Cellebrite

Domestic Terrorism

Crime and Terrorism Have Changed: Today's Investigators Rely on Digital Evidence

BY CHRISTIAN QUINN

SENIOR DIRECTOR OF GOVERNMENT AFFAIRS
FOR BROOKS BAWDEN MOORE, LLC

CONSULTANT FOR CELLEBRITE

Crime and Terrorism Have Changed. Today's Investigators Rely On Digital Evidence

Illicit activities such as human trafficking, gang crime, illegal gun sales, organized crime, and even terrorism have all become highly dependent on digital technology to coordinate activities among co-conspirators and to conceal the identities and actions of those involved. Nefarious planning and deals that may have once occurred in back alleys, business fronts, or secret locations now occur primarily in the digital world using cell phones and other connected devices.

Violent crime, including gun violence, is surging in many communities. In addition, the threat of terrorism has grown increasingly complex, with recent attention shifting from international terrorism to homegrown violent extremism.

In April 2021, the Office of the Director of National Intelligence, on behalf of the U.S. Intelligence Community (IC) released its assessment of the threats posed to the United States.[1] In response, U.S. Senate Majority Whip Dick Durbin (D-IL), Chair of the Senate Judiciary Committee, noted the following in an official statement:

> *Specifically, the IC assesses that "racially or ethnically motivated violent extremists" are most likely to conduct mass-casualty attacks against civilians, while violent militia extremists will continue to target law enforcement and government personnel and facilities. The assessment warns that the likelihood and lethality of domestic terrorist attacks may increase in 2021.*[2]

Concern about these issues is bipartisan. The ranking member on the Senate Judiciary Committee, Senator Charles Grassley, stated in March 2021:

> *"As we move forward, I encourage both houses of Congress to review not just the events of January 6, but also domestic violent extremism across the board and the threat that it brings to our families and communities."*

- In April 2021, a 28-year-old Texas man was arrested for a plot to bomb Amazon data centers in Northern Virginia. The investigation began when Seth Aaron Pendley, allegedly using the online pseudonym, "Dionysus," posted alarming statements on MyMilita.com. The investigation was initially conducted in large part, in cyberspace.[3] Unfortunately, espousing extremist views online is not a novel phenomenon, nor does it always result in law enforcement interdiction before people are harmed.

- In June 2014, Patriot Movement extremists, Jerad and Amanda Miller, executed two Las Vegas police officers who were eating lunch, and then killed a community member who tried to intervene. They died following a shootout with responding officers. Before the event, they habitually espoused extreme anti-government views online including in the days before the killings that read, "To stop this oppression, I fear, can only be accomplished with bloodshed."[4]

- In May 2021, 39-year-old John Benjamin Thornton, of New Mexico was arrested and charged with transmitting an interstate commerce communication containing a threat to injure another. The FBI learned that Thornton allegedly sent text messages to people in Texas and Florida indicating that he was going to murder employees at a computer company, and then attempt to assassinate the President of the United States.

  FBI agents obtained a warrant on May 21, 2021, to locate Thornton's cell phone.[5] A defense attorney for Thornton stated that the text messages were taken out of context and were "simply political expression." [6]

Differentiating Between Distasteful and Destructive

In a democratic society that values free speech, one can espouse views that may be perceived by most people to be immoral and distasteful but still not necessarily be illegal. This creates a challenge for law enforcement who must differentiate between *protected speech* and that which incites violence or activities furthering criminal actions.

Conspiracy crimes, whether motivated by profit, ideology, or group membership, generally involve a foundational offense coupled with overt acts that constitute degrees of participation, and therefore, culpability. Laws governing this type of activity often incorporate aggravated penalties and/or expanded authority for investigation depending on the extent of an individual's involvement.

Law enforcement must always maintain a solemn regard for civil rights and privacy. However, when lawfully authorized, specialized tools are needed that can see beyond what is posted online publicly to disrupt criminal activities and safeguard communities. These resources allow investigators to examine and understand the nature of a subject's communications, establish links between criminal actors, and see the topics that they have researched. Investigators often uncover financial transactions, location information that reveals proximity to events, and other information to help them gather actionable insights to prevent violence or hold accountable those who have already committed criminal or terrorist acts.

Cyber-enabled Crime Has Drastically Increased

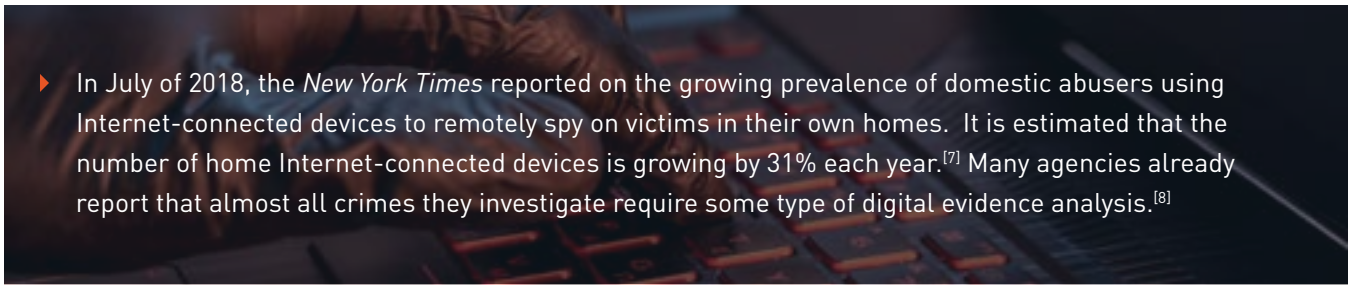
The global pandemic forced most conventional businesses to rapidly migrate to more digital practices. Criminal enterprises were no exception. The world was already becoming increasingly inter-connected through the "Internet of Things," which allowed certain types of criminal activity to scale significantly during the past few years. Perpetrators of child exploitation, organized crime, human trafficking, fraud, identity theft, gun trafficking, and even terrorism all benefit from the anonymized, connected nature of digitally linked networks.

An example of this phenomenon can be observed in gang-related homicide investigations. In recent years, multiple gruesome killings have occurred along the East Coast from Virginia to New York. Dismembered bodies of missing persons have been found in shallow graves in suburban parks and remote fields. Most of the victims were murdered for suspicion of cooperating with law enforcement or otherwise punished for a perceived insult to a gang.

Gang leaders, often referred to as "shot callers," routinely order killings from a distance—many times from within prison or even outside the country. To substantiate that the orders have been carried out, messages, frequently including photos or videos of the crime, are transmitted to gang leadership.

It is not uncommon to discover that video exists of a homicide, often with those involved deliberately ensuring that they appear in the video while actively involved in the murder to gain status in the gang. To close cases of this nature, provide answers to surviving families, and deliver justice for victims, investigators increasingly rely on digital evidence, including the analysis of numerous devices, social media accounts, and evidence stored in the Cloud.

Cases of lone offenders using Internet-connected devices to harass and stalk victims are also reportedly expanding. Devices such as locks, speakers, thermostats, lights, and security cameras are increasingly being used by suspects as instruments of harassment, monitoring, revenge, and control.



- In July of 2018, the *New York Times* reported on the growing prevalence of domestic abusers using Internet-connected devices to remotely spy on victims in their own homes. It is estimated that the number of home Internet-connected devices is growing by 31% each year.[7] Many agencies already report that almost all crimes they investigate require some type of digital evidence analysis.[8]

Technology Offers More Investigative Opportunities and More Challenges

The storming of the United States Capitol on January 6, 2021 resulted in arguably one of the most expansive criminal investigations since the terrorist attacks on September 11, 2001. More than 400 suspects have already been identified and charged in the event that left five people dead and numerous law enforcement officers injured.

To date, FBI Agents have executed nearly 1,000 search warrants in all 50 states and the District of Columbia, many of them seeking digital evidence held by telecommunications and technology companies. Some suspects reportedly attempted to thwart investigators, going so far as to throw away their cell phones or even attempting to destroy them in microwave ovens. The Justice Department referred to this investigation in court as, "one of the largest in American history, both in terms of the number of defendants prosecuted and the nature and volume of the evidence." [9]

Court documents reveal the extent of digital evidence sought in some cases related to the Capitol breach. *The Washington Post* reported that in one case, investigators lawfully gathered more than 12,000 pages of data from a suspect's phone (after obtaining a search warrant based on probable cause) using a solution from Cellebrite, a technology company offering investigators effective tools to unlock cell phones, and decrypt and extract data contained on devices. In addition, the search yielded 2,600 pages of Facebook records and 800 digital photos and videos.

Vehicles have become so dependent on digital technology that a shortage of computer chips has impacted inventories and increased prices and wait times for many new cars. This shift in automobile design has already yielded several innovative tools focused on vehicle digital forensics. Data related to telemetry and performance may be locally stored within the vehicle's systems or communicated back to the manufacturer to enable certain "smart" features such as maintenance and warranty notifications. Specific information related to turn-by-turn navigation, speed, acceleration, and braking is sometimes available as well.

Connected "infotainment" systems may contain information related to cell phones, which have previously synced with the vehicle via USB cable or Bluetooth, including GPS navigation, call logs, contacts, text messages, and apps installed on the device. [10] Collectively, this information allows investigators to view driver patterns and sometimes passenger behavior. In a criminal investigation, the timeline of car doors opening, seat belts fastening, weight detected on a seat for airbag monitoring, lights activating, and location information can provide a substantial amount of pertinent information to help re-create event sequences.

Ronald French, a grandfather of eight, had been missing for more than three weeks when his lifeless body was found in a cornfield in Kalamazoo County, Michigan in June 2017. Forensic evidence at the scene indicated that he had been bound and dragged behind a vehicle so violently that his skull was partially flattened. French's 2016 Chevy Silverado pick-up was stolen at the time of his disappearance.

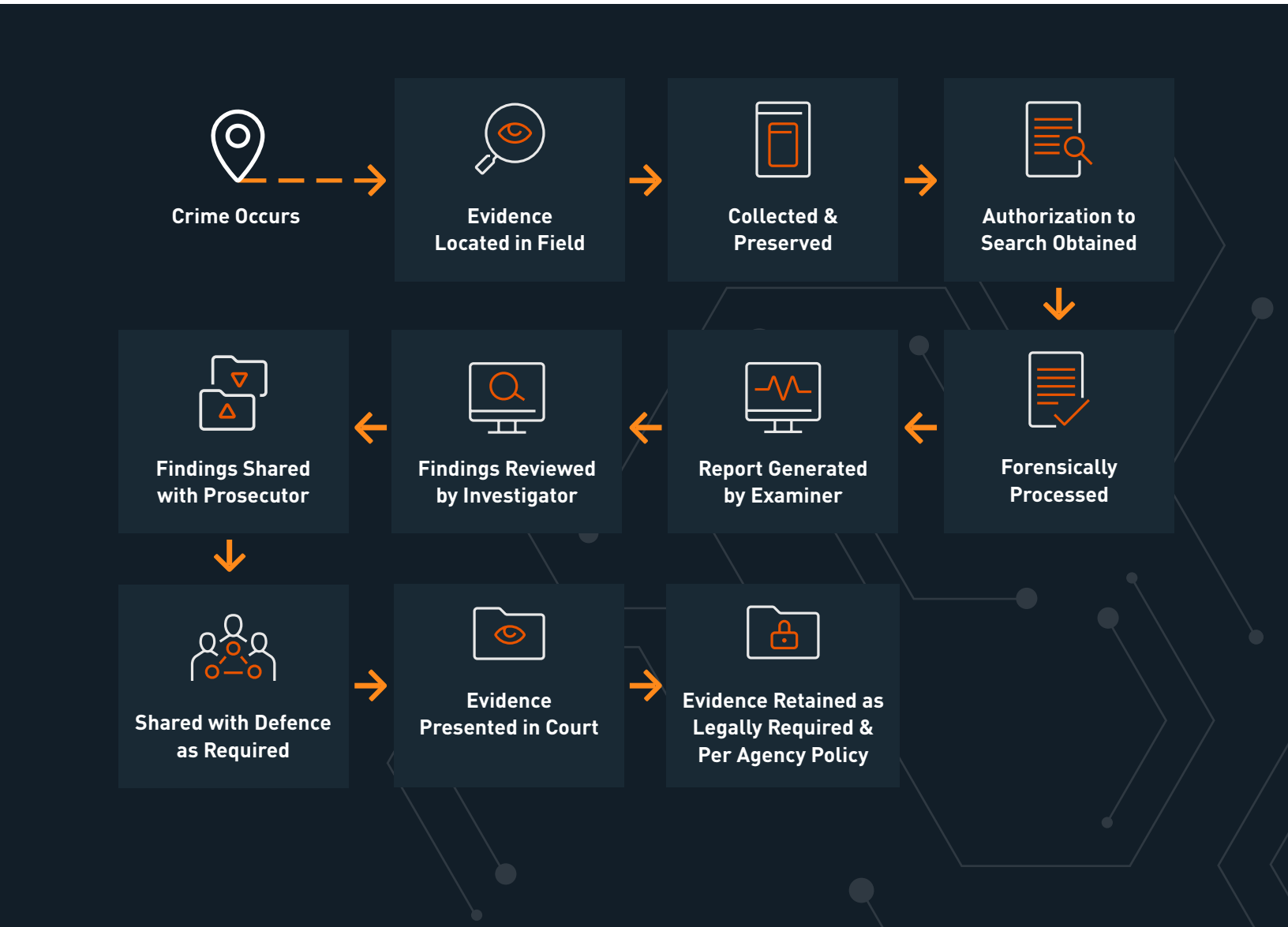
Detectives investigated the case to no avail. More than two years later, investigators directed their attention back to French's pick-up truck. Leveraging digital forensic tools, they discovered time-stamped audio recordings of someone else's voice using the hands-free controls to play the radio at the time of French's murder. That evidence led to the arrest of 32-year-old Joshua Wessel. [11]

The Digital Evidence Journey

Every year sees an exponential increase in the prevalence of digital technology such as smartphones, tablets, laptops, wearable technology, cloud storage, inter-connected household devices, video game consoles, and other emergent technologies which may hold evidence.

In one case, a murdered woman's Fitbit log and Facebook activity offered key evidence leading to the arrest of her husband who alleged she had been killed by a home intruder. [12] During a spree of hate-crimes in Texas, four defendants used a dating app to locate, lure, and brutally victimize at least nine victims. The victims were specifically targeted for their sexual orientation. [13]

As the availability of digital evidence increases, the need for effective forensic examinations also grows. The time required to complete digital forensic examinations is dependent on electronic processes and the number of devices and volume of data to be analyzed. There is no way to "work faster" without the appropriate tools to complete the analyses, and sufficient personnel who have the training to complete this specialized work. Regardless of the nature or type of cases, most digital evidence follows a similar path as illustrated in the graphic below.



What Kind of Tools Are Needed?

Encryption to secure access to devices and safeguard the data held within them is a good thing. This technology ensures privacy and affords the average consumer much needed options for cybersecurity. However, criminal actors often leverage such features to conceal dangerous planning and evidence of prior offenses. Unfortunately, some technology companies not only fail to assist law enforcement in investigations, but they also actively engineer themselves out of certain processes so they don't even have the ability to provide assistance even if legally ordered to do so. As companies move toward end-to-end encryption across entire platforms, the difficulty faced by investigators who need to access digital evidence will only increase.

Technical challenges are further complicated by inconsistent court rulings regarding how investigators may lawfully gain access to encrypted devices. Some courts have ruled that a suspect cannot be compelled to provide the passcode to a cell phone because it would constitute a testimonial act, which violates their Fifth Amendment right against self-incrimination. Other courts have upheld law enforcement compelling a suspect to place their thumb on a locked device to open it using a biometric feature. Most tangentially relevant Supreme Court precedents related to this specific topic predate the ubiquity of smartphones.

Advances in technology will likely continue to create similar challenges. Investigators may have to adopt tactics, such as operational planning that prioritizes the retrieval of digital evidence in a state so that it can be preserved for later forensic examination. Ultimately, investigative challenges posed by encryption could be addressed through "lawful access" statutes that would increase the ability for law enforcement to obtain digital evidence when lawfully authorized to do so.

In the absence of a lawful access statute, however, having effective tools to forensically unlock devices is essential to help law enforcement retrieve digital evidence when lawfully authorized. Strong analytics capabilities are also required to connect the dots between disparate pieces of information to provide investigators with a visual overview of the entire case. Ultimately, the goal is to adopt complete, end-to-end solutions that facilitate timely access, streamline workflows, preserve the best evidence, and produce reports that are both demonstrative for courts, and offer actionable insights for continued investigation.

Devices often hold evidence, but increasingly, they also serve as a medium to utilize apps offering encrypted communication and/or cloud-based data storage. Ironically, the Cloud offers digital investigators key advantages in their own work.

First, the Cloud offers investigators a more cyber-secure, cost-effective option for storing digital evidence. Digital forensic reports tend to be large data files. These must be maintained in a manner where access is controlled and the validity of the data can be authenticated. Furthermore, the original digital evidence examined must be preserved for both the prosecution of cases and in accordance with local data-retention laws that apply to government entities.

In addition to the advantages of storing data in the Cloud, many computing processes also take place on remote servers. This is also advantageous and usually more cost-effective over time. As digital forensic processes become increasingly robust, agencies may struggle to maintain sufficient computer processing capacity on their own premises. Some agencies report having spent considerable resources to acquire powerful computers typically used for gaming in an effort to keep pace with these demands only to find that the machines are already obsolete in less than two years. Leveraging the Cloud to outsource these complex processes is increasingly a more sensible option.

What About Privacy Concerns?

Many privacy coalitions have recently increased their advocacy to have "surveillance technology" banned for use by law enforcement. Specifically, some have cautioned that the breaching of the Capitol on January 6, 2021 should not open doors to any increased utilization of technical tools to conduct investigations. It is important to note that in the United States, most digital forensic tools are already regulated by relatively recent Supreme Court decisions. While clear guidance as to *how* agencies may lawfully unlock devices is lacking, specific direction as to when a search warrant is required is not. Furthermore, the technology discussed in this article focuses on tools used to investigate crimes and threats that can only be utilized with actual possession of a device. In short, law enforcement must have a device in hand, and then apply for, and obtain a warrant before searching its contents.

In 2014, the Supreme Court unequivocally declared that a search warrant is required to search the digital contents of a device. The device in the case of *Riley v. California* was a cell phone, but the interpretation generally applies to similar devices as well as peripheral instruments used in conjunction with cell phones, such as smart watches that sync with the phone for the purpose of sending or receiving text messages.

The *Riley* decision makes allowances for preserving access to a device, such as changing or disabling a passcode, during the time it takes to obtain a search warrant. Several other precedents, including the 2018 ruling in *Carpenter vs. United States*, have extended privacy protections to data stored by a 3rd party, such as cell site location information and call detail records.

Conclusion

Emergent technologies have changed the nature of crime and extremist threats that are unfortunately increasing and becoming more complex. Law enforcement agencies tasked with keeping communities safe and providing justice for victims must assess their current investigative resources to determine if they have sufficient solutions to address the wave of digital evidence that has become the norm, rather than the exception in most major investigations.

Safeguarding privacy and individual rights does not have to be at odds with maximizing opportunities to capitalize on digital investigative resources. Crafting sound policies and being deliberately attentive to developing legal trends can help law enforcement and the communities they serve strike an appropriate balance that equitably serves all stakeholders.

About the Author

Christian Quinn is the Senior Director of Government Affairs for Brooks Bawden Moore, LLC. He completed a 24-year law enforcement career, previously serving as a senior leader with the Fairfax County (VA) Police Department. As a capstone to his tenure, Mr. Quinn led the establishment of a new Cyber & Forensics Bureau to account for emergent trends related to digital evidence, technical investigations, and biometric identification.

Mr. Quinn serves on the International Association of Chiefs of Police's Communications & Technology Committee, and the Artificial Intelligence and Cyber sub-committees. He holds a Master of Forensic Sciences Degree from The George Washington University and is a graduate of the FBI National Academy in Quantico, Virginia.

End Notes

[1] Office of the Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community, (Apr 9, 2021), as retrieved 05-27-21 via: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.

[2] Committee on the Judiciary, Durbin Statement on DNI Assessment on Threat Posed by Domestic Violent Extremists, (Mar 18, 2021), as retrieved 05-27-21 via: https://www.judiciary.senate.gov/press/dem/releases/durbin-statement-on-dni-assessment-on-threat-posed-by-domestic-violent-extremists

[3] Hand, Mark. "Texas Man Charged With Planning To Blow Up Ashburn Data Center," Patch (April 12, 2021), as retrieved 05-27-21 via: https://patch.com/virginia/arlington-va/texas-man-charged-planning-blow-ashburn-data-center

[4] Shoichet, Catherine E. "Killer Las Vegas couple posted anti-government views online," CNN.com, (June 9, 2014), as retrieved 05-27-21 via: https://www.cnn.com/2014/06/09/justice/las-vegas-shooting-couple/index.html

[5] KFOX Staff. "Las Cruces man accused of plotting to kill President Biden." (May 26, 2021). https://kfoxtv.com/news/local/report-las-cruces-man-accused-of-plotting-to-kill-president-biden

[6] Associated Press. "Lawyer: Las Cruces resident denies threatening to kill Biden." (May 27, 2021). https://www.daily-times.com/story/news/2021/05/27/las-cruces-man-denies-plot-to-kill-president-joe-biden/7474867002/

[7] Bowles, Nellie. " Thermostats, Locks and Lights: Digital Tools of Domestic Abuse," New York Times (June 23, 2018). https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html

[8] Philipp, Joshua. "Nearly Every NYC Crime Involves Cyber, Says Manhattan DA," The Epoch Times (March 2, 2013). http://www.theepochtimes.com/n3/1476827-nearly-every-nyc-crime-involves-cyber-says-manhattan-da/

[9] Harwell, Drew and Timberg, Craig. " How America's surveillance networks helped the FBI catch the Capitol mob," Washington Post, (April 2, 2021), as retrieved 06-01-21 via: https://www.washingtonpost.com/technology/2021/04/02/capitol-siege-arrests-technology-fbi-privacy/

[10] Solon, Olivia. " Insecure wheels: Police turn to car data to destroy suspects' alibis," Washington Post, (Dec. 28, 2020), as retrieved 06-25-21 via: https://www.nbcnews.com/tech/tech-news/snitches-wheels-police-turn-car-data-destroy-suspects-alibis-n1251939

[11] Solon, " Insecure wheels"

[12] Watts, Amanda. " Cops use murdered woman's Fitbit to charge her husband," CNN, (April 26, 2017), as retrieved 06-04-21 via: https://www.cnn.com/2017/04/25/us/fitbit-womans-death-investigation-trnd/index.html

[13] Oliveira, Nelson. " Another Texas man admits using Grindr to target gay men, beat them up and rob them," New York Daily News, (June 4, 2021), as retrieved 06-04-21 via: https://www.nydailynews.com/news/national/ny-dallas-texas-man-pleads-guilty-violent-grindr-attacks-robberies-gay-men-20210604-xbtkq5ucmjb6tbg6zajb2qcsm4-story.html

About Cellebrite

Cellebrite's mission is to enable its customers to protect and save lives, accelerate justice and preserve privacy in communities around the world. Cellebrite is the global leader in Digital Intelligence solutions for the public and private sectors, empowering organizations to master the complexities of legally sanctioned digital investigations by streamlining intelligence processes. Trusted by thousands of leading agencies and companies in more than 140 countries, Cellebrite's Digital Intelligence platform and solutions transform how customers collect, review, analyze and manage data in legally sanctioned investigations.

To learn more visit us at www.cellebrite.com and www.cellebrite.com/en/investors.

Cellebrite