

Email Containing Legal Advice Remained Privileged after Being Found on Employee's Work Laptop

16 June 2023

Key Takeaways.

- The judgment in *Taylor v Evans* [2023] EWHC 935 (KB) is a useful reminder of the factors underpinning legal advice privilege, in particular the test being whether the recipient ought reasonably to understand that a document or information was communicated in confidence.
- The case reiterates that even where documents are obtained outside legal proceedings, the legal tests for privilege are the same.
- It is apparent that the Court will consider a wide range of factors and the circumstances in which a document came into the possession of an opponent in legal proceedings in deciding whether privilege has been waived.
- Although in this case privilege was maintained, companies and employers should exercise caution in deploying IT systems that allow employees to access personal email on work devices, particularly since personal documents accessed or stored on an employer's IT system may not always be considered confidential against their employer.

Introduction. In *Taylor v Evans* [2023] EWHC 935 (KB) the High Court considered whether privilege is lost where a litigant received an email (containing legal advice) from their opponent, outside of the legal proceedings. The central question upon which the case turned was whether the information remained confidential as against the recipient, in which case there was no loss of privilege. And that question in turn depended on whether a reasonable person in the position of the recipient would understand that the information was communicated in confidence. In the circumstances the Court held that it should have been apparent to the recipient that the information in the email was confidential, and therefore privilege was not lost.

The Facts. Multiple Claimants sued the Labour Party for publishing a report in respect of the Labour Party's governance and legal unit in relation to antisemitism in the period

2014-2019 (the “Report”). The Claimants alleged breach of their rights under the General Data Protection Regulation, misuse of their private information, breach of confidence, and unlawful discrimination (under the Equality Act 2010). The Defendant said that the Report was leaked by third parties, and lodged a counterclaim by the Defendant against the third parties.

The Defendant asked the Court for a declaration that an email (the “Email”) sent by one of the third parties to her lawyer (just before publication of the Report) was not privileged.

In connection with the Defendant’s investigation into the Report and its release, it asked employees to turn over their work laptops for forensic examination. Before surrendering her laptop, one such employee, Ms M, explained to the Defendant that she had removed all personal data required. In addition, the Defendant’s IT staff told her that the emails in her iCloud account would not be accessible during the course of the investigation. It was apparent that she thought this was the case.

However, in reality, the IT department had only uninstalled Ms M’s iCloud account which (contrary to what they expected) did not disconnect it from Ms M’s Outlook email account, so in fact her personal emails could be accessed. This was how the Email came into the hands of the Defendant.

In Court, Ms M submitted that any reasonable person in the position of the Defendant would realise that the circumstances in which they received the Email gave rise to a duty of confidence. She submitted that even assuming the iCloud account was her employer’s account, this did not permit the Defendant to use the Email against her. On this point she relied on *Jinxin Inc v Aser Media Pte Ltd* [2022] EWHC 2856 (Comm). In that case the court considered the realism of expecting a complete segregation between work and personal information in IT systems, stating: “*In a perfect world, no doubt, all the information on corporate servers would be confidential to the corporation alone, and it would only be the corporation’s confidentiality that employees would be obliged to protect. But the mere fact that they had access for proper purposes does not establish that the real world was perfect in that respect. An executive [...] might reasonably assume that their personal confidentiality would be equally protected by the duty of the corporation’s employees.*”

The Defendant relied on *Simpkin v The Berkeley Group Holdings plc* [2017] EWHC 1472 (QB). In that case it was held that an employee’s documents were not privileged against his previous employer because there was no reasonable expectation of privacy in connection with material stored on the employer’s IT system. This was particularly evident where they were neither separated from work files, nor password protected.

Ms M had sent the Email from her iCloud account, and not from the Defendant's email system. She had also used the iCloud account to send sensitive work emails. She synced her iCloud account with her Outlook account on her laptop. Nevertheless, the Defendant submitted that the facts were sufficiently similar to *Simpkin* so that the Court should find her Email was no longer privileged.

The Judgment. Chamberlain J held that the Email remained privileged even though it had come into the hands of the Defendant, in the way it had – and outside of the legal proceedings.

The question of whether confidentiality, and with it privilege, was lost depended on whether any reasonable person in the position of the recipient of the information would have understood that the information was being provided in confidence. Answering this question required close attention to the circumstances in which, in this case, the Email was received.

In arriving at an answer to the question Chamberlain J considered the key circumstances in this case to be:

- The Email was headed “LEGALLY PRIVILEGED” and it was clear on its face it was a request for legal advice.
- The location of the email in a laptop belonging to the Defendant did not imply that it had lost its confidentiality for all purposes.
- In addition, it was evident that the Defendant was aware the laptop might contain personal information.
- The email correspondence of the IT team demonstrated that they realised Ms M's attempts to remove personal information had not been completely effective.
- Since Ms M mistakenly thought that her personal information was removed from her laptop, the fact that she did not request any constraints on the Defendant's searches of her laptop was not material.

Considering the circumstances in which the Defendant came to possess the Email, the Court decided that it remained confidential as against the Defendant. The Defendant should have realised that it was confidential. Therefore, Ms M was within her rights to rely upon the Email still being privileged.

* * *

Please do not hesitate to contact us with any questions.

LONDON



Christopher Boyne
cboyne@debevoise.com



Julia Caldwell
jcaldwel@debevoise.com



Scott Morrison
smorrison@debevoise.com