



© Lucia | stock.adobe.com

## Guarding and Utilizing Mobile Phone Data:

### A Guide for White Collar Practitioners

Preserving, protecting, and utilizing data from mobile phones is frequently at the forefront of white collar investigations. The digital data contained on mobile phones are relevant to a wide range of investigations conducted by the Department of Justice, state and local law enforcement, and other regulatory agencies. In these scenarios, there are various considerations that white collar practitioners must weigh in determining how to obtain the data they need or how to potentially limit the government's access to certain digital data. For instance, when and how can the government compel a client to provide the passcode to gain access to her or his mobile device? What is the significance of whether the mobile phone used by a corporate executive is owned by her or the company? What steps should a company take to identify, preserve, gather, and review potentially relevant data on mobile phones owned by its employees? What are some of the key differences between representing a company and representing an individual in the context of mobile phone data collection and preservation?

This article provides a practical guide to white collar practitioners regarding how to obtain, protect, preserve, and review data on mobile phones.

#### I. Protecting a Client's Passcode to Mobile Phones

When can the government compel a client — generally a suspect in a criminal investigation — to unlock her personal cellphone device? This question often arises when law enforcement is executing a warrant that allows for the search and seizure of electronic devices. But when the agent attempts to search the seized cellphone, it is locked. Unlike laptops and other personal computers for which the government has technology that allows them to gain access to the data despite password protection, the government's ability to access data on mobile phones is far more limited. What now?

The answer lies at the intersection of protections provided by the Fourth and Fifth Amendments. The first consideration is whether the search and seizure comply with principles of the Fourth Amendment's guarantee of protection of personal privacy against unwarranted intrusion by the government. The second consideration is whether compelling the production of a password complies with the Fifth Amendment's guarantee against self-incrimination. To complicate matters further, these considerations are different depending on the jurisdiction because the development of technology is outpacing the law.

A proper analysis of this problem begins with the 2014 Supreme Court decision recognizing the central-

---

BY INGRID S. MARTIN, MICHAEL R. DISTEFANO,  
AND LORRAINE D. BELOSTOCK

ity of cellphones and digital devices in modern life, and the resulting need to ensure that constitutional safeguards against arbitrary access to personal information by government officials are maintained as technology evolves. In *Riley v. California*, the Supreme Court held that when the government seeks to search the digital data on a cellphone, the Fourth Amendment generally requires a search warrant.<sup>1</sup> “Modern cellphones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans the privacies of life.”<sup>2</sup>

The constitutional analysis for compelling an individual to unlock a mobile phone has become more complicated and nuanced as technology has advanced. There are significant legal differences between compelling an individual to produce a numerical passcode as opposed to producing a fingerprint or face scan to unlock a mobile phone for law enforcement. When providing a passcode, law enforcement compels an individual to provide information that likely only she or he possesses. In contrast, providing biometric information arguably involves a lesser degree of disclosure of information or cooperation with law enforcement. It has long been acceptable, for example, for law enforcement to compel an individual to provide a fingerprint.

In May 2021, the U.S. Supreme Court declined to hear a case on appeal from the Supreme Court of New Jersey that presented the issue whether the Self-Incrimination Clause of the Fifth Amendment protects an individual from being compelled to recall and truthfully disclose a memorized passcode, where communicating the passcode may lead to the discovery of incriminating evidence to be used against him in a criminal prosecution.<sup>3</sup> The Supreme Court of New Jersey, in a 4-3 decision, held that the Fifth Amendment privilege against self-incrimination does not shield individuals from being compelled to communicate their passcodes.<sup>4</sup> In reaching its conclusion, the court reasoned that the passcodes were of “minimal testimonial value,” and that they could therefore be compelled because their existence, possession, and authentication were “foregone conclusions.”<sup>5</sup> The highest state court in Massachusetts also held that the government can compel a defendant to unlock an electronic device provided that it meets two prerequi-

sites: (1) that it establish the defendant knows the passcode to decrypt a particular electronic device before his or her knowledge of the password can be deemed a foregone conclusion (i.e., the government can independently prove that this is a device to which the defendant has access); and (2) that it prove beyond a reasonable doubt that the defendant’s knowledge of the passcode is a foregone conclusion.<sup>6</sup> These decisions stand in contrast to others, like *United States v. Sanchez*,<sup>7</sup> which found that the government violated a parolee’s Fifth Amendment right when a parole officer demanded that the parolee provide the passcodes for cellphones seized from the seat of a luxury vehicle that parolee was driving shortly after his release from prison.

The reasoning and legal landscape appears to shift somewhat when the government asks a person to provide her fingerprint to unlock the phone seized pursuant to a valid warrant. The Northern District of Illinois held that compelling a suspect to use his fingerprints and thumbs, which the government would select, would not be testimonial, and therefore would not violate a suspect’s Fifth Amendment privilege against self-incrimination.<sup>8</sup> In reaching its decision, the court noted, “the application of a finger to the home button on an iPhone ‘can be done while the individual sleeps or is unconscious,’ and thus does not require any revelation of information stored in a person’s mind.”<sup>9</sup> In contrast, a district court in Nevada held that law enforcement forcibly unlocking a defendant’s phone with his face was testimonial in nature and therefore violated the defendant’s Fifth Amendment rights.<sup>10</sup> In reaching its decision, the court noted two fundamental differences between using a biometric feature to unlock a device and submitting to fingerprinting or a DNA swab:

First, a biometric feature is functionally the same as a passcode, and because telling a law enforcement officer your passcode would be testimonial, so too must the compelled use of your biometric feature to unlock a device. Second, unlocking a phone with your face equates to testimony that you have unlocked the phone before, and thus you have some level of control over the phone.<sup>11</sup>

Other courts, however, have held that the government may use an individual’s biometrics to unlock a device. A judge in the District Court for the District of Columbia set out the following protocol:

When attempting to unlock a telephone, computer or other electronic device during the execution of a search warrant that authorizes a search of the device, the government may compel the use of an individual’s biometric features, if (1) the procedure is carried out with dispatch and in the immediate vicinity of the premises to be searched, and if, at time of the compulsion, the government has (2) reasonable suspicion that the suspect has committed a criminal act that is the subject matter of the warrant, and (3) reasonable suspicion that the individual’s biometric features will unlock the device, that is, for example, because there is a reasonable suspicion to believe that the individual is a user of the device.<sup>12</sup>

Certainly, any circumstance in which a client has been compelled to provide any sort of assistance to the government to unlock her or his electronic device is susceptible to suppression. Until the U.S. Supreme Court provides clear guidance and rules regarding the manner and means by which a person can be compelled to provide a passcode to a mobile phone, it is imperative to utilize the various cases and rationales discussed above to protect a client’s constitutional rights concerning her or his mobile phone. Accordingly, when representing an individual whose mobile device has come into the possession of the government, it is important to consider whether to comply with any governmental request to help the government access its contents. There may be a sound legal basis to refuse to cooperate.

## II. Guarding and Preserving Mobile Phone Data by Employers

Looking at the problem of cellphone data from the perspective of a corporation, the calculus is often very different. Corporations do not have a Fifth Amendment right to refuse to supply information to the government, and they often

seek to portray themselves as cooperative and forthcoming with investigators. In this context, recent Department of Justice (DOJ) guidance relating to mobile phone data is important. In September 2022, the Department of Justice issued a memorandum on Further Revisions to Corporate Criminal Enforcement Policies. The memorandum makes clear that when prosecutors evaluate how cooperative a corporation is being with a DOJ investigation, they should consider whether a corporation has instituted policies to ensure that it will be able to collect and provide to the government all non-privileged responsive documents relevant to an investigation, including work-related communications (e.g., texts, e-messages, or chats) and data contained on phones, tablets, or other devices that are used by its employees for business purposes. Within weeks of the DOJ issuing its memorandum on corporate criminal enforcement policies, the U.S. Securities and Exchange Commission fined several substantial banks and brokerages a collective \$1.8 billion over employees' use of private texting applications to communicate about work and for not preserving all of the messages.<sup>13</sup>

The message is clear: the government expects corporations to have policies to capture all relevant data and to put these policies into action. While the message is clear, putting it into practice is not easy. Bring your own device (BYOD) has proven to be a major obstacle to companies and banks trying to obtain and preserve all communications between employees. There are significant problems with employees using their own mobile phones for work: (1) personal emails are often not archived or accessible to employers; (2) private messaging applications such as WhatsApp are encrypted and inaccessible to employers and may even be set to autodelete within hours of sending; and (3) there are a host of ways employees can communicate via personal mobile phones without any preservation of the communications. The list of problems is extensive and troublesome.

At the outset of an investigation, the attorney representing the corporation should determine whether any of the employees who may have relevant electronic communications may have used their personal devices for those communications. Counsel should carefully review any corporate policies and notifications regarding the expectation of privacy — or lack thereof — concerning an employee's use of cor-

porate servers and devices. Policies, notifications, and employee handbooks clearly setting out that an employee's workspace can be accessed by the employer and that the employee has no expectation of privacy in using her employer's devices and networks will certainly undercut an employee's assertion that she had an expectation of privacy with respect to her employer's devices and network.<sup>14</sup>

In the civil context, courts have held that a company does not possess or control the text messages from the personal phones of its employees and may not be compelled to disclose text messages from employees' personal phones.<sup>15</sup> However, it is not clear whether that position will hold, as is already suggested by the DOJ guidance on cooperation. The Eastern District of Michigan aptly observed:

The nation's workplaces are ever evolving. The ability to transact business remotely, through handheld devices and home computers, has meant that the line between personal and work domains has been blurred. The current pandemic crisis has only accentuated this phenomenon.<sup>16</sup>

The issue before that court was whether information on an employee's personal device may be compelled by way of a document request directed to the employer without any further indicia of control over the device by the employer.<sup>17</sup> In analyzing the degree of control that the employer had over its employees' mobile phones, the court noted that control is "context specific."<sup>18</sup> The court expanded on this observation by noting that employers may contract for the right to access the employees' personal devices, and employees and employers may agree to use software that segregates employer data from the rest of the device.<sup>19</sup> Ultimately, the court in that case held that the company was not required to produce the employee's mobile phone data, but the careful analysis that led to the outcome suggests different facts could lead to a different result.

Generally, when employees communicate or store documents on devices that are issued to them by their employers, they do not have the ability to prevent their employers from accessing the data on those devices. Stated differently, employees do not

maintain a reasonable expectation of privacy in the information stored on their work computers when the employee is notified that the employer has retained the right to access or inspect the information stored there.<sup>20</sup> Notifications such as banners and policies generally eliminate a reasonable expectation of privacy in the contents stored in an employer's network account.<sup>21</sup> However, some courts have concluded that employee privacy rights are often curtailed but not necessarily eradicated in the workplace.<sup>22</sup> When using a company-provided device, employees can maintain some expectation of privacy if, for example, the employer permits personal use on the devices or if the digital data, such as text messages or emails, is labeled personal or confidential.<sup>23</sup>

A similar analysis applies to public employees and government-provided devices. *United States v. Linder* is an illustrative case examining the lack of a public employee's expectation of privacy in a government device.<sup>24</sup> There, the defendant, a Deputy United States Marshal for the Northern District of Illinois, was indicted for violating the civil rights of two individuals by using excessive force on them. The Office of the Inspector General of the Department of Justice investigated the allegations. As part of the investigation, the defendant was ordered to produce his government-issued Blackberry. A search of the Blackberry yielded incriminating evidence that the defendant sought to suppress. In support of his suppression motion, the defendant argued that he had a subjective expectation of privacy in the Blackberry because he kept personal videos and pictures of his friends and family on the device and that when he was ordered to give it to investigators, he expressed a desire to retain the personal data on it. The court soundly rejected his argument, noting that there was no evidence that the defendant did not believe the warnings and policies that he accepted informing him that he did not have a reasonable expectation of privacy in accessing and using the Blackberry and the government's computer system. The court further noted that any privacy interest that the defendant may have subjectively believed that he had in his Blackberry and files stored on the government server is not a legitimate privacy interest that society is prepared to recognize as reasonable.

### III. Possible Criminal Consequences for Failing to Preserve or Destroying Electronic Evidence

Aside from collecting data that is responsive to a government investigation from employee devices, counsel for a company also must ensure that data relating to the investigation is preserved. In addition to civil fines and sanctions, a corporation and its employees may be criminally charged with obstruction of justice if documents, emails, or other forms of evidence contained on mobile phones are destroyed, or if there is an attempt or agreement among employees to do so. Corporations can be charged based on a corporate criminal responsibility theory for destruction of corporate data.

While a subpoena or civil investigative demand makes clear when the legal obligation to produce information from mobile phones begins, the timing of when the legal obligation to preserve documents begins is less clear. The principal federal obstruction of justice statute is 18 U.S.C. § 1519, enacted in 2002 as part of the Sarbanes-Oxley Act, which provides, in pertinent part:

Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the *intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both.*

Section 1519 requires proof of an intent to impede, obstruct, or influence the investigation or proper administration of a matter within the jurisdiction of a federal agency or department “or in relation to or *in contemplation*” of such a matter. If there is not a federal investigation at the time an employee destroyed a document, the question is whether the employee committed an offense if he did destroy documents but did not know of or intend to affect a federal matter. The question posed is what intent, knowledge, or belief with respect to a potential future investigation or proceeding must be proven in order to show that it was “in contem-

plation” at the time any document destruction was committed or planned.

In 2002, Congress enacted § 1519 as part of the Sarbanes-Oxley Act, with the intent, according to the Senate report,

not to include any technical requirement, which some courts have read into other obstruction of justice statutes, to tie the obstructive conduct to a pending or imminent proceeding or matter. It is also sufficient that the act is done “in contemplation or in relation to a matter or investigation.”<sup>25</sup>

The Supreme Court, however, has continued to construe obstruction of justice statutes more narrowly than their literal language might permit. In *Yates v. United States*,<sup>26</sup> the Supreme Court considered whether the disposal of an undersized fish to avoid a federal fishing rules inspection could constitute a violation of § 1519, on the ground that a fish is a “tangible object.” Conceding that a fish meets the dictionary definition of a tangible object, the Court limited the term to an object “used to record or preserve information.”<sup>27</sup> The Court made clear that it was moved to this interpretation by the extraordinary breadth of the statute, noting that the principle of lenity in criminal cases was particularly relevant:

where the Government urges a reading of § 1519 that exposes individuals to 20-year prison sentences for tampering with *any* physical object that *might* have evidentiary value in *any* federal investigation into *any* offense, no matter whether the investigation is pending or merely contemplated, or whether the offense subject to investigation is criminal or civil.<sup>28</sup>

In *Marinello v. United States*, the Court took up the issue of the breadth of another federal obstruction statute, 26 U.S.C. § 7217(a), which punishes a person who “corruptly or by force” “endeavors to obstruct or impede the due administration of [the Tax Code].”<sup>29</sup> The Court held that “‘due administration of [the Tax Code]’ does not cover routine administrative procedures that are near-universally applied to all taxpayers, such as the ordinary processing of income tax returns.

## COMPUTER EXPERT ANALYSIS & TESTIMONY

- Successful Suppression of Seized Hard Drives/Electronic Devices
- Forensic Analysis of Electronic Devices by Computer Scientist
- Cell Phone & Cell Tower Analysis for Date/Time/Location Determination
- Device Usage Analysis
- Practice Areas: Criminal Defense, Commercial Litigation, Family Law, ADA, Medical Malpractice, Labor & Employment
- Clients include: Law Firms, Govt. Agencies & Companies

OVER 40 YEARS' EXPERIENCE,  
HUNDREDS OF CASES



Computer  
Consulting Systems

770-883-9115

www.ccsexperts.com

Rather, the clause as a whole refers to specific interference with targeted governmental tax-related proceedings, such as a particular investigation or audit.” The Court once again imposed “a ‘nexus’ between the defendant’s conduct and a particular administrative proceeding, such as an investigation, an audit, or other targeted administrative action.” Despite the absence of express support in the statute, it required “a relationship in time, causation, or logic with the [administrative] proceeding,”<sup>30</sup> and proof that the proceeding “at the least, was then reasonably foreseeable by the defendant.”<sup>31</sup>

In summary, if employees do destroy documents that the government later seeks in connection with an investigation, both the employees and the company are potentially exposed to prosecution. However, the Supreme Court has consistently been concerned with the breadth of obstruction statutes and the need to limit and specify their coverage. If the government were required to prove “nexus,” including knowledge that a federal investigation was likely, or knowledge that the destruction would probably affect the investigation adversely, the

government would have a much weaker hand — again depending, of course, on the states of knowledge and states of mind of the employees.

#### IV. Identifying and Obtaining Relevant Electronically Stored Information

As this legal landscape makes clear, it is critical to identify, obtain, and preserve relevant electronically stored data from the very beginning of a white collar investigation. Electronic evidence may be found on items beyond mobile devices. The initial checklist must be conformed to the unique facts and circumstances of the investigation, but a number of topics should be considered:

1. **Become familiar with the client's communications and data systems.** Communications and data systems are anywhere the client stores data. Some examples of data systems are file shares, in-house and external mail servers, the cloud, Google Drive, and Dropbox. Some corporate clients may have a large network of communications systems used by employees in multiple offices. It is essential to become

familiar with the client's various platforms such as Slack, Teams, and others. It is imperative to cast as wide a net as possible to ensure that all relevant sources of data are identified and captured.

2. **Identify the best person at the company to speak with about data collection.** While it seems logical to start the data collection by speaking with the company's IT director, bear a number of things in mind before doing so. First, make sure the IT director or no one else in the IT department is suspected of participating in any misconduct in connection with the investigation. Though it seems obvious, attorneys can shoot themselves in the foot by not taking this initial step in the data collection process. Second, identify someone in the IT Department who has full knowledge of the company's data systems and can explain it in clear terms. Ideally, the point person in the IT Department will be honest and straightforward. It may, however, be necessary to hire an expert who can serve as something akin to a translator between the IT Department and the legal team to help the legal team ask the right questions and understand the answers received. Third, assure the point person that though the data systems are likely not perfect, they must be comfortable and confident to disclose everything about the systems — good, bad, and ugly.

If a white collar attorney is representing an individual, the client may or may not be fully aware of the universe of electronic data that is connected to her mobile phone. Ask the client to walk through “a day on her device.” What websites and accounts does the client access on her mobile phone? Where are the primary accounts and digital information for the person?


3. **Speak to the client about identifying all relevant data.** Define the scope of relevant information. Be specific and tailor the list of relevant information to the investigation. For instance, an investigation into a corporate executive will likely require reviewing the executive's email, calendar invites, telephone logs, internet usage, and other data.

Define the sources of where the relevant information may be found. Sources may include hard copies, computer hard drives, removable data (CDs, DVDs, thumb drives), personal electronic devices (smartphones, iPads, wearables), Google location history, photos, home devices (Alexa, Google Home, and Ring), servers, and any other locations where hard copy or electronic data is stored by individuals who may have relevant information. Become familiar with the company's document retention policies; speak to the IT Department about where and how the company archives older data. Aside from knowing what devices to collect data from, it is important to be aware of where geographically the data is stored because it could have an impact on how the data is collected. Jurisdictions have different privacy rules — both within and outside the United States — so it is important to acknowledge and abide by them.

4. **Identify and preserve relevant messaging applications used by employees.** People use a wide range of messaging applications on mobile phones. A few examples include WhatsApp, WeChat, Signal, Wickr Me, and Dust. End-to-end encryption is a common feature of most private messaging applications, which means only the sender and recipient can see the message content. Wickr Me permits users to set timers for disappearing messages. Signal's safe chat application encrypts messages, voice calls, group messages, and video calls. Given the secretive nature of these messaging applications, preserving these messages is extremely difficult, if not impossible. Nonetheless, it is critical to inquire with employees regarding their use of the applications and what, if anything, can be retrieved.
5. **Write a letter to the client about preserving all relevant information, and help the client disseminate the preservation message to all relevant employees.** Instruct the client not to discard any mobile phones, computers, or other electronic devices that may contain information relevant to the investigation. Direct the client to turn off any

**NACDL**  
**Artificial**  
**Intelligence**  
**Task Force**

Change is here. The nation's criminal defense bar is on the forefront of studying artificial intelligence (AI) and its impact on the practice of criminal defense. NACDL will launch an AI “think tank” that will include lawyers, academics, and experts in the field. NACDL's task force will review AI and related emerging technologies to prepare criminal defense lawyers to navigate the legal landscape in the age of AI.



Check [NACDL.org/AI](http://NACDL.org/AI) for updates.

“automatic deletion” feature on electronic devices and stop any discarding of information pursuant to a retention policy cease. The importance of stopping automatic deletion is a point worth underscoring. In February 2023, the DOJ asserted that Google failed to timely suspend a policy allowing the automatic, permanent deletion of employees’ chat logs. The assertion came about in an anti-trust matter pending in the U.S. District Court for the District of Columbia.<sup>32</sup> Make it abundantly clear that substantial negative consequences may flow from the failure to take reasonable steps to preserve relevant data. In a civil investigation, Fed. R. Civ. P. 37(e) carries strict sanctions and penalties, such as dismissal and unfavorable jury instructions regarding the client’s failure to preserve the information.

6. **Determine who will collect the Electronically Stored Information (ESI).** For cost reasons, the client may want to rely on its own IT Department to gather the ESI. Be sure to communicate with the relevant personnel the importance of a thorough and forensically sound collection of information. Ideally, a client will authorize the legal team to engage an outside vendor who will gather the information in a manner that is sound and irreproachable. Cutting corners in data collection will create additional problems beyond those involved in the ongoing investigation. Data must be collected the right way, not the fastest way.
7. **Consider formulating a written ESI protocol.** Some basic elements to include in a written ESI protocol include the scope of the collection, format of production, and handling of privilege information. Set out the locations to be searched and the ESI types. Identify the custodians, date ranges, and search terms. Be specific about the production format; information may be contained in a wide range of forms, including native (original) format, metadata, pdf, and many others. For example, a text message contained in a pdf file will be lacking important metadata contained in the native forms of the text message. It is critical that any documents that may be privileged are identified as such.

## V. Reviewing Electronically Stored Data

Once the scope of relevant information is gathered, it is critical that the review is comprehensive and beyond reproach. The outcome of any investigation is only as strong as the integrity by which it was conducted. Depending on the volume of the information, it may be necessary to select a vendor with an appropriate platform to review the materials. Beyond the basic requirements of a comprehensive and thorough review, defense counsel should bear in mind some important guideposts.

First, be aware of confirmation bias. As an advocate, it is only natural to have a certain “lean” or lens when setting out to review information pertinent to an investigation. Ideally, a review will be conducted by more than one attorney working on behalf of the client. The exchange of ideas and opinions that flow from a collaborative setting helps keep any confirmation bias in check. Additionally, to the extent that experts, such as forensic accountants, are part of the review team, it is critical that they provide a comprehensive review that will not be vulnerable to claims of confirmation bias. Be as comprehensive as possible in setting out the issues and data for expert review.

Second, review the information with a focus on how to best organize it in a way that makes it readily presentable to a client and potentially the government. Identify appropriate categories in which to segregate relevant information that may be used in a presentation. Beyond the traditional categories such as “hot docs,” it is helpful to utilize other descriptors such as “client sensitive” or “helpful” or “harmful.” Certainly, the scope and nature of the categories will vary depending on the nature of the investigation. For organizational purposes, such categories are a helpful way to review and ultimately analyze data.

Third, a review of mobile phones and the associated metadata is best conducted by a forensic expert. While searches of mobile phones can yield a treasure trove of information, if the data is not interpreted correctly, it is worthless, and even worse, can be harmful to the client. For instance, the web history on a corporate executive’s mobile phone may indicate that she or he searched Google for certain information. If the timing of the Google search is not interpreted correctly, the search itself may mean a lot less. To give context, if the executive claims to have had no knowledge of certain issues prior to the beginning of an investigation,

a Google search history on the executive’s mobile phone for terms related to those issues prior to the beginning of the investigation would certainly be relevant. Again, an expert who can definitively interpret the timing of when the Google search occurred is critical to making sure the data is properly interpreted.

Fourth, review electronic data to ensure authenticity. In this digital age, the expectation is that a person’s version of an event will be corroborated by some form of electronic data — a photograph, video, text message, email, or some other digital footprint. While it is often the case that there will be some degree of digital data to corroborate an account, practitioners must be skeptical of purported digital data that is “too good to be true.” The so-called “smoking gun” email or text message may not be authentic but instead “spoofed” by a bad actor. A spoofed email or text message will often appear genuine at first glance. For example, bad actors can utilize various technologies to create a text message or photograph that appears to be genuine. It is critical to capture the native data behind an email, text message, photograph, or any similar type of electronic communication. If the individual who claims to have received a so-called “hot” or “smoking gun” document will not provide the original source to establish the authenticity of the document, that is a red flag.

## VI. Matching the Government’s Tools to Capture Electronic Data

The government has many tools to gather electronic data that are not available to defense attorneys. A prosecutor can file search warrants for a wide variety of information. Some commonly used search warrants for location information include geofence warrants and cellphone tower search warrants. With geofence warrants, the government can obtain Google location history for a certain mobile device at certain dates and times. Similarly, a cellphone tower search warrant will reveal the location of the cell towers near where a particular mobile device traveled during certain dates and times.

Of course, the government may not disclose certain information, such as location data, to defense counsel for a variety of reasons. Nonetheless, it is critical to leverage all the electronically stored data available to get the necessary information. Aside from text messaging and information posted through social media applications, mobile phones store a wide variety of information as

part of the default settings. Defense attorneys should carefully review the Privacy and Terms of Use Agreement associated with their client’s mobile phone. These agreements often set out what data is stored and for how long. The volume and nature of stored information on mobile phones are often surprising to practitioners and clients alike. If data from a mobile phone is not helpful or available, practitioners should consider other ways to ascertain information based on the large digital footprint that most people create daily by using other electronic devices.

**Conclusion**

For better or worse, digital data is an integral part of white collar investigations. It is essential for white collar practitioners to embrace and fully explore the universe of electronically stored information. In order to do so, it is critical to take methodical steps all along the process. Depending on the facts and circumstances of a particular investigation, it is important to know all the ways information on mobile phones can be safeguarded from government searches. In some circumstances, a practitioner must identify, obtain, review, and effectively use mobile phone data on behalf of the client. Whether guarding or utilizing mobile phone data, practitioners could benefit by reviewing the steps outlined in this article as a blueprint for navigating the ever-evolving landscape of mobile phone data on both the technological and legal fronts.

© 2023, National Association of Criminal Defense Lawyers. All rights reserved.

**Notes**

1. See *Riley v. California*, 573 U.S. 373 (2014).
2. *Id.* at 403 (internal citations omitted).
3. *Andrews v. New Jersey*, 243 A.3d 1254 (N.J. 2020), cert. denied, 141 S. Ct. 2623 (U.S. May 17, 2021) (No. 20-937).
4. See *State v. Andrews*, 243 N.J. 447, 234 A.3d 1254 (2020).
5. *Id.* at 480.
6. *Commonwealth v. Jones*, 481 Mass. 540 (2019).
7. *United States v. Sanchez*, 334 F. Supp. 3d 1284, 1295 (N.D. Ga. 2018).
8. *Matter of a Search Warrant Application for Cellular Telephone in United States v. Anthony Barrera*, 415 F. Supp. 832 (2019).
9. *Id.* at 839 citing *Matter of White Google Pixel 3 XL Cellphone in a Black Incipio Case*, 398 F. Supp. 3d 785, 794 (D. Idaho 2019).
10. *United States v. Wright*, 431 F. Supp. 1175, 1188 (D. Nev. 2020).
11. *Id.* at 1187.
12. *Matter of Search of [Redacted] Washington, D.C.*, 317 F. Supp. 3d 523, 532-33 (D.D.C. 2018).
13. <https://www.computerworld.com/article/3675289/16-wall-street-firms-fined-18b-for-using-private-text-apps-lying-about-it.html>.
14. See, e.g., *United States v. Angevine*, 281 F.3d 1130, 1134-1135 (10th Cir. 2002) (banner and computer policy eliminates a state university professor’s reasonable expectation of privacy in the contents of computer).

15. *Lalumiere v. Willow Springs Care, Inc.*, No. 1:16-cv-3133, 2017 WL 6943148, at \*2 (E.D. Wash. Sept. 18, 2017); and see *Cotton v. Costco Wholesale Corp.*, No. 12-2731, 2013 WL 381974, at \*6 (D. Kan. July 24, 2013).
16. *Halabu Holdings, LLC v. Old National Bancorp*, 2020 WL No. 20-10427, 2020 WL 12676263, at \*1 (E.D. Mich. June 9, 2020).
17. *Id.* at \*2.
18. *Id.*
19. *Id.*
20. See *United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000).
21. See, e.g., *United States v. Hamilton*, 778 F. Supp. 2d 651 (E.D. Va. 2011).
22. *Pierre v. Griffin*, No. 20-CV-1173-PB, 2021 WL 4477764, at \*5 (D.N.H. Sept. 30, 2021).
23. See *Mintz v. Mark Bartelstein & Assocs.*, 885 F. Supp. 2d 987, 990, 997 (C.D. Cal. 2012) (finding that an employee maintained a “limited expectation of privacy” in a device’s text messages, even where the employer owned and paid for the device, because the employer permitted personal calls on the device).
24. *United States v. Ramirez-Padilla*, No. 12 CR 22-1, 2012 WL 3264924, at \*2 (N.D. Ill. Aug. 9, 2012).
25. S. Rep. No. 107-146, at 14-15 (2002).
26. 574 U.S. 528 (2015).
27. *Id.* at 532.
28. *Id.* at 548 (emphasis in original).
29. *Marinello v. United States*, 200 L. Ed. 2d 356, 138 S. Ct. 1101, 1110 (2018).
30. *Id.* at 1109.
31. *Id.* at 1110.
32. *United States v. Google LLC*, U.S. District Court for the District of Columbia, No. 1:20-cv-03010-APM. ■

**About the Authors**

Ingrid S. Martin, a partner at Todd & Weld



LLP, focuses her practice on the intersection of criminal defense and healthcare law. She defends criminal investigations, civil false claims allegations, licensing and accreditation

challenges, and other governmental healthcare investigations.

**Ingrid S. Martin**

Todd & Weld LLP  
Boston, Massachusetts  
617-720-2626

**EMAIL** imartin@toddweld.com  
**WEBSITE** www.toddweld.com

Michael R. DiStefano, a partner at Todd &



Weld LLP, resolves a wide range of sensitive criminal defense and government investigation matters with a diplomatic and effective approach. In addition, he advises clients in forums outside of court, including college and university disciplinary matters and professional licensing board hearings.

**Michael R. DiStefano**

Todd & Weld LLP  
Boston, Massachusetts  
617-720-2626

**EMAIL** mdistefano@toddweld.com  
**WEBSITE** www.toddweld.com

Lorraine D. Belostock concentrates her



practice on government investigations and criminal defense, including clients at trial and in pre-indictment government investigations.

**Lorraine D. Belostock**

Todd & Weld LLP  
Boston, Massachusetts  
617-720-2626

**EMAIL** lbelostock@toddweld.com  
**WEBSITE** www.toddweld.com