, several online news websites reported on a partnership between one of the largest IoT doorbell camera companies and LE. The company gives free products to LE to pass out to the community to enhance the local LE surveillance network. In return, LE is contractually obligated to promote the product and encourage the community members to download an app for sharing suspicious incidents. Additionally, if individuals accept the free device, they are required to turn over the surveillance footage whenever LE asks. This arrangement allows LE to obtain footage without having to issue warrants or subpoenas to the device manufacturer. Additionally, the company provided LE scripts to engage with the public and request footage directly from device owners without going through the courts.[i] As of 26 September 2019, the company has partnered with more than 400 police departments in the country, according to another online news outlet.[ii]

(U) Online privacy advocates are concerned with the widespread adoption of these devices, paired with social networking applications, which are being used to share suspicious incidents and create a surveillance program without regulatory oversight. Privacy advocates believe this will result in racial profiling issues and privacy abuse as these cameras record activities up to 30 feet away and can record anyone without their knowledge or consent. Additionally, the company includes language in their terms of service for the community app that allows the company full permission to the content to do with as it sees fit without any consent or compensation from the user who generated the content.[iii]

(U) *Sources*

[i] (U) Online news article | Techdirt.com | "Amazon's Free Doorbell Cameras Only Cost Law Enforcement Agencies Their Dignity and Autonomy" | 30 July 2019 | http://www.techdirt.com/articles/20190725/16252942657/amazons-free-doorbell-cameras-only-cost-law-enforcement-agenceis-their-dignity-autonomy.shtml | accessed on 2 October 2019.

[ii] (U) Online news article | Wired.com | "The Ringification of Suburban Life" | 26 September 2019 | http:www.wired.com/story/ring-surveillance-suburbs | accessed on 2 October 2019.

[iii] (U) Online news article| Buzzfeed News | "Ring is Using Its Customers' Doorbell Camera Video for Ads. It Says It's Allowed To." | 7 June 2019 | http://www.buzzfeednews.com/article/daveyalba/amazon-ring-doorbell-company-useing-security-footage-for-ads | accessed on 2 October 2019.

(U//FOUO) This is the first FBI product that addresses how IoT devices affect LE operations and investigations. Previous FBI products on IoT devices have focused on IoT device vulnerabilities and how cyber actors have targeted the devices. The 15 August 2017 FBI Intelligence Bulletin, titled "(U//FOUO) IoT Devices Vulnerable to Compromise and Exploitation by Cyber Actors," focused on how cyber actors were exploiting IoT device vulnerabilities, how devices were used in destructive cyber attacks, and the ease in which cyber actors could identify vulnerable devices. The 26 July 2018 FBI Intelligence Bulletin, titled "(U//FOUO) Cyber Actors Almost Certainly IoT Botnets as Proxies To Anonymize and Facilitate Malicious Cyber Activities," highlighted how cyber actors used compromised IoT devices as intermediaries for Internet requests to route malicious traffic.

(U) Outlook

(U//FOUO) The FBI assesses IoT devices will provide new opportunities and challenges for LE during the next two years, as LE continues to adapt to new technologies, incorporate them into operations, and use them to aid investigations. Widespread use of IoT device data in investigations by LE has yet to occur due to limited knowledge within state, local, and federal LE agencies about how the devices work, how data is collected, and where data is stored. Multiple efforts, however, are underway at LE agencies to gain a better understanding of IoT device functionality, data-collected opportunities, and usefulness to future investigations. The number of devices in use is expected to rise to 20 to 50 billion by 2020, and IoT devices continue to collect more information, which can help LE establish patterns of life, identify departures from daily routines, and help assess the accuracy of alibis or other key investigative details.

(U//FOUO) Based on backlash from the public on privacy issues associated with data from IoT devices being used in LE investigations in recent years, IoT manufacturers may decide to implement stronger device encryption and store data for shorter amounts of time. Both efforts would complicate LE efforts to obtain evidence and limit the companies' ability to respond to lawful LE requests, including court-ordered production of the information. Additionally, device manufacturers are likely to continue to be reluctant to comply with LE requests for access to password-protected devices or applications on First and Fourth Amendment grounds, in an attempt to prevent government overreach and protect user privacy.

(U) If you would like to provide qualitative feedback on this product, please send an email to the appropriate address with the product title as the subject line: DI_Customer_Feedback@fbi.gov; DI_Customer_Feedback@fbi.sgov.gov; or DI_Customer_Feedback@fbi.ic.gov.

(U) Cyber Division's Technology Cyber Intelligence Unit (TCIU) and Operational Technology Division's Technical Intelligence Unit (TIU) of the FBI prepared this technical analysis bulletin. Comments and queries may be addressed to the TCIU Unit Chief at 1-703-633-5566 or the TIU Unit Chief at 1-703-985-2901.

(U) Appendix A: Expressions of Likelihood

(U) Phrases such as "the FBI judges" and "the FBI assesses," and terms such as "likely" and "probably" convey analytical judgments and assessments. The chart below approximates how expressions of likelihood and probability correlate with percentages of chance. Only terms of likelihood should appear in FBI products; the chart includes terms of probability strictly for comparison, as they sometimes appear in reporting of other government agencies. Furthermore, the FBI does not arrive at judgments through statistical analysis and will not use terms of probability to convey uncertainty in FBI external intelligence products.

UNCLASSIFIED

Terms of Likelihood	**Almost No Chance**	**Very Unlikely**	**Unlikely**	**Roughly Even Chance**	**Likely**	**Very Likely**	**Almost Certain(ly)**
Terms of Probability	Remote	Highly Improbable	Improbable (Improbably)	Roughly Even Odds	Probable (Probably)	Highly Probable	Nearly Certain
Percentages of Chance	1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%

(U) Table showing terms of likelihood aligned with terms of probability and percentages of chance.

(U) Appendix B: Confidence in Assessments and Judgments Based on a Body of Information

(U) Confidence levels reflect the quality and quantity of the source information supporting a judgment. Consequently, the FBI ascribes high, medium, or low levels of confidence to assessments, as follows:

(U) **High confidence** generally indicates the FBI's judgments are based on high quality information from multiple sources. High confidence in a judgment does not imply the assessment is a fact or a certainty; such judgments might be wrong. While additional reporting and information sources may change analytical judgments, such changes are most likely to be refinements and not substantial in nature.

(U) **Medium confidence** generally means the information is credibly sourced and plausible but not of sufficient quality or corroborated sufficiently to warrant a higher level of confidence. Additional reporting or information sources have the potential to increase the FBI's confidence levels or substantively change analytical judgments.

(U) **Low confidence** generally means the information's credibility or plausibility is uncertain, the information is too fragmented or poorly corroborated to make solid analytic inferences, or the reliability of the sources is questionable. Absent additional reporting or information sources, analytical judgments should be considered preliminary in nature.

(U) Endnotes

[1] (U) Online news article | *Fortune* | "Fitbit Data Implicates Another Murder Suspect, This Time a 90-Year-Old Man Accused of Killing His Stepdaughter"| 4 October 2018 | http://fortune.com/2018/10/04/fitbit-activity-data-murder-san-jose | accessed on 19 October 2018.
[2] (U) Online news article | Apple Insider | "Apple's Heath app provides key evidence in German rape & murder case" | 11 January 2018 | https://appleinsider.com/articles/18/01/11/apples-health-app-provides-key-evidence-in-german-rape-murder-case| accessed on 24 August 2019.
[3] (U) Online news article | Wired.com | "Your own pacemaker can now testify against you in court" | 29 July 2017; https://www.wired.com/story/Your-own-pacemaker-can-now-testify-against-you-in-court/ | accessed on 08/24/2019.
[4] (U) Online news article | 5 News Online | "Bentonville PD Says Man Strangled, Drowned Former Georgia Officer" | 23 February 2016 | https://5newsonline.com/2016/02/23/bentonville-pd-says-manstrangled-drowned-former-georgia-officer/ | accessed on 24 August 2019.
[5] (U) Online news article | Daily Mail UK | "Woman is caught keying a Tesla in school parking lot causing $2,000 worth of damage by the car's NINE on-board cameras" | 1 October 2019 | http://www.dailymail.uk/news/article-7525115/Woman-caught-keying-Tesla-vehicles-nine-board-cameras.html | accessed on 1 October 2019.
[6] (U) Online newspaper article | *Reporter Newspaper* | "Sandy Springs Police charge man with mail theft, identity fraud" | 18 July 2019 | https://www.reporternewspapers.net/2019/07/18/sandy-springs-police-charge-man-with-mail-theft-identity-fraud/ | accessed on 27 September 2019.

[7] (U) Online news article | 7 News Miami | "Hi-tech help; New technology is helping police catch crooks" | 17 September 2018 | https://wsvn.com/news/special-report/h-tech-help-new-technology-is-helping-police-catch-crooks/ | accessed on 27 December 2018.
[8] (U) Online news article | IoT World Today | "How IoT security devices helped nab a suspected serial shooter" | 29 November 2017 | http://www.iotworldtoday.com/2017/11/29/how-iot-security-devices-helped-nab-a-suspected-serial-shooter/ | accessed on 24 August 2019.
[9] (U) Online news article | Freep | "How doorbell cams are creating dilemmas for police, neighborhoods" | 24 August 2018 | https://wwww.freep.com/story/news/local/michigan/2018/08/23/doorbell-camera-videos-ring-police/1000358002 | accessed on 24 August 2018.

[10] (U//FOUO) FBI | SIR | 18 April 2018 | 18 April 2018 | "(U//FOUO) Panoramic Camera Bulb Capabilities Could Pose Potential Risk to Law Enforcement" | UNCLASSSIFIED//FOR OFFICIAL USE ONLY | UNCLASSIFIED//FOR OFFICIAL USE ONLY | Source is an officer of another LE agency.
[11] (U) Online news article | Apple Insider | "Apple's Heath app provides key evidence in German rape & murder case" | 11 January 2018 | https://appleinsider.com/articles/18/01/11/apples-health-app-provides-key-evidence-in-german-rape-murder-case| accessed on 24 August 2019.
[12] (U) FBI | SIR | 28 July 2017 | 25 July 2017 | "(U) Video Doorbell Devices Pose Risk to Law Enforcement in New Orleans, Louisiana as of 25 July 2017" | UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE; UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE | Source is an FBI agent.