

The Sedona Conference Draft  
Commentary on Application of  
Attorney-Client Privilege and  
Work-Product Protection to  
Documents and Communications  
Generated in the Cybersecurity  
Context, Second Edition  
(October 2021)

---



This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

**The Sedona Conference  
Draft Commentary on Application of Attorney-Client  
Privilege and Work-Product Protection to  
Documents and Communications Generated in  
the Cybersecurity Context, Second Edition  
(October 2021)**

**Drafting Team Members:**

Kate Baxter-Kauf (Drafting Team Co-Leader)

David Cohen (Drafting Team Co-Leader)

Mathea Bulander

Kelly Iverson

Anderson Lunsford

Douglas McNamara

Kelly Ruane Melchiondo

Daniel Robinson

Sara Romine

Caitlin Saladrigas

Ronni Solomon

Jud Welle

Ruth Promislow (Steering Committee Liaison)

Jonathan Wilan (Steering Committee Liaison)

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

## **I. Objective**

- The purpose of this outline is to set forth the Drafting Team’s plan for revising the *Commentary on Application of Attorney-Client Privilege and Work-Product Protection to Documents & Communications Generated on the Cybersecurity Context*.
- Each part of the outline was drafted by distinct sub-groups of the Drafting Team and subject to limited review and revision by the Drafting Team leaders. Due to time constraints, the Drafting Team as a whole has not yet reviewed and commented on, much less approved, either this outline as a whole or any particular portion of the outline. This outline therefore is intended to represent only a “draft of a draft” of the plan for the Commentary, and is being distributed solely for the purpose of facilitating discussion of the pending Commentary at the Working Group 11 Meeting in October 2021.

## **II. Updates to the Case Law and Additional Discussion of Relevant Factors**

- Overall:
  - We propose to update Part C of the Commentary with key new cases that have been issued since the last Commentary.
  - Relatedly, since one of the new *Marriott* cases involves the expert privileges – which garnered little treatment in the original Commentary – we propose to add a discussion of the basic principles of the expert privileges to Part B of the Commentary.
  - Leveraging the new cases, we also propose to revise Part C to expand on the factors courts will consider in deciding the discoverability question.
- Key factors to be added/expanded upon based on the new cases include:
  - In regard to forensic investigators, whether and how the company had a pre-breach relationship with the investigator
  - The content of the engagement agreement with the vendor
  - Whether the company made public statements suggesting a non-legal purpose for the breach investigation.
  - Whether the content of the forensic report suggests a nonlegal purpose (e.g., remediation recommendations).
  - How the company distributed and used the results of the investigation
  - How the company designated the expense of the investigation (legal versus business expense)
  - Whether there was a true “dual track” investigation in which the legally driven investigation was separate from the business oriented investigation.
  - Whether, at the time the investigator was hired, the company had concluded that a breach had occurred – or merely that it may have occurred.
  - Whether the documents in question were actually sent to counsel.
- Key cases to be added to Part C:
  - Attorney/client privilege:
    - In *Guo Wengui v. Clark Hill, PLC*,<sup>1</sup> the court granted the plaintiff’s motion to compel the defendant, his former law firm, to produce all

---

<sup>1</sup> . See *Guo Wengui v. Clark Hill, PLC*, 338 F.R.D. 7, 10-11 (D. D.C. 2021).

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

reports of its forensic investigation into a cyberattack that led to the public dissemination of the plaintiff's confidential information. At the time of the breach, the defendant employed an IT vendor. The defendant retained counsel to represent it in matters related to the breach, and counsel retained a forensic consultant to investigate the breach and defendant's response to it. The court rejected the defendant's argument that its counsel retained the forensic consultant solely for the purpose of obtaining legal advice from its lawyer. The forensic consultant undertook a full investigation to determine not only how the attack happened but also how the defendant could strengthen its cybersecurity. The consultant also shared the information with the defendant's IT staff and with the FBI. Thus, the court found, the report was not subject to the attorney-client privilege.<sup>2</sup>

- Rulings in *In re Marriott International, Inc. Customer Data Security Breach Litig.* (D. Md. 2021):
  - Emails within the company to employees that were never transmitted to counsel are not privileged, even though made as part of counsel-directed breach investigation.
  - Attachments to emails to/from Marriott's outside counsel sent for purposes of legal advice are protected as privileged. While a company can't turn a non-privileged document into a privileged one by sending the document to its lawyer, nevertheless a document is protected as an attachment to the email to the lawyer when sent to bring information to the lawyer's attention or answer one of the lawyer's questions for purposes of legal advice. This is because "[t]he fact that a client included a document in a request for legal advice is privileged" since "it partially reveals the substance of the client's privileged communication to an attorney." In other words, "the email with its attachment sent to or from" the attorney "is the privileged 'communication.'"
  - Ruling sustaining Marriott's privilege claim over post-breach work by IBM, specifically its work to help Marriott's counsel understand how Marriott's security alerting tool functioned, and to conduct a post-incident security assessment. Plaintiffs pointed to Marriott's prior business relationship with IBM to argue that the real reason for hiring IBM for these tasks was business-driven, but the court disagreed: the declarations submitted by Marriott demonstrated that the purpose of the inquiry into the alerting system was to help Marriott's counsel understand a specific, distinct issue relating to the alerting system as relevant to understanding the breach for purposes of advising Marriott on its legal obligations, which was different from the prior work. It also found, again based on the declarations, that the post-breach

---

<sup>2</sup> . *Id.* at 13-14.

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

security assessment was to help develop the legal strategy for responding to regulatory investigations and lawsuits.

▪ *In re Facebook* case:

- *Attorney General of the Commonwealth of Massachusetts v. Facebook*, SJC-12946, slip op. (Mass. March 24, 2021): ruled that most of the Attorney General’s requests for information on Facebook’s investigation into the Cambridge Analytica scandal did not seek communications between Facebook and its counsel, but instead sought to ascertain the underlying facts revealed by the investigation. As the Court observed, “[i]n the first five requests [of the CID], the Attorney General is not requiring the production of documents or communications that were exchanged between Facebook (including its employees) and its attorneys, and the requests permit Facebook to comply without disclosing any such communications.” The sixth request did seek communications that could be protected by the attorney-client privilege. Agreeing with the trial court, the appellate court remanded the matter so that Facebook could prepare a detailed privilege log. The Attorney General could then challenge withheld documents on a case-by-case basis

- In *Maldondo v. Solara Medical Supplies, LLC*, Civil Action No. 20:12198-LTS (D. Mass. June 2, 2021), the Magistrate Judge denied Plaintiffs’ motion to compel third-party Charles River Associates to comply with a subpoena to produce documents related to a “privileged forensic investigation” for which no report was completed and findings were communicated verbally throughout the investigation. The Magistrate held that the documents at issue were both privileged and work product, and that privilege attached because the work was performed to assist counsel in advising Solara. Order at 9.

○ Work product:

- In the case *In re Dominion Dental Services USA, Inc. Data Breach Litigation* 429 F. Supp. 3d 190 (E.D. Va. 2019) the court considered a motion to compel a report written by a third-party cybersecurity firm (Mandiant) following the underlying data breach at issue in the case. Despite arguments from Defendants that the report was prepared to inform legal counsel in anticipation of litigation, and is thus protected through work-product protection, the court granted the motion. In granting the motion, the court pointed to the company’s pre-existing relationship with Mandiant and the company’s own touting of Mandiant’s investigation to its customers.
- In *In re Capital One Consumer Data Sec. Breach Litig.* (E.D. Va. 2020), the court found that, although at the time the forensic consultant began its incident response services, there was a “very real potential” that Capital One would face substantial claims following its announcement of a data breach that affected millions of consumers, Capital One failed to establish that its consultant would not have

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

prepared the report in substantially similar form “but for the prospect of litigation.” The court reviewed the scope of services covered under the consultant’s engagement agreement with Capital One’s counsel, and a scope of work agreement between the consultant and Capital One that predated the breach, and noted that the primary difference between the two was a specific reference in the letter agreement to outside counsel’s role. Accordingly, the court noted that, in the absence of outside counsel’s involvement, there was “no difference” between what the consultant produced and what it would have produced in the ordinary course of business absent outside counsel’s involvement.

- Compare to a separate work product decision in the Capital One litigation, *Capital One Consumer Data Security Breach Litigation* (MDL No. 1:19-md-2915 (E.D.Va. 2020)) where plaintiffs filed three separate motions seeking to compel the production of a root cause analysis report prepared by PricewaterhouseCoopers (the “PwC Report”). Capital One opposed each motion, arguing that the PwC Report was protected by the work-product doctrine. Capital One prevailed each time. The key distinction with the decision on the Mandiant report appears to be the lack of a pre-incident relationship between Capital One and PwC.
- In *Clark Hill*,<sup>3</sup> the court quoted *Dominion Dental* and *Premiera I* when it rejected the defendant’s argument that a forensic report was prepared in anticipation of litigation. The defendant had presented a nuanced argument that the post-incident CI report qualified as being prepared in anticipation of litigation because it was the result of only one half of a “two-tracked investigation of the incident.”<sup>4</sup> One track, Clark Hill’s usual cybersecurity vendor worked to investigate and remediate the attack to preserve business continuity, and, on a “separate track,” the defendant’s counsel hired the forensic consultant for the sole purpose of gathering information to render legal advice.<sup>5</sup> The court flatly rejected the defendant’s argument, finding no support in the evidentiary record. Rather, defendant’s internal emails referred to the forensic consultant as the “incident response team,” and defendant had not involved its usual cybersecurity vendor once counsel retained the forensic consultant.<sup>6</sup>
- In *In re Rutter’s Data Sec. Breach Litig.*,<sup>7</sup> the court found that the work-product doctrine did not shield the forensic consultant’s report because it was not prepared for litigation purposes. The court focused primarily on the timing of the retention of the consultant and its scope of work.

---

<sup>3</sup> *Guo Wengui v. Clark Hill*, 338 F.R.D. 7, 10-11 (D. D.C. 2021).

<sup>4</sup> *Id.*

<sup>5</sup> *Id.*, citing Target, 2015 WL 6777384 at \* 2-3.

<sup>6</sup> *Id.* at 11.

<sup>7</sup> *In re Rutter’s Data Security Breach Litigation*, 2021 WL 3733137 (M.D. Pa. July 22, 2021).

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

The consultant's scope of work described its services as relating to determining whether unauthorized activity within the Rutter's systems environment resulted in the compromise of sensitive data, and if so, the extent of the compromise.<sup>8</sup> The court determined that that language demonstrated that the defendant "did not have a unilateral belief that litigation would result at the time it requested" the consultant prepare a report.<sup>9</sup> Put another way, "without knowing whether or not a data breach occurred, Defendant cannot be said to have unilaterally believed that litigation *would* result."<sup>10</sup> Moreover, the defendant's corporate representative testified that he was unaware of anyone contemplating a lawsuit at the time the consultant prepared its report.<sup>11</sup>

- *Attorney General of the Commonwealth of Massachusetts v. Facebook*, SJC-12946, slip op. (Mass. March 24, 2021):
  - The Attorney General of Massachusetts issued Civil Investigative Demands to Facebook in the wake of the Cambridge Analytica incident. Specifically, the Attorney General sought information generated by Facebook's "App Developer Investigation" ("ADI") launched in March of 2018 in response to the revelation that Cambridge Analytica had used data obtained through a Facebook app developer to influence the 2016 Presidential election in the United States. Facebook refused, on work product and attorney-client privilege grounds, to produce "information generated in the course of its ADI about the specific apps, groups of apps, and app developers that Facebook claims to have flagged as potentially problematic or, at the very least, has identified as worthy of additional examination." 2020 WL 742136 at \*5. The trial court concluded that the ADI was not undertaken in anticipation of litigation, but was instead performed for business purposes. In support of this conclusion, the court pointed to Facebook's "ongoing app enforcement program from 2012 to the present, not for reasons of litigation or trial, but rather because the Company has made a commitment, and has a corresponding obligation to protect the privacy of its users." *Id.* \*10. The Court was "unpersuaded . . . by Facebook's argument that the information and materials generated by its ADI qualify for work-product protection because the ADI is a 'lawyer-driven effort' that was 'born amid and because of' the Cambridge Analytica incident." *Id.* at \*10 n.4. The Massachusetts Supreme Court reversed this holding. While recognizing that "the existence of an ongoing compliance program is an important consideration when assessing whether

---

<sup>8</sup> . *Id.* at \*2.

<sup>9</sup> . *Id.*

<sup>10</sup> . *Id.*

<sup>11</sup> . *Id.* at \* 3.

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

an internal investigation was undertaken in anticipation of litigation,” the unanimous court reasoned that “the ADI is meaningfully distinct from Facebook's ongoing enforcement program. It is staffed by outside counsel and outside forensic consultants, and it has its own distinct methodology. It is focused on past violations, not ongoing operations, and it serves a very different purpose: defending Facebook against the vast litigation it is facing, rather than just improving its ongoing operations.”

- Agreeing with the trial court, the Supreme Court also ruled, however, that although the information in question was protected by the work-product protection, the Attorney General had shown a “substantial need” for the information and that there was no other source from which the substantial equivalent of the withheld information could be obtained without “undue hardship. Unlike the trial court, however, the appellate court could not conclude that none of the requested information fell into the category of opinion work product, which would remain protected. It listed the following as an example of a category of information that may constitute opinion work product: the request that Facebook identify apps that posed “an elevated risk of potential policy violations,” as such a request “appears to seek to reveal undisclosed aspects of the ADI process that may divulge counsel's investigatory practices, legal risk assessment, and other thought processes and impressions.” Accordingly, the Supreme Court remanded the matter to the trial court to determine what information constituted fact work product as opposed to opinion work product
- In *Maldonado v. Solara Medical Supplies, LLC*, Civil Action No. 20:12198-LTS (D. Mass. June 2, 2021), the Magistrate Judge denied Plaintiffs’ motion to compel third-party Charles River Associates to comply with a subpoena to produce documents related to a “privileged forensic investigation” for which no report was completed and findings were communicated verbally throughout the investigation. The Magistrate held that the documents at issue were both privileged and work product, and that work-product protection attached because the materials were prepared “to prepare for the inevitable lawsuits that followed the data breach.” Order at 9. The Magistrate further held that Plaintiff had not established substantial need for the materials to prepare for their case because the factual information was otherwise available to Plaintiff with few limitations. Order at 9.
- Expert privilege
  - In *re Marriott* (D. Md. 2021): Plaintiffs’ requests for discovery of certain documents relating to CrowdStrike’s forensic investigation were denied due to the nontestifying expert privilege (FRCP 26(b)(4)(D)) because Marriott hired CrowdStrike in anticipation of litigation, and this *reason for hiring CrowdStrike* rather than *the*



This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

*reasons for generating the specific documents at issue* controlled the discoverability question under the nontestifying expert privilege.

- This highlights that relying on the nontestifying-expert privilege can potentially avoid the need for a document-by-document analysis of the reason for generating particular material.
- Marriott had originally claimed work product and attorney/client privilege over CrowdStrike's breach investigation, but rather than rule on whether those protections apply, the court in a 2020 ruling deferred decision until Marriott decided whether it would call CrowdStrike as an expert witness. The court's thinking was that if Marriott did decide to call CrowdStrike as a testifying expert, then discoverability would be determined by the discovery rule applicable to testifying experts (FRCP 26(b)(4)(C)) rendering the work product/privilege question moot. Ultimately, Marriott decided not to call CrowdStrike as a testifying expert, and plaintiffs then moved to compel.
- Basic principles to be added to Part B of the Commentary:
  - Fed. R. Civ. P. 26(b)(4) sets forth rules for materials pertaining to experts.
    - General rules for non-testifying experts: Fed. R. Civ. P. 26(b)(4)(D)
    - General rules for testifying experts:
      - Draft reports/disclosures: Fed. R. Civ. P. 26(b)(4)(B).
      - Attorney/expert communications: Fed. R. Civ. P. 26(b)(4)(C)

### **III. Practical Guidance: Dual Track Investigations**

- Overall:
  - Based on the new cases and existing case law, we propose to revise the Commentary to explain in more detail the relationship between privilege, work product, and dual track investigations that may occur in the cybersecurity context. We propose that this addition would be a new subsection to Part C of the Commentary.
- Dual-track investigations attempt to split the internal investigation following a data breach into a legally oriented track and a track that is focused on remediation (and/or, in the case of a payment card breach, a track required by card brand rules).
  - Companies can then seek to assert privilege over the legal track, and disclose the remediation-focused track.
- The law is novel and unsettled with respect to the application of privilege in such dual track investigations.
- Benefits of dual track investigations to defendants and responding parties:
  - Creating separate investigations improves the likelihood that defendants will be able to assert privilege over their legally oriented tracks
    - Defendants can therefore obtain legal advice and assist their counsel in anticipation of litigation while minimizing the risk of revealing sensitive elements of their defense strategy

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

- A clear line between tracks allows defendants to more easily identify what should and should not be privileged
- Benefits of dual track investigations to plaintiffs and requesting parties:
  - Can aid with discovery of relevant facts; defendants should be more willing to disclose the findings of their remediation-focused investigations if certain sensitive elements are protected within the legally focused track
  - This could speed up the discovery process
- Drawbacks to Dual-track Investigations
  - Expensive - doubles the cost to have two investigators doing the same work
  - Cumbersome - both investigators need access to the same information and will be walking all over each other to do this work
  - Encourages companies to make one investigation (the business track) more cursory and to present the information in a more favorable way for the company
  - Takes more time to get a second forensic investigator, especially when speed to respond and recover are critical issues for the business--generally more critical than preserving privilege.
  - Lines between dual tracks can blur significantly as the court found in *Clark Hill*.
- Several recent cases provide guidance on how courts analyze privilege asserted in conjunction with a dual track investigation
  - Courts often consider whether the two tracks of investigations were performed by separate teams.
    - *In re Target*, 2015 WL 6777384 (D. Minn. Oct. 23, 2015), provides an example of this; Target hired Verizon to conduct both tracks of its investigation, but only asserted privilege as to the findings of one track
      - The legally oriented team, for which Target asserted privilege, was designed to “enable counsel to provide legal advice to Target, including legal advice in anticipation of litigation and regulatory inquiries.” *Id.* at 1.
      - The remediation team, for which Target did not assert privilege, investigated “so that Target and Verizon could learn how the breach happened and Target (and apparently the credit card brands) could respond to it appropriately.” *Id.* at 2.
    - *In re Capital One Consumer Data Security Breach Litigation*, No. 1:19-md-2915, 2020 WL 2731238 (E.D. Va. May 26, 2020), suggests that separate teams may improve the likelihood of protecting their legal track’s findings by hiring separate firms to conduct each track of the investigation
      - In *In re Capital One*, Capital One attempted to assert privilege as to the findings of two investigations, one conducted by Mandiant and one conducted by PwC. They were successful only as to the PwC report.

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

- The court did not consciously distinguish between the two investigations because they were conducted by different firms, but following this aspect of Capital One's approach may be useful to defendants from an optics standpoint because it will reinforce the notion that the tracks are indeed separate
  - Splitting a dual-track investigation between multiple firms might also decrease the risk of unauthorized cooperation between the tracks, which could in turn compromise a company's ability to assert privilege
- In another case, an investigation launched merely under suspicion that a breach *might* have occurred was not be considered to be "in anticipation of litigation," *In re Rutter's Data Sec. Breach Litig.*, No. 1:20-CV-382, 2021 WL 3733137, at \*2 (M.D. Pa. July 22, 2021)
  - In *Rutter's*, the defendant sought to withhold a report it had commissioned from Kroll Cyber Security after it was notified of a potential data breach
  - Because the purpose of the report "was to determine *whether* data was compromised," the court held that Rutter's "did not have a unilateral belief that litigation would result at the time it requested the Kroll Report."
  - The court contrasted this from a successful dual-track approach in *In re Target*, wherein Target directed Verizon to conduct a legally focused investigation only after litigation had commenced
- The courts further look to whether the legal track was clearly designed to, and actually intended to, inform counsel and aid the company in its preparation for litigation
  - Again, *In re Target* is illustrative. In determining that the findings of Target's legally-oriented investigation were privileged, the court relied on the fact that this investigation was specifically designed to inform Target's lawyers about the breach: "Target's lawyers needed to be educated about the breach so that they could provide Target with legal advice and protect the company's interests in litigation that commenced almost immediately after the breach became publicly known." *In re Target*, 2.
  - Similarly, in *In re Capital One*, the court found that the contents of the PwC report were privileged because the "driving force [behind the PwC report] was ... to deal with the litigation and the legal issues" relating to the data breach and to "provide legal advice to [Capital One's] Board."
  - In contrast, Capital One unsuccessfully sought to assert privilege over its Mandiant report; court held that that Capital

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

One did not demonstrate “sufficient evidence to show that the incident response services performed by Mandiant would not have been done in substantially similar form even if there was no prospect of litigation.” 2020 WL 3470261 at 4.

- By stating at the outset of a legally focused investigation that that the purpose is to inform a company’s counsel about a recent data breach and arm them with the necessary knowledge to litigate on the company’s behalf, a company will improve its chances of being able to successfully assert privilege over the findings of that investigation at a later date
- Even where a dual track investigation is performed, courts still analyze whether the requirements for privilege or protection are satisfied for the legal track of an investigation and have declined asserted privileges in some circumstances.
  - At least two courts have viewed the existence of a contractual relationship between an affected company and cyber security firm that began prior to a breach as evidence that any subsequent report was not prepared for litigation
    - See, e.g., *In re Capital One; In re Dominion Dental Servs. USA, Inc. Data Breach Litig.*, 429 F. Supp. 3d 190, 194 (E.D. Va. 2019).
    - In contrast, the court found the lack of an existing relationship to be persuasive when it extended privilege to Solara’s legally oriented investigation in *Maldondo v. Solara Medical Supplies, LLC.*, Civil Action No. 20:12198-LTS, at 8 (D. Mass. June 2, 2021).
  - In *In re Dominion Dental*, the court found that the existence of a preexisting relationship between the defendant and Mandiant, along with the fact that Dominion did not sufficiently alter its instructions to Mandiant after litigation became a possibility, made it implausible to claim that Mandiant’s report was prepared “in anticipation of litigation”
    - “Most significantly, the actual description of services promised in the April 2019 statement of work, which include computer incident response support, digital forensics support, advanced threat actor support, and advanced threat/incident assistance . . . are almost identical to the services promised in the June 2018 statement of work, entered into by the defendants and Mandiant months before any threat of litigation. The addition of language referencing ‘under the direction of Counsel’ appears to be designed to help shield material from disclosure rather than to fundamentally alter the business purposes of the work.” *Id.* at 194.
    - The court placed a focus on the fact that no new directive was issued to the cyber-security firm:

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

“Defendants publicized the retention and work of Mandiant for ‘non-litigation purpose[s]’ such as reassuring customers and communications strategy.” *Id.* at 194.

- Another court rejected assertions of privilege where the findings of the legal track were disseminated widely and used for purposes other than litigation.
  - In *Wengui v. Clark Hill PLC*, No. 19-3195 (D.D.C. Jan. 12, 2021), Clark Hill nominally conducted a dual-track investigation by retaining separate firms to conduct each track of its investigation
  - The court declined to extend privilege to the findings of the Duff & Phelps report, which Clark Hill asserted was a legally-oriented report designed to inform its counsel
  - The court relied in part on the fact that the Duff & Phelps report was shared “not just with outside and in-house counsel, but also with ‘select members of Clark Hill’s leadership and IT team.’” *Id.* at 12. The report was also shared with the FBI.
  - This, along with the fact that the report focused on remediation, undermined the assertion that it was attorney work product intended only to prepare Clark Hill for trial
- In denying privilege to Clark Hill’s Duff & Phelps report, the court also relied in part on the fact that nearly all of the factual findings could be found only in that report; the competing report from eSentire was effectively worthless.
  - “Clark Hill turned to Duff & Phelps instead of, rather than separate from or in addition to, eSentire, to do the necessary investigative work.” *Clark Hill* at 12.
  - Because of this, Clark Hill could not reasonably claim that the Duff & Phelps report existed only to aid its legal counsel, and plaintiffs could demonstrate a substantial need for the report’s factual findings.
- In contrast, the court in *Solara* denied the plaintiff’s motion to discover Solara’s legally oriented investigation because the factual findings it contained were all available in the other track of Solara’s investigation. *See Maldondo v. Solara Medical Supplies, LLC*, Civil Action No. 20:12198-LTS, at 9 (D. Mass. June 2, 2021) (“[T]he underlying facts are available to plaintiffs without any need to invade’ privileged materials”).
- Where dual track investigations occur, crosstalk between the two investigative teams is worth considering.
  - Crosstalk could arise in various contexts, such as:

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

- Legal track consultants discover an indicator of compromise (IOC) and pass it along to the remediation track team to ensure that it is addressed
- A legal track consultant installs EDR tools to study ongoing malware operation and wants to share telemetry with the remediation track team
- The remediation track team observes something of note and asks the legal track team if it has observed the same thing
- Crosstalk between the tracks may have benefits:
  - Both plaintiffs and defendants in a cyber security breach case have an interest in preventing new or ongoing data breaches
  - It would be counterproductive to discourage defendants from sharing information between teams in circumstances like these by threatening to remove the protection of privilege if they do
  - Furthermore, limited crosstalk between teams should improve the efficiency of each investigation; this should save both plaintiffs and defendants time and money
- There is limited court guidance on how such crosstalk may affect claims of privilege.
  - In finding that Capital One could assert privilege over its PwC report, the *In re Capital One* court noted that “Capital One pursued two separate paths, one litigation driven; one, business driven” and the fact that “those paths crossed at some point does not erase the critical difference created at birth in the provenance of those separate investigations.”
    - This is despite the fact that some aspects of the PwC report were used for remediation
    - The court noted that a report from a legally oriented investigation “may also be used for ordinary business purposes without losing its protected status.”
  - Comparing *In re Capital One* and *Clark Hill* shows some of the different considerations that affected those determinations
    - Certain findings from Capital One’s PwC report were used to supplement the separate efforts of a team from Mandiant; Clark Hill’s eSentire report had little value, so the information Clark Hill used for remediation came *almost exclusively* from the Duff & Phelps report
    - This went far beyond “crossing paths,” as it was described in the *Capital One* opinion

#### **IV. Practical Guidance: Relationship Between the Burden Of Proof and Limits on the Ability to Obtain Information, and an Exploration of the Concept of “Substantial Need”**

- Overall:
  - Based on the new cases and existing case law, we propose to revise the Commentary to add a section exploring in more detail the relationship between privilege, work product, and limits on the ability to obtain relevant

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

information when facts and privilege are intertwined in the cybersecurity context. We propose that this addition would be a new subsection to Part C of the Commentary.

- There are the key facts that a plaintiff needs to prove its case that it can only acquire through the defendant
- Factual questions plaintiff needs to answer
  - DATA SECURITY PRACTICES (pre-breach discovery)
    - What written (internal and external privacy) and security policies did the organization have in place?
    - What security practices did the defendant implement prior to the incident?
      - What was the state of the company's pre-breach security controls (eg patching)?
      - What/when were critical vulnerabilities known and how, if at all, addressed?
    - Was the defendant aware of the vulnerability that led to the incident? If so, what did the defendant do to mitigate that vulnerability?
  - TIMELINE OF THE BREACH
    - When did the incident occur?
    - When did the defendant become aware of the incident?
    - When did the defendant determine or have enough evidence to determine that the incident was a breach?
    - When did the defendant determine the scope of the data impacted?
    - What notifications and public statements did the defendant make to regulators, customers, contract partners, and the general public?
    - When did the defendant notify regulators, customers, contract partners?
  - SOURCE OF THE BREACH
    - How did it occur?
    - What caused the incident?
    - Who was involved in the incident
  - SCOPE OF BREACH
    - What systems were impacted?
    - What data and information was impacted?
    - Was data accessed, acquired, etc.?
    - Was the data encrypted?
  - REMEDIATION
    - What actions did the defendant take once it became aware of the incident?
      - What remedy was given to consumers (eg credit monitoring)?
    - How was the incident resolved?
      - Has the security vulnerability or issue been addressed/cured?
- There are many sources to discover those facts, some are purely factual and unlikely to be considered privileged and some tend to have privileged aspects

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

- In some ways, this is an extension of the *Attorney General of the Commonwealth of Massachusetts v. Facebook* case where the court found “substantial need” for the information sought by the Attorney General, but ultimately remanded the matter for the trial court to determine what information was fact work product vs opinion work product.
- Sliding scale of sources from least likely to be privileged to most likely to be privileged based on how likely opinion might be intertwined with facts.
  - We used some of the types of CI detailed in the commentary but also expanded some of the categories.
  - Each of the sources below would contain facts that help answer the questions above.
    - Pre-Breach
      - Technical Inventories, Configuration Reviews, Vulnerability Scans, and Penetration Tests, Security and IT-oriented alerts and logs
      - Company Policies, Practices, Procedures, IR Plans, IR Playbooks, Risk register
      - Security Risk Assessments, Outside Audits, Internal Audits, and Remediation Efforts
      - Reports of the Security Team and Tabletop Exercises
      - Board-level documents and communications
    - Post-Breach
      - Security and IT-oriented alerts and logs
      - ticketing systems, messaging systems, GRC systems, collaboration tools, helpdesk phone logs
      - Post-Incident Security Assessments
      - Regulatory and Industry standard reports
      - Law enforcement and investigation disclosures
      - Sworn testimony and interviews
      - Breach log (document or spreadsheet)
      - Emails about the breach
      - Forensic consultant report

## V. **Entity Specific Guidance**

- Overall:
  - Based on the new cases and existing case law, we also propose to revise the Commentary to provide entity-specific guidance for a variety of additional entities based on the appropriateness or availability of case law related to each individual entity relationship, including, potentially: insurer/insureds, service providers/vendors, joint defense groups/joint common interest groups, agency/affiliate relationships, and communications between different/unrelated companies on areas of mutual interest/risk.
  - We propose that this addition would involve consideration of modifications to subsection 3 of Part C of the Commentary waiver section for particular entities, and potentially addition of a new subsection to Part C of the Commentary with a



This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

title such as “Legal Evaluation and Practice Guidelines as to Application of Attorney-Client Privilege and Work-Product for Specific Entities.”

- As of the date of this draft, we have not fully investigated the insured/insurer relationship, but would seek to do that in the next iteration of this drafting group. In the meantime we have noted some preliminary considerations on this issue below.
- Entity specific guidance for vendors and service providers
  - A range of external vendors and service providers may be engaged to assist an organization and its legal counsel to prepare for and respond to cybersecurity incidents. These may include, among others:
    - Digital Forensics/Incident Response firms
    - Managed Security Service Providers
    - E-Discovery/data hosting and analytics firms
    - Penetration testing firms
    - Source code review consultants
    - Cyber risk assessment consultants
    - Crisis communications and public information consultants
  - Cases involving attorney-client privilege and work product protection in the cybersecurity context suggest that the practices of these third parties are material considerations and may even be pivotal in a court’s determination. As such, firms offering pre- and post-incident services may wish to observe the following guidance.
  - **Pre-Engagement Practices**
    - *Training.* Vendors should train their engagement managers and service delivery teams to sensitize them to the nuances of privilege in the cybersecurity context. Doing so will prepare them to address the potential privileged nature of the vendor’s work in the pre-engagement scoping and contracting phase and help them avoid actions during the engagement that might waive privilege.
    - *Engagement Agreements.* Courts have scrutinized engagement agreements to discern the purpose of the vendor’s retention. Accordingly, in engagements that support counsel’s provision of legal advice, the agreements should include language making clear the purpose of the retention. When a client-vendor relationship is created pre-incident and for an apparent business purpose, if there is the potential that the vendor will be called upon to support counsel’s provision of legal advice, the parties are best served to use a specific statement of work or separate agreement to address those circumstances.<sup>12</sup> Even in those circumstances, a court may conclude that the business purpose for the vendor’s original retention is imputed to a successive assignment, especially if the scope of

---

<sup>12</sup> *New Albertson’s Inc. v. Mastercard Int’l, Inc.*, Case No. CV01-17-04410 (Idaho Dist. Ct. 4<sup>th</sup> Dist. May 31, 2019), at 5 (noting that prior direct retention of cybersecurity firm (Dell) by client was terminated once outside counsel was engaged and outside counsel retained same firm for privileged investigation).

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

services has not materially changed.<sup>13</sup> Therefore, in an abundance of caution, the vendor may wish to assign separate personnel to the latter work to counter the view that it was only an extension prior services rendered to the client for business purposes.

- *Billing and Payment Arrangements.* In setting up an engagement, vendors should consider what entity, unit, or individual should be chosen for billing and payment. If the engagement's purpose is to support outside counsel's provision of legal advice and/or in anticipation of trial, it may be better for the vendor to bill outside counsel for the services, rather than the ultimate client. Where that arrangement is not feasible, submitting invoices to internal legal counsel may strengthen a client's claim of privilege of CSI involving or generated in the engagement. The same can be said of having the engagement funded through the client's legal departments budget, as opposed to another business unit.<sup>14</sup> While vendors cannot control this, they can facilitate a discussion with the client about this option and the potential bearing it may have on later determinations about privilege.
- **Practices During an Engagement**
  - *Meetings and interim written communications* Vendors should confer with legal counsel at the outset of and regularly during the engagement to provide verbal updates and receive guidance related to progress of the work.<sup>15</sup> In addition, the vendor's staff should refrain from meeting with, reporting to, or receiving taskings from others in the client's business, unless supervising counsel specifically approves. While the participation of others in the business may be required at various times to support the vendor's work (e.g., to inform the vendor about the client's IT environment and data holdings, to furnish access to data or systems) care should be given not to widen the circle of participants beyond those necessary to support legal counsel's provision of advice.

---

<sup>13</sup> *In re: Capital One Consumer Data Security Breach Litigation*, MDL No. 1:19md2915 (AJT/JFA) (Document 490) (E.D. Va. May 26, 2020), at 11 (distinguishing prior case in which outside counsel retained cybersecurity vendor from instant case in which a client-vendor relationship existed when incident was discovered in determining that report was not prepared because of potential litigation).

<sup>14</sup> *In re: Capital One Consumer Data Security Breach Litigation*, MDL No. 1:19md2915 (AJT/JFA) (Document 490) (E.D. Va. May 26, 2020), at 8 (determining that investigation was not entitled to privileged status in part because the client paid a cybersecurity investigator out of a retainer that was classified as "business-critical and not a legal expense at the time it was paid"); *id.* at 13 (noting that scope of work had not materially changed from prior direct engagement by client of cybersecurity investigator and later engagement of same by outside counsel).

<sup>15</sup> *New Albertson's Inc. v. Mastercard Int'l, Inc.*, Case No. CV01-17-04410 (Idaho Dist. Ct. 4<sup>th</sup> Dist. May 31, 2019), at 6 (finding privilege extended to investigation supervised by external counsel who "did take an active role in directing the ongoing investigation").

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

- Relatedly, written communications between a vendor's staff and the client's team should be limited to what is necessary to advance the objectives defined by legal counsel. Counsel should we copied on any such communications and the messages themselves should bear an appropriate marking that they are privileged CSI.
- Diary entries for timekeeping purposes should, at a minimum, note the participation of legal counsel in meetings and note any taskings received from the attorneys.
- *Internal Procedures.* Vendors will undoubtedly have executed a written agreement with confidentiality provisions at the start of the engagement. The vendor's internal files should be maintained and marked in such a way that the privileged status of their work is apparent (if indeed they are supporting the provision of legal advice and not serving only a business purpose of the client) and access limited to personnel assigned to the matter or with a bona fide need-to-know.
  - A vendor should preserve data that it receives for analysis from a client in a privileged engagement so that it is available for production to a third party in litigation. The availability of such data offers a potential litigant the ability to analyze it and may help the client maintain privileged status over the vendor's analysis of the same data.
- *Deliverables (Reports, Presentation Slides, and Memoranda)* Before documenting findings in a written report, presentation slides, or memorandum in a privileged engagement, the vendor should confer with counsel as to whether such a deliverable is desired and what its scope should be. Recommendations for remediation or future improvements should not be incorporated into a forensic report detailing matters that occurred in the past without specific instructions from counsel to include them. Deliverables should be maintained in draft and circulated to counsel for review and comment prior to sending to the ultimate client. Vendors should avoid sending written deliverables to individuals or groups within the client's organization who are not involved in supporting counsel's provision of legal advice without first discussing with counsel.<sup>16</sup> Even

---

<sup>16</sup> Compare *Guo Wengui v. Clark Hill, PLC*, 338 F.R.D. 7, 12 (D.D.C. 2021) (distribution of forensic report beyond outside and in-house counsel, specifically to "select members of [client's] leadership and IT Team," supported finding that report was not protected work product), *In re: Capital One Consumer Data Security Breach Litigation*, MDL No. 1:19md2915 (AJT/JFA) (Document 490) (E.D. Va. May 26, 2020), at 10 (cybersecurity firm's report was disseminated widely, including to the client's "cyber technical, enterprise services, information security and cyber teams" and that it was used by the client "for various business and regulatory purposes"), and *In re Dominion Dental Servs. USA, Inc. Data Breach Litig.*, 429 F. Supp. 3d 190, 194 (E.D. Va. 2019) (client could not represent that purportedly privileged forensic report was not shared with its incident response team), with *In re Experian Data Breach Litig.*, 2017 WL 4325583 (C.D. Cal May 18, 2017), at \*3 (stating that if the report "was more relevant to the [client's]

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

when a wider distribution is authorized by counsel, caveats limiting the deliverable's use, as well as restrictions on further dissemination, should be placed in the document.<sup>17</sup>

- Entity Specific Guidance for agency/affiliate relationships
  - There are very few cases directly on point concerning 1) agency/affiliate relationships, or 2) communications between different/unrelated companies on areas of mutual interest/risk. Since both of these concepts are discussed in the current section entitled 'Common Interest, Joint Defense, and Joint Representation Arguments Against Waiver' starting on page 74 of the Commentary, there may not be enough new cases to justify separate sections for these two topics, and the analysis would be very similar to what is already in there. The case law may counsel revisions to the current section, however, incorporating certain passages from cases below.
  - On Agency/Affiliate, *Premera I*, 296 F. Supp.3d 1230, 1247–50 (D. Or. 2017) discussed in the Common Interest section still seems to be the case most on point. The Commentary states, in part, the following: “The court in *Premera I* had the occasion to review whether the disclosure of CI to third parties who were not defendants in the same litigation, but in similar litigations, was shielded by the common-interest doctrine. Noting that generally joint-defense or common-interest parties are subject to the same litigation, the court found that entities in similar litigation to which *Premera* had disclosed documents would share a sufficient common interest if they were subject to the same data breach, but otherwise would not.”
  - This applies to communications between different/unrelated companies on areas of mutual interest/risk, but doesn't really address agency/affiliation relationships.
  - As for agency/affiliate relationships, there isn't really much data breach law on agency/affiliate relationships at all. There is a secondary source cited in the commentary that somewhat discusses this:
    - “In addition to clients and lawyers, the definition of privileged persons includes agents of the client and the lawyer who assist in the representation. Privileged agents include non-employees such as paralegals and investigators. The presence of these third party agents does not waive the privilege if their presence was to permit the client and lawyer to communicate effectively or to further the representation in some way.”
  - The drafting team is not currently aware of any recent data breach cases where privilege was challenged based on waiver because of disclosure to a paralegal, investigator etc. One case, *In re Rutter's Data Sec. Breach Litig.*, No. 1:20-CV-

---

internal investigation or remediation effort, as opposed to being relevant to defense of the litigation, then the full report would have been given to [client's incident response team].”).

<sup>17</sup> *In re: Capital One Consumer Data Security Breach Litigation*, MDL No. 1:19md2915 (AJT/JFA) (Document 490) (E.D. Va. May 26, 2020), at 5 (noting that client seeking to avoid producing forensic report failed to identify any handling restrictions placed on dissemination of report within client's organization, to its board, to an external accounting firm, and to four regulators).

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

382, 2021 WL 3733137, at \*3 (M.D. Pa. July 22, 2021), has the following dicta that is on point and may be appropriate for a new section (or inclusion in a revised current section) of the Commentary:

“However, “[a]s a general matter, the privilege is not destroyed when a person other than the lawyer is present at a conversation between an attorney and his or her client if that person is needed to make the conference possible or to assist the attorney in providing legal services.” *Miller v. Haulmark Transp. Sys.*, 104 F.R.D. 442, 445 (E.D. Pa. 1984) (privilege not waived by presence of insurance agent who arranged coverage and aided in preparation of answer); *see also Quagliarello v. Dewees*, 802 F.Supp.2d 620, 632-33 (E.D. Pa. 2011) (finding no waiver of attorney-client privilege where 18-year-old student-plaintiff consulted with her lawyer in the presence of her parents and a neighbor who facilitated her obtaining legal counsel); *Harkobusic v. Gen. Am. Transp. Corp.*, 31 F.R.D. 264, 266 (W.D. Pa. 1962) (holding attorney-client privilege applied to communications between client's brother-in-law and various attorneys where brother-in-law was acting as client's agent in seeking legal advice). “These exceptions are consistent with the goal underlying the privilege because [this] type of disclosure is sometimes necessary for the client to obtain informed legal advice.” *Westinghouse*, 951 F.2d at 1424.”

*Rutter* didn’t really involve a waiver argument though—the plaintiffs sought production of a Kroll report prepared following a data breach and the analysis focused on whether it was prepared “in anticipation for litigation” or are communications that had a “primary purpose of providing or obtaining legal assistance” for the defendant. The case doesn’t really apply to waiver.

- *Guo Wengui v. Clark Hill, PLC*, 338 F.R.D. 7, 12 (D.D.C. 2021) has some language that could potentially be used in a revised section. There, the defendant’s General Counsel shared a Duff & Phelps investigative report “with outside and in-house counsel, but also with ‘select members of Clark Hill's leadership and IT team’ to ‘assist[ ] [Clark Hill] in connection with managing any issues, including’ — but notably not limited to — ‘potential litigation ... related to the ... cyber incident.’” The report was also shared with the FBI. The court thus found the following:

“The fact that “the [R]eport was used for a range of non-litigation purposes” reinforces the notion that it cannot be fairly described as prepared in anticipation of litigation. *Dominion Dental*, 429 F. Supp. 3d at 194; compare *id.* at 195 (“[I]n *Experian*, the full report was withheld from defendants’ incident response team. Here, defendants have not represented that the full report was withheld from them.”), with *In re Experian Data Breach Litig.*, No. 15-1592, 2017 WL 4325583, at \*2 (C.D. Cal. May 18, 2017) (concluding forensic report was work product) (“If the report was more relevant to *Experian's* internal investigation or re-mediation efforts, as opposed to being relevant to

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

- defense of this litigation, then the full report would have been given to that team.”); see also *In re Capital One Consumer Data Sec. Breach Litig.*, No. 19-2915, 2020 WL 2731238, at \*5 (E.D. Va. May 26, 2020) (rejecting work-product protection for forensic report “used by Capital One for various business and regulatory purposes”), *aff’d*, No. 19-2915, 2020 WL 3470261 (E.D. Va. June 25, 2020).”
- This case is not directly on point for waiver—it focused on whether the report would have been created in the absence of litigation, and the court expressly stated that “[b]ecause the Court finds the Report not subject to attorney-client privilege, it does not address Plaintiff’s separate argument that Defendant waived the privilege by disclosing the Report to the FBI.” Disclosure to law enforcement is also a separate category.
  - *In re Cap. One Consumer Data Sec. Breach Litig.*, No. 1:19MD2915 (AJT/JFA), 2020 WL 3470261, at \*6 (E.D. Va. June 25, 2020) is similar. Although the court noted “[t]hat distribution was to approximately 50 employees, a “corporate governance office general email box,” Capital One’s Board of Directors, and “four different regulators and to Capital One’s accountant” the court used this to support a finding that the report was not privileged.
    - The Capital One court also expressly stated that “[b]ecause the Court finds that the Report is not protected work product, it does not address Plaintiffs’ alternative positions that Capital One waived protection over the Report or that the Report must be disclosed pursuant to Federal Rule of Civil Procedure 26(b)(3).” Thus, waiver was not addressed and this case does not really apply.
    - A second Capital One decision has a bit more language that we can use in a new/revised section, but it also did not reach a decision on waiver because it found the report was not privileged:

“Given the ruling on the work product issue based on the “because of” standard, it is not necessary to address the waiver or substantial need issues discussed by the parties in their briefs. That said, it appears that the waiver argument may have some merit given the lack of evidence presented in this motion concerning the distribution of the Mandiant Report and what protections were taken to avoid having the Mandiant Report or the information contained therein disclosed to a person or entity in an adversarial relationship. As to substantial need, while it would be more efficient for the plaintiffs to have the results of Mandiant’s investigation, based on current record it appears that the event logs and network diagrams reviewed by Mandiant may be available to the plaintiffs.”
  - Finally, *Premiera II*, 329 F.R.D. 656, 667–68 (D. Or. 2019), has some language with respect to waiver, but it’s from 2019 and the Court did not have enough information to make a significant ruling

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

“Regarding documents provided to third-party vendors, the Court notes that not all \*668 third-party vendors are providing a business service. In the Privilege Opinion the Court found that some appear to be providing legal services. For vendors providing legal services, privilege and work-product protections attach in the same manner as communications with counsel and there is no waiver. The Court suggests that if disputes between the parties remain relating to documents shown to third-party vendors, Premera provide more information regarding how the vendor is performing legal services (e.g., whether the vendor was hired by counsel, the broad category of services being provided by the vendor, etc.) so that Plaintiffs can more effectively determine whether to challenge the disclosure as creating a waiver.

Regarding Mandiant, Mandiant has been hired by Premera's outside counsel and thus is not a “third party” that would trigger the waiver of privilege if documents are shown to Mandiant. Although the Court found that Mandiant's change in supervision from Premera to outside counsel was insufficient to change Mandiant's focus from a business purpose to a legal purpose because the scope of work did not change, that does not turn Mandiant into a stranger for purposes of privilege. Indeed, the Court expressly anticipated that there would be attorney-client privileged and work-product protected information provided to Mandiant that would need to be protected. *In re Premera*, 296 F.Supp.3d at 1246 (“[G]iven Mandiant's role in working with outside counsel, there may be some privileged communications or work-product protected information in the withheld documents. Thus, if there are specific documents or portions of documents that Premera contends contain privileged information ... or work-product information ... then they may properly be withheld.” (alteration added) ). Accordingly, disclosure to Mandiant does not waive privilege.”

- Overall, there may not be enough new case law to justify a stand-alone section for agency/affiliate, as the section would be very similar to the current section encompassing such a relationship and there are very few cases directly on point. The section could be updated, though, to include passages from the above cases, and to highlight that courts oftentimes do not reach the waiver argument because the facts of disclosure end up support a finding that the reports were not produced for litigation purposes.
- Entity Specific Guidance for communications between different/unrelated companies on areas of mutual interest/risk
  - As for the section on communications between different/unrelated companies on areas of mutual interest/risk, there are also very few data breach cases on point to include in an updated Commentary. The most extensive, which is already discussed in the Commentary, is *Premera I*, 296 F. Supp.3d 1230, 1247–50 (D. Or. 2017), which is discussed in part above. The current section (or a new section) could go into more detail on the *Premera I* decision, which is directly on point, but this is a case from 2017. The detail that could be added in a new or



This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

revised section would essentially be the following from the decision, which is currently addressed in the Commentary but in less detail:

“Premera stretches the definition of “common interest” beyond reasonable bounds. Under Premera's interpretation, different people or entities around the country that have a similar alleged product defect, or allegedly engaged in similar fraudulent schemes, or have been accused of similar forms of misconduct generally can claim a common interest and enter into common interest agreements. Under Premera's argument, as long as the claims asserted against those parties are the same or reflect the same the theory of liability, then they would have a “common” defense. That is not, however, how the common interest or joint defense doctrine works

...

As discussed above, communications between Premera and entities with data breaches other than the data breach that is the subject of this case, even if the data breach is “similar” or “connected to,” are not protected by the common interest doctrine. Thus, those communications are not privileged, and otherwise privileged information contained in such communications has had the privilege waived.”

- There are a few non-data breach cases that could be included in an updated Commentary, such as *In re Lawrence*, 954 N.W.2d 597, 602 (Minn. Ct. App. 2020), review denied (Mar. 16, 2021) (holding that as matter of first impression, waiving the joint-client privilege required the consent of all joint clients); *Choi v. Liberty Mut. Ins. Co.*, No. 16-CV-5392 (WFK), 2021 WL 790381, at \*5 (E.D.N.Y. Feb. 9, 2021), appeal dismissed (July 30, 2021) (“Plaintiff asserts the email is not privileged because the communication was between Defendant Liberty Mutual and a ‘third party.’ However, at the time Defendants produced this document Liberty Life Assurance Company of Boston was Liberty Mutual's subsidiary. The Court therefore finds the communication occurred between agents of a corporate parent and subsidiary, not between Defendants and a ‘third party.’”). These cases, however, are entirely outside the data breach or cybersecurity context, so it may not make sense to create a new subsection of the Commentary based on them.
- Entity specific guidance based on insurer/insured relationships
  - We are not aware of any data breach decisions addressing privilege or protection for communications between insurers and insureds.
  - Under non-breach case law applicable to insured/insurer communications, the inquiry is highly fact-specific. For instance, whether there is a “common interest” between insurer and insured may depend on whether the insurer has accepted coverage, whether litigation is anticipated or underway, and the reason for the communication at issue. We anticipate the practical guidance here would include a cautionary note that communications with insurers have a significant risk of being discoverable, except in limited situations.



This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

## **VI. Business Versus Legal Advice**

- Overall:
  - Based on the new cases and existing case law, we also propose to revise the Commentary to explain in more detail the line between legal advice and nonprotected business advice. We propose that this addition would be a new subsection to Part C of the Commentary with a title such as “Legal Evaluation and Practice Guidelines as to Application of Attorney-Client Privilege and Work-Product Protection in Evaluating Business versus Legal Advice.”
- In addressing claims of attorney-client privilege and work-product privilege, courts continue to grapple with the distinction between legal and business advice in the cybersecurity context.
  - The line is not always clear, particularly for in-house counsel.
  - In particular, courts often struggle with evaluating privilege claims over communications relating to compliance evaluations, network testing, and remediation.
- Attorney-Client Privilege: communication must be made for legal purpose.
  - Developments in the law—a primary purpose/the primary purpose vs. functionality/subject matter test framework from old commentary
  - Factors identified by courts:
    - Some relevant factors courts consider to determine the primary purpose of a mixed communication include: (1) the context of the communication and the content of the document; (2) whether the legal purpose permeates the document and can be separated from the rest of the document; and (3) whether legal advice is specifically requested and the extent of the recipient list. *Phillips v. C. R. Bard, Inc.*, 290 F.R.D. 615, 629 (D. Nev. 2013).
    - Briefly address *Premera* and *Clark Hill*, but focus only on guidance for determining what is legal vs. business—preexisting relationships (ordinary course of business), part of standard business operations, and whether legal advice is being requested or provided.
  - Application to specific categories of individuals (in-house lawyers, consultants, etc.)
    - Some courts apply a different standard when evaluating attorney-client privilege claims w/r/t communications with in-house counsel, as opposed to outside lawyers.
      - *In Re Ford Motor Co. Crown Victoria Police Interceptor Products*, 2003 WL 22217673, \*1 (N.D. Ohio July 1, 2003) -- In cases involving claims of privilege based on communications with in-house counsel, the law requires that the protections afforded by the attorney-client privilege be “applied more narrowly and cautiously.”
    - Rationale is that in-house counsel wear multiple hats and may be acting in a business capacity.
      - *Burgos-Stefanelli v. Napolitano*, 09-60118-CIV, 2009 WL 10667764, at \*2 (S.D. Fla. 2009) (recognizing unique issues regarding the attorney-client privilege arise when in-house counsel

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

is involved); *See also Georgia-Pacific Corp. v. GAF Roofing Mfg. Corp.*, 93 Civ. 5125, 1996 WL 29392, at \*3 (S.D.N.Y. 1995)(applying state law and recognizing "difficult fact specific questions" arise from communication between in-house counsel and management); *See Note Funding Corp. v. Bobian Investment Co.*, 93 CIV. 7427, 1995 WL 662402, at \*3 (S.D.N.Y. 1995)(recognizing the complexity of issues faced by in-house counsel as attorney or business consultant).

- Courts look at the communication and context to determine whether in-house counsel is acting as a legal advisor or business associate.
  - *In re Grand Jury Proceedings*, 2001 WL 1167497, \*27-28 (S.D.N.Y. Oct. 3, 2001)(privilege applied where in-house counsel was “functioning as an attorney”) -- “[l]ess protection is warranted when company officers have a mixed responsibility incorporating both business and legal aspects, and where their advice and communications are based on an on-going permanent business relationship rather than specific requests for legal advice.” *Id.* However, “the attorney-client privilege applies to communications between corporate counsel and corporate employees when the communications were made in order to secure legal advice from counsel.”
- Application to specific contexts
  - Compliance work—it’s a grey area.
    - Cover *Premera* and *In re Capital One Consumer Data Security Breach Litigation*, No. 1:19md2915 (E.D. Va.), and application [here](#).
    - *In re Seroquel Prods. Liab.Litig.*, No. 06-md-1769, 2008 WL 1995058, at \*7 (M.D. Fla. May 7, 2008) -- discussing “mixed purpose” documents involving in-house counsel including those involving regulatory compliance and ordering production of same; the court stated the fact of “extensive or pervasive regulation does not make the everyday business activities legally privileged from discovery.” *Id.* at 7.).
    - *Hennigan v. General Electric Company*, No. 09-11912, 2011 WL 13214444 (E.D. Mich. Jun. 1, 2011) -- ordering production of documents reflecting communications with in-house lawyer as to certain safety concerns related to microwaves manufactured by the defendant over privilege objections because the “Safety Council” where those safety concerns were discussed occurred in the ordinary course of the company’s operations and the related documents “consist[ed] of reports of a technical nature relating to consumer complaints or reported incidents of microwave fires or self-starts” rather than clear legal advice.
  - Public Relations issues: High bar.
    - *Premera I* has an extensive discussion of this issue.

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

- *In re Riddell Concussion Reduction Litigation*, No. 13-7586, 2016 WL 7108455, at \*7 - \*8 (Dec. 5, 2016) -- finding communications between in-house lawyers and other non-legal employees were not privileged because they involved “messaging” concerns and not legal issues.
- *Amway Corp. v. Procter & Gamble Co.*, No. 1:98-CV-726, 2001 WL 1818698, at \*5 (W.D. Mich. 2001) -- overruling privilege objections as to certain documents and communications exchanged between in-house counsel and other senior members of non-legal departments because, for example, certain documents related only to the defendant company’s “public relations strategy, which included the possibility of filing lawsuits.”
  - Other contexts:
    - *Burgos -Stefanelli v. Napolitano*, 09-60118, 2009 WL 10667764, at \*2 (S.D. Fla. Dec. 17, 2009) -- finding the attorney client privilege protected certain drafts of letters addressed to the plaintiff where the in-house attorney provided input and recommendations but ordering final versions to be produced.
- Work Product:
  - Developments in the law—would it have been generated anyway? Necessarily focused on whether its something created in the ordinary course of business.
  - Factors identified by courts
    - Preexisting relationship with the vendor
    - Use of the report for business purpose (PR, remediation, etc.)
  - Application to specific contexts—incident response work, forensics reports, etc.
    - Forensic reports—high bar.
      - *Dominion Dental*: preexisting relationship and use of report for PR purposes → no privilege.
      - *In re Capital One*: Significant business purpose where had pre-existing relationship with vendor, report widely distributed,
      - But see *Mass. AG v. Facebook* decision.
- Practical Guidance:
  - Front end considerations
    - Pre-Incident
      - Pre-incident communications most often with in-house counsel.
        - So, what do you tell your business clients based on the state of the law?
          - Don’t just add a lawyer and expect it to be privileged; it is not effective and only adds to costs down the road in litigation
          - Know your role and make it obvious in the communication.
          - May be ambiguity regarding what law applies.
      - Be cognizant of how the advice will be used.

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

- Consider the business implications of potential (or anticipated) disclosure of incident prevention efforts including security scans and table-top exercises.
  - Limit audience
- Post-Incident/Pre-Litigation
  - Consider who hired the IT consultant? Is it the legal department or is it the IT department?
    - Which department is paying the consultant?
    - Should this really matter? [Maybe not, but prepared to explain why it doesn't matter...in an affidavit]
  - Consider the scope of work for any IT consultant:
    - Is the work focused on remediation?
    - Or is it focused on providing technical advice to the attorneys to assist in the provision of legal advice?
  - Consider what facts are discoverable and how the other side can access basic information?
    - Privilege does not protect facts, only legal advice.
      - But it can also protect communications of facts for the purposes of facilitating legal advice
    - Get ahead of the substantial need issue and consider your defense—it will involve access to basic facts.
    - Be prepared to provide underlying forensic images
    - Should a non-privileged timeline be prepared/produced?
- In litigation:
  - Forward-thinking Rule 26 conference and disclosures—be proactive and prepared to discuss ways of front-loading privilege discussions to avoid later disputes or belated productions.
  - Provide training on privilege logs/practical considerations with focus on relevance of the communications and robust quality control efforts
  - Consider the cost of the fight for both sides and ways to streamline the approach.
  - Know the problems with categorical approaches.

## **VII. Updates to the Qualified Cyber-Security Privilege Previously Proposed**

- Overall: We discussed whether updates to Part D of the Commentary, the proposed qualified cybersecurity privilege, are within the scope or purview of a drafting group to consider. According to the charter, the drafting team is to consider: “(1) whether any jurisdiction has adopted the qualified privilege; and (2) whether any update in the case law warrants different discussion or conclusion from first Commentary.”
- The drafting team remains unaware of any jurisdiction that has adopted the qualified privilege proposed in Part D of the Commentary.
- As of now, we have not proposed updates, but will continue to consider whether the case law updates discussed above warrant changes, additions, or edits to Part D if we can achieve consensus on those sections.