The information in this resource is educational and intended for informational purposes only. It does not constitute legal advice, nor does it substitute for legal advice. Any information provided is not intended to apply to a specific legal entity, individual or case. NCVLI does not warrant, express or implied, any information it provides, nor is it creating an attorney-client relationship with the recipient.

This resource updates a 2015 NCVLI memorandum; updates supported by Grant No. 15JOVW-21-GK-02231-ICJR awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this resource are those of the contributors(s) and do not necessarily reflect the views of the U.S. Department of Justice.

PROTECTING VICTIMS' PRIVACY RIGHTS: SMARTPHONE DATA[1]

It is commonplace for individuals to use cell phones, particularly "smartphones," in nearly every aspect of their life. Indeed, as the Supreme Court has observed, "[c]ell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification." *City of Ontario v. Quon*, 560 U.S. 746, 760 (2010). Commenting on the pervasiveness of smartphones, the Supreme Court observed that they "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude that they were an important feature of human anatomy." *Riley*, 573 U.S. 373, 385 (2014); *see also In re Application of the United States of America for an Order Authorizing the Release of Historical Cell-Cite Information*, 809 F. Supp. 2d 113, 115 (E.D.N.Y. 2011) ("For many Americans, there is no time in the day when they are more than a few feet away from their cell phones."). Whether one is browsing social media sites, storing and sharing pictures, participating in telephone calls or video chats, researching via search engines, texting or emailing friends, family, co-workers, or clients, reading, creating, or editing documents, or managing finances, many tasks, both work-related and personal, are now accomplished using smartphone technology. The result is that smartphones "place vast quantities of personal information literally in the hands of individuals." *Id.* at 2485.

Victims are often concerned about maintaining their privacy when law enforcement or prosecutors request access to smartphones that may contain evidence of a criminal offense or when a subpoena issues from a defendant in a criminal case or an opposing party in a civil case.[2] Notably, some victims who provide their smartphones to law enforcement later confront defense requests to access their private content, claiming that the smartphone may contain information falling within the scope of the prosecution's *Brady* disclosure obligations.[3]

Fortunately, in recognition of the advanced capabilities and storage abilities of smartphones, courts are acknowledging that an individual's privacy rights are strongly implicated with respect to smartphone data. Smartphones compile in one place "many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record." *Riley*, 573 U.S. at 394. Additionally, the sheer volume of information that can be stored and catalogued on a smartphone far surpasses any

amount of data an individual might otherwise carry around in physical form. *See, e.g., id.* (observing that "[a] person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all of his communications with Mr. Jones for the past several months, as would routinely be kept on a phone"). Although not every piece of electronic data stored on a smartphone is sensitive in nature, much of it may be. *See, e.g., id.* at 395 ("Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception."). Smartphones play an often-central role in modern life, to the extent that they "are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans the privacies of life." *Id.* at 403 (quotation and citation omitted); *see also State v. Granville*, 423 S.W.3d 399, 405-412 (Tex. Crim. App. 2014) (citing cases, finding that "a person has a legitimate expectation of privacy in the contents of his cell phone," and observing that because smartphones can "receive, store, and transmit an almost unlimited amount of private information," this means that the "potential for invasion of privacy, identity theft, or at a minimum, public embarrassment is enormous"); *State v. Branigh*, 313 P.3d 732, 738-39 (Idaho Ct. App. 2013) (collecting cases holding that individuals have an expectation of privacy in the content stored on their smartphones).[4]

In light of the context and case law, how can a victim best safeguard their privacy while also sharing information or evidence housed on a smartphone with law enforcement or the prosecution? The following practice tips provide options that practitioners may want to consider when analyzing privacy in the context of smartphone data:

- If one physically turns over an entire smartphone to the prosecution or to law enforcement, either for manual review or for "imaging"/copying of the smartphone's contents, *Brady* requirements may subsequently require or be interpreted to require disclosure of the contents of the entire smartphone to the defense.
- Depending on what information a victim wishes to share with the prosecution or law enforcement, the following methods of conveying the information may facilitate limited disclosure while protecting the victim's privacy with respect to the remainder of the smartphone data:
    - Printing individual pictures or files stored on the smartphone and providing law enforcement or the prosecution with the printed information;
    - Taking a screenshot or photograph of text messages, including metadata, or other materials;
    - Downloading videos or other information to a DVD, thumb drive, or another portable form of electronic data storage;
    - Investigating other sources of obtaining information (*e.g.*, seeking a list of numbers dialed or from which calls were received from the wireless service provider or informing law enforcement if defendant also has a copy of certain materials in their possession); or

- Retaining a private technology company to extract specific information from the smartphone.

[1] A smartphone generally refers to a cell phone (a term short for cellular phone) that has advanced features, including Internet browsing, software applications, and an operating system. Although the two terms technically refer to different devices—with cell phones having only text and/or telephone call capabilities—many people use the terms interchangeably. Because many or most of the cell phones in use are smartphones with greater potential to store and transmit sensitive information about the user, the term smartphone is used inclusively to refer to both devices throughout this resource. Also, as used in this resource, "smartphone data" refers to content contained in a smartphone as well as historical smartphone location data (often referred to as cell-site location information or "CSLI") collected by a wireless carrier. Courts have recognized the privacy interests inherent in both types of smartphone-related information. *See, e.g.*, *Riley v. California*, 573 U.S. 373, 401 (2014) (holding that the "a warrant is generally required before [searching information stored in a smartphone], even when a cell phone is seized incident to arrest"); *Carpenter v. United States*, 585 U.S. 296, 310, 315–16 (2018) (holding "that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI" and that "[t]he Government's acquisition of the cell-site records was a search within the meaning of the Fourth Amendment" subject to the warrant requirement).

[2] This resource provides information regarding and suggestions about how a victim who wishes to share some but not all information on their smartphone with law enforcement or prosecutors can do so while protecting their privacy rights. If formal demands are made for a victim's smartphone or the information contained therein in connection with a criminal case—for example, if defendant serves a subpoena on the victim to compel the victim to provide their smartphone or smartphone data, or a court orders the victim to provide this information to defendant—and the victim does not wish to do so, the victim has legal options, including filing a motion to quash the subpoena or appealing the court order. For more information on victims' rights in legal systems or to request technical assistance, please visit NCVLI's website at www.ncvli.org.

[3] *See, e.g.*, *Brady v. Maryland*, 373 U.S. 83, 87 (1963) (holding that the failure of the prosecution to disclose "evidence favorable to an accused" violates defendants' constitutional due process rights "where the evidence is material either to guilt or to punishment, irrespective of the good faith or bad faith of the prosecution"). It is important to distinguish prosecutors' disclosure obligations under *Brady* from broader requests for access to information by defendants, as it is well established that "[t]here is no general federal constitutional right to discovery in a criminal case, and Brady did not create one . . . ." *Weatherford v. Bursey*, 429 U.S. 545, 559 (1977). Nor do defendants have an established federal constitutional right to pretrial discovery of a crime victim's personal records under the Confrontation Clause. *See Pennsylvania v. Ritchie*, 480 U.S. 39, 52 (1987) (plurality opinion) (emphasizing that the right to confront is a trial right and that the Court has never held that a defendant has a right to pretrial discovery under the Confrontation Clause).

[4] In addition to the privacy rights acknowledged by courts in the context of smartphone content and CSLI specifically—which include Fourth Amendment protections to be free from unreasonable government intrusions into their person, home, papers, and effects, U.S. Const. amend. IV—there is also a federal constitutional right to keep personal information private. *See Whalen v. Roe*, 429 U.S. 589, 598–600 (1977) (recognizing a federal constitutional right to informational privacy that includes the individual interest in avoiding disclosure of personal matters); *see also Eastwood v. Dep't of Corrections,* 846 F.2d 627, 630–31 (10th Cir. 1988) (stating that the right to informational privacy is implicated when an individual is forced to disclose information regarding personal sexual matters). Many states also afford or recognize victims' privacy rights in their victims' rights laws. *See, e.g.*, Cal. Const. art. I, § 28(b)(1) (affording victims the right "[t]o be treated with fairness and respect for [the victim's] privacy and dignity . . . throughout the criminal or juvenile justice process"); Idaho Const. art. I, § 22(1) (affording victims the right "[t]o be treated with fairness, respect, dignity and privacy throughout the criminal justice process"); Ill. Const. art. I, § 8.1(a)(1) (affording victims "[t]he right to be treated with fairness and respect for their dignity and privacy . . . throughout the criminal justice process"); Ky. Const. § 26A (affording victims "the right to fairness and due consideration of the crime victim's safety, dignity, and privacy"); Mich. Const. art. I, § 24(1) (affording victims "[t]he right to be treated with fairness and respect for their dignity and privacy throughout the criminal justice

process"); Nev. Const. art. I, § 8A(1)(a) (affording victims the right "[t]o be treated with fairness and respect for his or her privacy and dignity, and to be free from intimidation, harassment and abuse, throughout the criminal or juvenile justice process"); N.H. Rev. Stat. Ann. § 21-M:8-k(II)(a) (affording victims "[t]he right to be treated with fairness and respect for the victim's safety, dignity, and privacy throughout the criminal justice process"); N.M. Const. art. II, § 24(A)(1) (affording victims of enumerated crimes "the right to be treated with fairness and respect for the victim's dignity and privacy throughout the criminal justice process"); N.M. Stat. Ann. § 31-26-4(A) (affording victims the right to "be treated with fairness and respect for the victim's dignity and privacy throughout the criminal justice process"); N.D. Const. art. I, § 25(1)(f) (affording victims "[t]he right to privacy, which includes the right to refuse an interview, deposition, or other discovery request made by the defendant, the defendant's attorney, or any person acting on behalf of the defendant, and to set reasonable conditions on the conduct of any such interaction to which the victim consents"); Ohio Const. art. I, § 10a(A)(1) (affording victims the right "to be treated with fairness and respect for the victim's safety, dignity and privacy"); Okla. Const. art. II, § 34(A) (affording victims the right "to be treated with fairness and respect for the victim's safety, dignity and privacy"); Okla. Stat. Ann. tit. 21, § 142A-2(A)(2) (affording victims the right to "be treated with fairness and respect for the safety, dignity and privacy of the victim"); S.D. Const. art. VI, § 29(6) (affording victims "[t]he right, upon request, to privacy, which includes the right to refuse an interview, deposition or other discovery request, and to set reasonable conditions on the conduct of any such interaction to which the victim consents"); Tex. Const. art. I, § 30(1) (affording victims "the right to be treated with fairness and with respect for the victim's dignity and privacy throughout the criminal justice process"); Wis. Const. art. I, § 9m(2)(b) (affording victims the right "[t]o privacy"). Some states explicitly provide all individuals—not just crime victims—with a constitutional right to privacy. *See, e.g.*, Cal. Const. art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."); Fla. Const. art. I, § 23 ("Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein…"); Mont. Const. art. II, § 10 ("The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest.").

© 2024 National Crime Victim Law Institute