Privilege Lessons From Clark Hill Cybersecurity Doc Ruling

By **Doug Meal, Michelle Visser and David Cohen** (January 20, 2021)

Doug Meal

Michelle Visser

David Cohen

The U.S. District Court for the District of Columbia's recent decision in Wengui v. Clark Hill PLC[1] is the latest in a string of cases showing that courts will closely scrutinize claims of attorney-client privilege and work-product protection over documents and communications generated in the wake of a cybersecurity breach.

Even though there are compelling legal reasons to investigate and contain a cybersecurity breach, in Wengui the court rejected claims of attorney-client privilege and work-product protection over a forensic investigation report and related material generated by a cybersecurity firm after a breach because it concluded the information was generated primarily for business reasons.

The decision teaches that companies need to structure their breach investigations and defend motions to compel those materials in a way that makes clear the legal concerns at play as well as how those legal concerns affect the content of the forensic report and related documents.

Background

The privilege dispute arose in a malpractice suit by Chinese dissident Guo Wengui against Clark Hill PLC, the law firm Wengui had hired to represent him in connection with his application for asylum.

According to Wengui's complaint, Clark Hill did not adequately protect his personal information and therefore suffered a cyberattack in which hackers sponsored by the Chinese government broke into Clark Hill's computer network and stole personal information concerning Wengui, including his entire asylum application.

During discovery, Wengui sought, among other things, the forensic report and related materials generated by a cybersecurity firm in connection with its investigation of the security breach. The cybersecurity firm had been retained to conduct its investigation by law firm Musick Peeler & Garrett LLP, which was representing Clark Hill in connection with the attack.

Clark Hill declined to produce the forensic report and related materials as well as to answer related interrogatories, because it contended they were covered by the attorney-client privilege and the work-product protection. Wengui then filed a motion to compel the discovery.

Court's Holdings on Work Product and Privilege

Among other discovery issues addressed in the ruling, the court held that the forensic report and related materials generated by the cybersecurity firm were not subject to either the attorney-client privilege or the work-product protection.

Work Product

As to the work-product protection, the court observed that documents are covered by this doctrine only if generated "in anticipation of litigation," i.e., because of the prospect of litigation. Thus, documents that "would have been created in substantially similar form regardless of the litigation" are not protected.

Seeking to apply that test, the court held that Clark Hill had not met its burden to show that the forensic report or related materials would not have been created in substantially similar form but for the prospect of litigation. The court stated that organizations have a business need to investigate and remediate security breaches.

The court further noted that its in-camera review of the actual report suggested that it was the type of document that would further that type of business need, as the report set forth investigation findings and remediation recommendations, and thus in the court's view "would have been prepared in any event as part of the ordinary course of defendant's business."

Clark Hill argued that it had hired a separate security firm to conduct a business-driven investigation, strengthening its claim that the distinct investigation by the cybersecurity firm whose report was at the center of the privilege dispute was driven by legal rather than business considerations, as the U.S. District Court for the District of Minnesota held in 2015 in sustaining a claim of work product over forensic investigation materials in In re: Target Corp. Customer Data Security Breach Litigation.[2]

However, the court rejected Clark Hill's comparison to Target as factually inaccurate on the ground that the record indicated the cybersecurity firm whose report was at issue was retained to replace the earlier firm, who never completed its initial investigation, rather than to create a second full investigation.

The court also noted that Clark Hill shared the report with members of Clark Hill's leadership and information technology teams, as well as the FBI to assist the FBI's investigation. The court further observed that the declaration submitted by Clark Hill's general counsel stated that the report was used to assist the firm "in connection with managing any issues, including potential litigation, related to the cyber incident," and did not say that litigation was the only use.

The fact that the report was "used for a range of non-litigation purposes," the court said, "reinforces the notion that it cannot be fairly described as prepared in anticipation of litigation."

Attorney-Client Privilege

For similar reasons, the court did not accept Clark Hill's assertion of attorney-client privilege over the report and related information.

Although the court noted that the privilege can apply to the work of consultants when the purpose of that work is to facilitate legal advice, the court concluded based on its discussion of similar issues relating to work product that "Clark Hill's true objective was gleaning" the cybersecurity firm's "expertise in cybersecurity, not in obtaining legal advice from its lawyer."

Implications

There is no doubt that, with many cybersecurity and data breach notification laws on the books and with litigation and regulatory enforcement over cybersecurity breaches ever on the rise, companies that have suffered such breaches have a compelling need for legal advice and, in many instances, to prepare for litigation.

And lawyers, no matter how experienced in cybersecurity, need technical experts to translate the technical facts for them so that they can provide that legal advice and representation. The case for privilege and protection over breach response documents and communications is accordingly compelling, as many cases upholding the privilege or protection in that context demonstrate.

Nevertheless, the Wengui decision is the latest in a string of cases showing that courts will closely scrutinize these privilege and protection claims.

In making these determinations, courts have looked to all evidence put before them relating to the reasons for the investigator's work, including the following:

- Who hired the investigator;
- The timing of the investigator's retention;
- The statement of purpose in the engagement agreement with the investigator;
- The declarations submitted by the company about the nature of and reason for the work;
- Whether there was a separate business-focused investigation, which can reinforce the argument that the investigation under review was for distinct legal reasons;
- Who received the forensic report and how they used it;
- What the company said publicly about the investigation;
- Whether the company designated the work as a legal expense; and
- The content of the actual forensic report and related documents.

Of these factors, the Wengui decision seems to underscore especially that courts will look closely — fairly or unfairly — at the uses to which the company put the forensic report after it was generated in determining why it was generated in the first place. Accordingly, carefully limiting distribution and use of the report can significantly enhance the chances of the privilege and protection being recognized.

And the decision also shows that courts may look closely at the actual report and related materials to understand the nature of the work and whether it seems to be oriented toward assisting lawyers, underscoring the need to be mindful of whether those documents demonstrate the purpose for which they were generated.

Finally, the decision is vulnerable to criticism for recognizing a business need to investigate and remediate security breaches but ignoring that companies also routinely can and do face legal claims for allegedly inadequate security practices and breach response, as in the Wengui case itself, and thus have a compelling legal need for legal advice and reduction of

litigation exposure with the help of forensic investigators.

The court's hesitance to recognize the compelling legal reasons for forensic work underscores that companies need to structure their breach investigations and defend motions to compel in a way that makes clear the legal concerns at play as well as how those legal concerns affect the content of the forensic report and related materials.

Doug Meal is a partner and head of the cyber and privacy litigation and enforcement practice at Orrick Herrington & Sutcliffe LLP.

Michelle Visser is a partner at Orrick.

David Cohen is of counsel at the firm.

[1] Wengui v. Clark Hill PLC, No. 19-3195 (D.D.C. Jan. 12, 2021).

[2] In re: Target Corp. Customer Data Security Breach Litigation, 2015 WL 6777384 (D. Minn. Oct. 23, 2015).