

Winter 2023

## Grand Jury Information and Government Contractors: Reconciliation Through Privacy Law

Andrew Holzmann

Follow this and additional works at: <https://scholarship.law.marquette.edu/ipilr>



Part of the [Intellectual Property Law Commons](#)

---

### Recommended Citation

Andrew Holzmann, *Grand Jury Information and Government Contractors: Reconciliation Through Privacy Law*, 27 Marq. Intell. Prop. & Innovation L. Rev. 87 (2023).

This Comment is brought to you for free and open access by the Journals at Marquette Law Scholarly Commons. It has been accepted for inclusion in Marquette Intellectual Property & Innovation Law Review by an authorized editor of Marquette Law Scholarly Commons. For more information, please contact [megan.obrien@marquette.edu](mailto:megan.obrien@marquette.edu).

# GRAND JURY INFORMATION AND GOVERNMENT CONTRACTORS: RECONCILIATION THROUGH PRIVACY LAW

ANDREW HOLZMANN

I. THE STRICT CONSTRUCTION OF FEDERAL RULE OF CRIMINAL PROCEDURE	
SIX.....	90
A. Government personnel .....	91
B. Preliminary to or in connection with a proceeding .....	94
C. Particularized need .....	95
II. AMERICAN PRIVACY LAW FRAMEWORKS DEMONSTRATE A MODEL THAT WOULD ALLOW THE USE OF CONTRACTORS IN UNIQUE CRIMINAL PROSECUTIONS WHILE MAINTAINING PRIVACY .....	96
A. HIPAA as a Guide.....	96
B. Other American Law as a Guide .....	98
III. CONCLUSION .....	99

“On January 6th, 2021, a joint session of the United States Congress convened at the United States Capitol to carry out the constitutional duty of certifying the vote count of the Electoral College of the 2020 Presidential Election. This ritual of democracy was disrupted by a rioting mob that breached the Capitol and put a temporary halt to the electoral vote count, assaulting members of law enforcement, destroying property, and encouraging others to join in the mayhem along the way.”<sup>1</sup>

The United States government began investigating this attack at the Capitol shortly after it occurred<sup>2</sup>; the prosecutions of members of the “rioting mob” continue to the time of writing.<sup>3</sup>

---

1. *In re Capitol Breach Grand Jury Investigations Within the District of Columbia*, 339 F.R.D. 1, 3 (D.C. Cir. 2021).

2. *Id.*

3. *Capitol Breach Cases*, U.S. DEP’T OF JUSTICE, <https://www.justice.gov/usao-dc/capitol-breach-cases>, (last visited October 15, 2022).

This comment will analyze this ongoing prosecutorial effort through the lens of Federal Rule of Criminal Procedure Six<sup>4</sup> (FRCrimPro Six), a rule of criminal procedure that prevents matters occurring before a grand jury from being shared with non-government personnel. Federal Rule of Criminal Procedure Six has played an acutely impactful role in the prosecution of the many defendants and potential defendants involved in the January 6th attack:<sup>5</sup> evidence collected for use in subsequent prosecutions has been presented to grand juries<sup>6</sup> as support for felony charges against more than 200 such defendants and used to secure thousands of grand jury subpoenas.<sup>7</sup>

FRCrimPro Six's preclusionary force in this instance is extraordinarily strong: the amount of evidence to be used in the January 6th prosecution may be "the largest in American history."<sup>8</sup> Moreover, much of the evidence contains significant metadata that is difficult to extract without specialized techniques; techniques that include the use of advanced software. Given the government's obligation to share potentially exculpatory electronic evidence with counsel for the numerous defendants in the case pursuant to their discovery requests, the presence of this metadata is more than a headache. Indeed, it serves as a roadblock unless and until the requisite techniques and software are made available.

Thus enter DeLoitte. DeLoitte is a special litigation contractor that assists with both discovery review *and* litigation—the latter of which is crucial to this analysis while the former must be done out of necessity, i.e., the need to enlist outside assistance for the removal of metadata is a requirement that exists

---

4. Fed. R. Crim. Pro. 6(e).

5. *In re Capitol Breach*, 339 F.R.D. at 3. ("To date, more than 500 individuals located across the country have been charged, in over 175 misdemeanors and over 170 indictments, with criminal offenses in this District resulting from their participation in the attack on the Capitol.")

6. *In re Capitol Breach*, 339 F.R.D. at 3. (Presentations before grand juries pursuant to the Jan. 6th attack occurred in the Federal District Court for the District of Columbia.)

7. *Id.* at 3.

8. Per the Gov'ts brief in support of its motion to authorize the disclosure of grand jury materials to DeLoitte, the evidence consists of "more than 14,000 hours" of surveillance footage from the Capitol grounds; "[m]ore than 2,000 hours of body worn camera footage from multiple law enforcement agencies"; "[o]ver 300,000 tips" from members of the public, "including approximately 237,000 digital media tips"; "[o]ver 2,000 digital devices"; "[l]ocation history data" and "[c]ell tower data" for thousands of electronic devices present "inside the Capitol building" on January 6; "[i]nformation" obtained "from the searches of hundreds of accounts maintained with electronic communications service providers and/or remote computing services [sic] providers"; "over one million Parler posts, replies, and related data, collected by" the Federal Bureau of Investigation ("FBI") "from publicly accessible locations on the Internet"; an additional "over one million Parler videos and images (approximately 40 terabytes of data) scraped by an Internet user who voluntarily provided the material to the FBI"; "[s]ubscriber information and two weeks of toll records for hundreds of phone numbers . . . associated with a Google account identified from . . . [a] geofence search warrant"; and "[o]ver 240,000 [FBI] investigative memoranda and attachments."

largely because of the discovery requests received. The government sought to engage DeLoitte as a contractor, and though the terms of that contract did not enter into the record, the government states that DeLoitte was enlisted to help “process[], review, and produc[e] . . . the voluminous materials collected in the course of the government’s investigation and to “populat[e]” [a] database.”<sup>9</sup>

The significance of FRCrimPro Six in light of the volume and format then, is that much of the electronic evidence has been shared with grand juries in the D.C. Circuit in support of felony charges against more than 200 defendants.<sup>10</sup> Moreover, more than “6,000 grand jury subpoenas have been issued for the production of significant portions of the information collected by the government,” a number likely to grow as the investigation continues.<sup>11</sup> There are two layers of disclosure of the digital mountains of collected evidence: the primary—and focus of this comment—is the evidence to be used to prosecute defendants, but the same evidence will also have to be made available to the numerous criminal defendants on a case-by-case basis to comply with individual discovery requests. The discovery request piece is ultimately immaterial because this analysis will focus on the possibility of the initial disclosure, which, if found impermissible, would preclude Rule 6(e) from any attendant secrecy concerns from being triggered at the discovery stage.

Now, with such a large dataset forming the bulk of the admissible evidence for both prosecution and defense, the government sought the services of DeLoitte LLP and retained them to “assist in document processing, review, and production” of evidence.<sup>12</sup> However, because Rule 6(e) serves to prevent any and all “matters” occurring before a grand jury from being shared with non-government personnel, *none* of the information shared with grand juries in pursuit of the aforementioned felony charges may be shared with DeLoitte. Rule 6(e) renders any expertise DeLoitte may be able to offer the prosecution impermissible as it pertains to a massive portion of what is potentially the largest collection of electronic data in American history.

The body of this comment will begin with an exploration of the present strict construction of FRCrimPro Six before arguing, by way of analogy to American Privacy law, that FRCrimPro Six can be read more broadly while remaining true to its purpose.

---

9. *In re Capitol Breach*, 339 F.R.D. at 6.

10. *Id.* at 3.

11. *Id.*

12. *Id.* (quoting Gov’ts Suppl. Mem. at 4).

I. THE STRICT CONSTRUCTION OF FEDERAL RULE OF CRIMINAL PROCEDURE  
SIX

The absolute phrasing expressed above would come to be true. *In re Capitol Breach Grand Jury Investigations Within Dist. of Columbia*, held that Rule 6(e) and its provision allowing disclosure of grand jury matter only to government personnel would apply to the insurrection prosecution.<sup>13</sup> Rule 6(e)(3) is known as the “secrecy rule” in Criminal Procedure. It is a strict rule—very few exceptions exist—and it governs all grand jury proceedings in the federal system. One of the exceptions to the prohibition on disclosure the secrecy rule provides is the allowance of disclosure to “government personnel.”<sup>14</sup> As such, the core issue in the present case is whether DeLoitte LLP and, more precisely, its employees, constitute government personnel such that disclosure would be permitted.

*McKeever v. Barr*, a DC circuit case, limits disclosure in this context, but it appears that other circuits might allow disclosure.<sup>15</sup> The First, Second, and Tenth Circuits have not adopted the same framework for interpreting Rule 6(e) set out by the D.C. Circuit in *McKeever* and therefore are not bound by either the conclusion that the text of Rule 6(e)(3) must be narrowly and literally construed or the determination that Rule 6(e)(3)’s exceptions represent an exhaustive list of the available exceptions to grand jury secrecy. Each of these three circuits’ approach to Rule 6(e) disclosures is best demonstrated by the following cases: *United States v. Pimental*<sup>16</sup>; *In re Biaggi*<sup>17</sup>; *In re Special Grand Jury 89-2*<sup>18</sup>, (acknowledging that district courts may have inherent authority to disclose grand jury materials beyond the non-exhaustive exceptions enumerated in Rule 6(e) but declining to define the scope of that authority).

Of those foregoing authorities, *In re Special Grand Jury* offers the most realistic—and indeed *realist* view—of a court’s role in the construction of “government personnel.” In that case, the Tenth Circuit determined that it, as a federal court, possessed an inherent authority to determine if and when the disclosure of matters occurring before a grand jury were appropriate. As such, this inherent power view could be construed to mean that federal courts have the power to interpret Rule 6(e) as they fit or, more drastically, to fully eschew the rule’s restrictions and instead order disclosure at their discretion. While this

---

13. *In re Capitol Breach*, 339 F.R.D. at 8.

14. Fed. R. Crim. Pro. 6(e)(3)(A)(ii).

15. 920 F.3d 842, 850 (D.C. Cir. 2019).

16. 380 F.d 575, 596-97 (1st Cir. 2004).

17. 478 F.2d 489, 493 (2d Cir. 1973).

18. 450 F.3d 1159, 1178 (10th Cir. 2006).

(extremely) broad view has received some support<sup>19</sup>, the interpretive rule has received considerable endorsement. The authorities cited above all recognize it as a viable interpretation of the judiciary’s role in interpreting the federal rules of criminal procedure, and the Supreme Court has even suggested the disclosure of grand jury materials is “committed to the discretion of the trial judge.”<sup>20</sup> Indeed, it has even been plainly stated that the Secrecy rule is little more than a declaratory statement that disclosure is committed to the trial judge’s discretion<sup>21</sup>

So why, then, does the court assert that it is completely hamstrung by the rules in the present case? Why does the court insist that it is categorically lacking in discretionary capacity when the very rule it asserts it is hamstrung by can be read as a positive affirmation of the very discretionary power it claims to lack? Moreover, why do the particularly high stakes of the trial(s) related to the January 6th insurrection militate solely *against* disclosure? Were the court to have used its discretion to determine that disclosure would have been inappropriate, the result would be conscionable. It is the court’s complete dereliction of its own ability to use judicial discretion that makes this conclusion somewhat—well, conclusory.

#### A. Government personnel

First, “government personnel” was held, authoritatively, to mean exactly that: only employees of public governmental entities could meet the definition.<sup>22</sup> It is important to articulate at this point in the Comment the logic motivating Rule 6(e): secrecy. That is, Rule 6(e), which governs all grand jury proceedings, contains an explicit and overriding protection of the secrecy of grand jury proceedings. It follows, then, that limiting disclosures exclusively to government personnel is the *only* way to maintain this secrecy; at least, that is what the case law tends to indicate<sup>23</sup> The case law precedent to *In re Capitol Breach* militated strongly against government contractors falling within this definition, and the case itself ruled that no matter how robust DeLoitte’s commitment to confidentiality was—and it fully appears that confidentiality

---

19. See, e.g., *Id.*

20. *Pittsburgh Plate Glass Co. v. United States*, 360 U.S. 395, 399 (1959).

21. *Id.* (“Rule 6(e) is but declaratory of [the proposition that disclosure is committed to the trial judge’s discretion]”).

22. *In re Capitol Breach Grand Jury investigations Within Dis. Of Columbia*, 339 F.R.D. 1, 22(D.D.C. 2021). See generally, *McKeever v. Barr*, 920 F.3d 842 (D.C. Cir. 2019).

23. *Markarian v. Alloian*, N.D.Ill.1993, 836 F.Supp. 529; *McKeever v. Barr*, 920 F.3d 842, 844, (D.C. Cir. 2019); See generally *Dennis v. U.S.*, 384 U.S. 855 (1966).

was top of mind for DeLoitte as they entered into this contract with the government<sup>24</sup>—well, rules are rules, and this rule is absolute.<sup>25</sup>

The court's concerns in deciding that DeLoitte LLP and its employees did not fit the definition of government personnel was largely because DeLoitte would not have been subject to extensive government control. Indeed, though DeLoitte had instituted, in partnership with the government, a vigorous data protection policy that would be in place throughout the duration of their government contract<sup>26</sup>, DeLoitte would have retained control over the disclosed material. Per the U.S. Government, the contract with DeLoitte involved data encryption and data residing in the DeLoitte hosting environment that complies with federal security parameters. Further, DeLoitte employees involved in the insurrection prosecution were bound by a strict confidentiality agreement and were prohibited from taking secure materials out of the DeLoitte facility (both physical and virtual). Finally, DeLoitte would have been required to return all materials to the government upon the completion of the contract. While a disclosure to a third party, or really any use outside of the scope of DeLoitte's contract would have almost certainly been a breach of contract, the very possibility of unauthorized access was found incompatible with the secrecy rule.

Indeed, it appears that the main, if not sole, requirement for a party to be considered government personnel is government control over the party. For example, in *Pimental*, employees of the Massachusetts Fraud Bureau, an entity that evaluates allegations of fraudulent insurance transactions, were found to be government personnel.<sup>27</sup> On its surface, at least, this make-up appears analogous to the present situation, in which DeLoitte and its employees are being proffered to assist the government in an investigation. However, in *Pimental*, the instrument governing the relationship between government and entity was not a contract but rather a statute.<sup>28</sup> And not just any statute: the statute allowed for Massachusetts to determine the “purpose, organizational

---

24. *In re Capitol Breach*, 339 F.R.D. at 6. Per the government, their “contract with Deloitte contains all applicable personnel and information security requirements required by the Federal Acquisition Regulation[,]” 48 C.F.R. § 1 *et seq.* Gov't's Mot. at 5; *see also* Gov't's Suppl. Mem. Supp. Mot. Authorize Disclosure of Grand Jury Materials (“Gov't's Suppl. Mem.”) at 4, ECF No. 2. As to information security, the government assures the Court that the contract includes “stringent information security protocols that entail the use of data encryption, a dual-container configuration, and other measures.”

25. *In re Capitol Breach*, 339 F.R.D. at 7. “Rule 6(e) . . . presumptively prevents the government from disclosing any grand jury matters and related materials . . . in connection with its contract . . . unless one of the exceptions . . . applies.”

26. *Id.* at 6 (citing Government memoranda and motions).

27. *United States v. Pimental*, 380 F.3d 575, 591 (1st. Cir. 2004).

28. *Id.* at 592-93.

scheme, and basis operations” of the Bureau and provided the Massachusetts legislature with “constant oversight.”<sup>29</sup> Accordingly, despite the Massachusetts Fraud Bureau’s status as an independent contractor, the court still found disclosure appropriate because the Bureau’s statutory constraints made it a “quasi-governmental entity.”<sup>30</sup> A finding of such status provided a “functional showing” that some of the employees of the Bureau were government employees for the purposes of the statute.<sup>31</sup> Naturally, the government sought to offer *Pimental* as authority that their use of DeLoitte, as an independent contractor, could be construed as a government employee by a functional showing. Hamstrung by its own precedent, the court elected to dismiss that position out of hand, stating “A ‘functional showing’ standard of this sort is, of course, foreclosed in this Circuit by *McKeever*’s requirement that district courts ‘hew strictly’ to the text of Rule 6(e)(3)’s exceptions.”<sup>32</sup>

The relationship presented in *United States v. Anderson* is another instance of a federal circuit recognizing that a bona fide non-governmental employee as the statute strictly defines was still permitted to access disclosed materials.<sup>33</sup> Indeed, this individual was a trust law expert retained under contract with the government<sup>34</sup>, a relationship remarkably similar to that of DeLoittes’ employees. Nevertheless, the court here found the authority lacking in persuasive value; yet another demonstration of the D.C. Circuit’s strict commitment to the secrecy rule.

The jurisprudence body of Rule 6(e) analysis (though rather scant) therefore reveals a fairly simple two-step analysis for analyzing the propriety of a disclosure under the rule. First, one must ask if the party to whom disclosure is sought falls under the definition of government personnel. If the party does not fit this definition (and in the D.C. Circuit, any personnel not an employee of the government will almost certainly *not* fit the definition), then Rule 6(e)’s secrecy rule applies. That, however, is not quite the end of the analysis. Indeed, Rule 6(e)’s narrow construction can be ever-so-slightly expanded in cases where the disclosure in question is “preliminarily to” or “in connection with” that proceeding; and, finally, show a “particularized need” for the requested grand jury materials.<sup>35</sup> Naturally, as this issue represents, the United States

---

29. *Id.* at 593.

30. *Id.* at 596.

31. *Id.* at 596.

32. *In re Capitol Breach Grand Jury Investigations Withing the District of Columbia*, 339 F.R.D. 1, 20 (D.C. cir. 2021) (quoting *McKeever v. Barr*, 920 F.3d 842, 846 (D.C. Cir. 2019)).

33. 778 F.2d 602, 605 (10th Cir. 1985).

34. *Id.*

35. *United States v. Sells Eng’g*, 463 U.S. 418, 443 (1983) (“Rule [6(e)(3)(E)(i)] simply authorizes a court to order disclosure ‘preliminarily to or in connection with a judicial proceeding.’ . . .



government was not able to meet either alternative. That is, DeLoitte LLP and its employees were found to be excluded from any and every construction of the term “government personnel,” and the alternative “particularized need” standard for disclosure for use preliminary to or in connection with a judicial proceeding was not found to be met.

Further, Rule 6(e) does allow disclosure of grand jury matter where the rule “provides otherwise.”<sup>36</sup> This “provides otherwise” item is undeniably facially appealing, and was naturally pursued by the government as a theory for propriety of DeLoitte’s assistance. However, despite the encouragingly broad verbiage, the “provides otherwise” exception exists as a functional redundancy in contemporary case law, limiting the so-called exceptions to individuals and actors who would otherwise meet the definition of government personnel. As a practical matter, this interpretation changes the exception from one of practical necessity to a reinforcement mechanism for the already taught rigidity of the “government personnel” disclosure limitation.

#### *B. Preliminary to or in connection with a proceeding*

Turning next to the “preliminary to” or “in connection” with a proceeding rule, a portion of the compelled or ordered disclosure piece of Rule 6(e).<sup>37</sup> As discussed above, trial judges possess a degree of inherent authority, and it is in this space that such authority could be used. Indeed, Section (E)(i) provides that “a court may *authorize* disclosure . . . subject to any . . . conditions that it directs . . . of a grand-jury matter: (i) preliminary to or in connection with a judicial proceeding.”<sup>38</sup> It is here that the court is at its most pedantic, as it asserts that disclosure, even if permitted, could not be granted for the series of like prosecutions. Instead, the Rule constrains the court to *single* judicial proceedings, i.e., one single trial at a time.<sup>39</sup> Accordingly, even if the court found disclosure appropriate (which it does not), it could only find it appropriate for one instance at a time, a holding that renders DeLoitte’s role as litigation database builder and manager for handling the evidence across *all* related cases nearly obsolete.

---

We have consistently construed the Rule, however, to require a strong showing of particularized need for grand jury materials before any disclosure will be permitted.”)

36. Fed. R. Crim. Pro. 6(e)(2)(B).

37. Fed. R. Crim. Pro. 6(e)(3)(E)(i).

38. *Id.*

39. *In re Capitol Breach Grand Jury Investigations Withing the District of Columbia*, 339 F.R.D. 1, 23 (D.C. cir. 2021) .

### C. Particularized need

Of the foregoing, the “particularized need” for disclosure is facially the most compelling. However, rather than an invitation for the trial judge to make a judgment call on the degree of need, this provision instead mandates a balancing test. Only where “(1) the requested materials are ‘needed to avoid a possible injustice in another judicial proceeding; (2) the need for disclosure is greater than the need for continued secrecy; and (3) the request is structured to cover only material so needed.’”<sup>40</sup> So, the trial judge is theoretically given a degree of discretion to determine need, but is strictly construed by the balancing test in element (2), that the “need for disclosure [be] greater than the need for continued secrecy.”<sup>41</sup> This balancing test is tilted considerably in favor of non-disclosure: because of the premium placed on secrecy, this test has been interpreted to mean that only where disclosure is an effective necessity might it outweigh the potential breach of secrecy that the Rule works judiciously to protect.<sup>42</sup> Indeed, in holding that a particularized need did not exist in the present case, the court stated “the added inconvenience and administrative burden of the government segregating, reviewing, and processing grand jury materials internally, without Deloitte’s assistance, is not enough to support a finding of particularized need, even if these internal methods might be slower or marginally less accurate than the methods employed by Deloitte.”<sup>43</sup> The tolerance for error that Rule 6(e) imports in this instance hardly seems tolerable given the circumstances.

In sum, though a reasonable construction of the government personnel definition would appear to accommodate government contractors in DeLoitte’s position, it was held that DeLoitte could not be defined as such, largely as a function of the government’s lack of control over any disclosure made to them. Further, had disclosure been permitted pursuant to DeLoitte’s status as government personnel, even then it would only be permitted on a trial-by-trial basis, therefore gutting the unique role DeLoitte was contracted to play in the first place. Finally, the “particularized need” standard was not met because, effectively, DeLoitte’s assistance was not absolutely mandatory to the prosecution. Because a present construction of Rule 6(e), at least in the D.C. Circuit, will not accommodate a relationship of the type contemplated in the present case, a reference to HIPAA and its privacy rule will help demonstrate how the goal of Rule 6(e) can still be effectuated even with a disclosure to a government contractor.

---

40. *In re Capitol Breach*, 339 F.R.D. at 24 (quoting *Sells Eng’g*, 463 U.S. at 443).

41. *Id.*

42. *Id.* at 25.

43. *Id.* at 26.

## II. AMERICAN PRIVACY LAW FRAMEWORKS DEMONSTRATE A MODEL THAT WOULD ALLOW THE USE OF CONTRACTORS IN UNIQUE CRIMINAL PROSECUTIONS WHILE MAINTAINING PRIVACY

A marginally less strict reading of Rule 6(e) would allow DeLoitte to assist the government, as the ethos of the rule—namely, secrecy—would be maintained. In turn, should this marginally less strict reading be adopted, it would still leave an interpretive void; the rule and its potential exceptions have always been interpreted as absolutes, so no framework exists for disclosures made to non-government for the simple reason that no such disclosure has been permitted under the current set of rules (at least, not in the D.C. Circuit). Because much of the concern about secrecy being compromised stems from the Government’s lack of control over the disclosure once released, some legal mechanism stronger than a contract may serve to assuage those fears and enable the use of contractors like DeLoitte for similar prosecutorial assistance to that the government requests in this instance. Fortunately, an existing American privacy law framework may serve as a useful guide for this legal mechanism. Moreover, this framework is particularly relevant because it has come to contemplate the large number of digital data entities endemic to the present day.

What is more, the secrecy rule embedded within Rule 6(e) has been interpreted by circuits other than the D.C. Circuit as a use-limiting rule instead of an absolute prohibition on disclosure.<sup>44</sup> In fairness, the uses available under the rule are severely restricted and ultimately at the discretion of the trial judge, but they nonetheless demonstrate that there is *some* play in the joints when it comes to secrecy. In that sense, the “secrecy” rule has some latent “privacy” qualities, particularly if privacy is read as a principle governing the proper *use* of information more than it governs the propriety of *access* to that same information.

### A. HIPAA as a Guide

First, HIPAA, the Healthcare Information Privacy Access Act, provides a structure that entities like DeLoitte could very well seamlessly join under a slightly less strict interpretation of Rule 6(e)’s secrecy provisions. In the main, this structure is that of the so-called “business associate.” HIPAA is a comprehensive privacy rule that governs the disclosures covered entities may make as regards personal health information (“PHI”). Further, the “business associates” of such covered entities are *also* governed by HIPAA. In relevant part, an entity is a business associate when it

---

44. See generally *In re Capitol Breach*, 339 F.R.D.

[p]rovides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation, . . . management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.<sup>45</sup>

Moreover, HIPAA designates privacy requirements that are at least as demanding as those DeLoitte has imposed upon itself.<sup>46</sup>

Under this definition, entities providing a useful, government assisting/covered entity assisting task are subsumed under the relevant privacy law in exactly the same way as the principal entity. Here, the practical effect would be that DeLoitte is subject to the same rules—and the same punishment for violations thereof—as the U.S. Government, and with very little room for nuance. Indeed, while it seems that much of the present concern expressed in the case law comes from the lack of control over the privacy of the grand jury materials once disclosure is made to non-government personnel, HIPAA provides a model demonstrating how control can be maintained when an additional party gets involved.

This fact is evinced by the mission statement of sorts on the CDC page dedicated to the HIPAA privacy rule. The site states “A major goal of the Privacy Rule is to ensure that individuals’ health information is properly protected while allowing the flow of health information needed to provide and promote high-quality health care and to protect the public’s health and well-being.”<sup>47</sup> This principle is extraordinarily conducive to absorption within Rule 6(e)’s secrecy rule, especially in light of the potential for a somewhat more liberal, albeit limited, construction of the rule than it is currently receiving in the D.C. Circuit.

---

45. 45 C.F.R. § 160.103(1)(ii).

46. See 45 C.F.R. § 164.306 Security standards: General rules.

(a) General requirements. Covered entities and business associates must do the following:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.

(4) Ensure compliance with this subpart by its workforce.

47. *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, CENTER FOR DISEASE CONTROL AND PREVENTION, <https://www.cdc.gov/php/publications/topic/hipaa.html> (last updated June 27, 2022).

In practice, DeLoitte and other government contractors in DeLoitte's position as government contractors assisting with prosecution could exist in a role analogous to that of a "business associate" under HIPAA. If the government is considered to be the covered entity in this relationship, then the Privacy Rule of HIPAA would extend to DeLoitte, extending both liability and potential punishments for breaches of privacy and, perhaps most importantly, providing the government with control over the disclosed material outside of the contractual protections inserted already. Should the lack of procedural control governing disclosures be the root cause of the D.C. Circuit's reluctance to permit disclosure in the first place, HIPAA provides a framework by which disclosure can be made pursuant to restrictions governing their use. Moreover, the secrecy of the grand jurors—the ultimate aim of Rule 6(e)—would remain preserved.

### *B. Other American Law as a Guide*

HIPAA is not the only law with privacy conditions that provide a framework applicable to DeLoitte and future government contractors. For example, the Gramm-Leach Bliley Act, which generally prohibits financial institutions from disclosing personal information they hold to third parties, enables those financial institutions to disclose such information for investigations related to public safety.<sup>48</sup> Disclosures are still limited, of course, but the prohibition accommodates such disclosures where there is a particular need.

Other Federal laws require certain *contractual* privacy conditions between controllers of information and third parties with whom they share it. The FTC suggests, for example, that entities contract for security and privacy provisions when contracting with third-party software providers and that those entities monitor their activity regularly to ensure the protection of the entity's information.<sup>49</sup> Moreover, entities are already incentivized to ensure that their disclosure agreements are watertight by the FTC's broad enforcement power under FTC Act.<sup>50</sup>

Further, comprehensive consumer protection laws<sup>51</sup> like the California Consumer Privacy Act (CCPA) also provide a contractual formula. The CCPA

---

48. 15 U.S.C. § 6802 (e)(5).

49. Lesley Fair, *Data Security Settlement with Service Provider Includes Updated Order Provisions*, FEDERAL TRADE COMMISSION (Jun. 12, 2019), <https://www.ftc.gov/business-guidance/blog/2019/06/data-security-settlement-service-provider-includes-updated-order-provisions>.

50. 15 U.S.C. § 45.

51. See Anokhy Desai, *US State Privacy Legislative Tracker*, IAPP, <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/> (last updated Oct. 7, 2022). In the United States, the number of comprehensive state consumer privacy laws continues to grow. In

permits entities to share personal information they control with third parties, so long as those entities have a contract in place with that shared party strictly proscribing the available uses of that information by the third party.<sup>52</sup> While these provisions are enumerated (the statute requires three express qualifications to be met by the contract), the language essentially requires that the sharing party limit the third parties' available uses to those for which it was provided to them.<sup>53</sup> If the CCPA were to govern the intended Government-DeLoitte grand jury information sharing, the government would be permitted to share the evidence that appeared before grand juries but would also have a contractual agreement in place limiting DeLoitte's use of that evidence to the purpose for which they were contracted: assistance with the prosecution. And that is exactly what the government did.

So, as these other laws demonstrate, the *formula* exists for the D.C. Circuit court to recognize a situation in which disclosure is appropriate, perhaps even necessary, while the subjects of such information remain protected. As has been demonstrated, that formula is not currently being applied.

### III. CONCLUSION

The January 6th Capitol Insurrection, the trials for which remain ongoing as of the time of writing, remains an indelible mark upon recent American Political history. The disruptive effect the events of that day had on our understanding of political norms is as-of-yet incalculable. Indeed, it could very well be the case that the insurrection is of *little effect* on the next century of the American Presidency and American politics more generally. An important part of the calculation of the effect the insurrection might have on the future of American politics is the current prosecution of the so-called insurrectionists. This prosecution, the evidence collected for which may be "the largest in American history,"<sup>54</sup> and the effectiveness thereof serves a critical role in the

---

2022, Utah and Connecticut joined Virginia, Colorado, and California as states to have enacted comparable consumer privacy legislation.

52. CAL. CIV. CODE § 1798.140 (2018).

53. § 1798.100.

54. Per the Government's brief in support of its motion to authorize the disclosure of grand jury materials to DeLoitte, the evidence consists of "more than 14,000 hours" of surveillance footage from the Capitol grounds; "[m]ore than 2,000 hours of body worn camera footage from multiple law enforcement agencies"; "[o]ver 300,000 tips" from members of the public, "including approximately 237,000 digital media tips"; "[o]ver 2,000 digital devices"; "[l]ocation history data" and "[c]ell tower data" for thousands of electronic devices present "inside the Capitol building" on January 6; "[i]nformation" obtained "from the searches of hundreds of accounts maintained with electronic communications service providers and/or remote computing services [sic] providers"; "over one million Parler posts, replies, and related data, collected by" the Federal Bureau of Investigation ("FBI") "from publicly accessible locations on the Internet"; an additional "over one million Parler videos and images (approximately 40 terabytes of data) scraped by an Internet user who voluntarily provided the

resolution of the post-insurrection disruption. It is, as many high-stakes criminal trials are, much more than a quiet resolution of isolated facts – it is instead an omnipresent resolution of the shock that many experienced when a “ritual of democracy was interrupted by a rioting mob.”<sup>55</sup>

It is only in light of the immense stakes of the January 6th prosecutions that the strict construction of Rule 6(e) and its attendant secrecy provisions promulgated and adhered to by the D.C. Circuit court appears to lose a large degree of the protectionary function it purports to embody. This is especially true in light of the potential, perhaps even latent, areas in which the Rule could receive a limited liberal construction, particularly in high-stakes cases involving a unique composition and amount of evidence like the present one. Indeed, the precedent from other federal jurisdictions indicates that federal contractors like DeLoitte have met the definition of government personnel such that disclosure to them *is* appropriate in limited circumstances, particularly where their subject-matter expertise would be of great assistance to the prosecution. In line with the prevailing view that a trial judge possesses some degree of inherent authority to allow disclosures—either under Rule 6(e) or even if he or she deems disclosure necessary absent the Rule’s conditions—it seems logical that an event as cataclysmic as the January 6th insurrection might encourage the court to utilize that authority. Moreover, DeLoitte’s contract stipulates a robust degree of data protection that would theoretically require them to maintain a level of secrecy compliant with the logic motivating Rule 6(e)’s existence: the protection of grand juror secrecy.

It is considering all the foregoing that the D.C. Circuit court’s complete abandonment of a discretionary disclosure analysis is altogether frustrating. The events at play are significant; the evidence involved is complex and large; and if a change in the law is needed, examples exist as to how disclosure may proceed in a manner that comports with the secrecy goal of Rule 6(e). Perhaps it is too late for the Rule to change regarding the January 6th prosecution. If it is, may we all hope that the Rule’s rigidity does not serve as a restraint on the reconstruction of our democratic norms.

---

material to the FBI”; “[s]ubscriber information and two weeks of toll records for hundreds of phone numbers . . . associated with a Google account identified from . . . [a] geofence search warrant”; and “[o]ver 240,000 [FBI] investigative memoranda and attachments.”

55. *In re Capitol Breach Grand Jury Investigations Within the District of Columbia*, 339 F.R.D. 1, 3 (D.C. Cir. 2021).