

[HOME \(/\)](#)

[MENU](#)

Protecting Privilege in ‘Work From Anywhere’ Era

The move toward remote or hybrid work arrangements is underway and irreversible

by Erik Christenson and Jason Ayer Graham
November 17, 2021



[\(https://taxexecutive.org/protecting-](https://taxexecutive.org/protecting-privilege-in-work-from-anywhere-era/)

[privilege-in-work-from-anywhere-era/\)](https://taxexecutive.org/protecting-privilege-in-work-from-anywhere-era/)

Even prior to the COVID-19 pandemic, tax functions were adapting and reacting to fundamental change and uncertainty. Whether the changes were brought about by the Tax Cuts and Jobs Act, by ever more aggressive positions taken by state and local auditors, by complex and burdensome reporting regimes, by novel taxes or levies, or by the unprecedented international cooperation in global tax policy and rulemaking, to name just a few, tax departments were forced to quickly develop new compliance processes and new planning solutions. And these processes and solutions involved the use of newly developed tools and systems to model and measure results under recent legislation.

Against this backdrop of fundamental change and uncertainty in tax policy and administration, the way we work has forever changed in response to the COVID pandemic. The move toward remote or hybrid work arrangements is underway and irreversible. Technology, of course, has risen to the challenge by creating new tools for communication, collaboration, and information sharing.

Those two currents of disruptive change exist independent of each other, but they also intersect, requiring the modern tax department to focus on both substance and process. That is, the modern tax department has to ensure not only that its interpretation of the vast array of new tax rules is technically and substantively correct and defensible, but also that its use of new tools for communication, document sharing, and collaboration does not cause unintended consequences like, for example, waiving privilege or creating other unforeseen issues at the audit stage.

Complicating matters even further, the subjective intent behind tax planning plays a bigger role than ever before. The new generation of tax rules routinely includes intent-based “anti-abuse” rules or “principal purpose” tests that can negate the taxpayer’s affirmative position.¹ Some varieties of these rules provide the tax authority with tremendous discretion to invent a transaction that the taxpayer hypothetically *could have* engaged in and to assess tax on that basis.² Needless to say, this environment makes discovery an extremely potent weapon for the taxing authority and legal privilege the taxpayer’s first and most important line of defense.

Simply put, in tax planning, process matters. Subjective intent matters. Protocols matter. When a taxpayer is called upon to defend the tax position that results from a planning project, in many circumstances the manner in which planning was carried out and communicated could be more consequential than whether the technical position can be supported and defended.

Practical Steps to Protect Privilege in Digital Environment

With limited exceptions, attorneys have a responsibility to keep client information confidential.³ Beyond that, the attorney-client privilege operates to protect communications between a lawyer and client from disclosure to a court or other party. In general, the attorney-client privilege applies to (1) a communication (2) made between attorney and client (3) in confidence (4) for the purpose of seeking, obtaining, or providing legal assistance to the client.⁴ The third element, that the communication be made in confidence, is not absolute. That is, the privilege may not be waived if any disclosure of the communication was inadvertent and the holder of the privilege took reasonable steps to prevent disclosure and, afterward, to rectify the error.⁵

While taxpayers (and, on their behalf, their attorneys) need not be constantly on the watch for hidden eavesdroppers, a choice to hold discussions in public where they could be easily overheard demonstrates a lack of concern for confidentiality and likely would not be considered a reasonable approach to prevent disclosure.

In this era in which the working world is moving toward a virtual environment, one might think that taxpayers and lawyers do not need to worry as much about being in public with prying ears. However, because the untethering of work from a physical office opens up the possibility of working from anywhere, the virtual environment can actually exacerbate concerns about being overheard. Conducting a conference call at the beach may be relaxing but may also pose increased risks to the confidentiality of communications. And even in the safety of their own homes, it is easy for clients and attorneys to fall victim to complacency, forgetting that parents, spouses, significant others, and even children do not fall within the scope of the attorney-client privilege. If those persons hear otherwise privileged communications, that may cause the privilege to be waived. Taxpayers and their advisors should take care to avoid these situations.

In addition, it is now necessary to consider safeguards relating to the changing aspects of virtual work, including collaborative document editing, cloud-based file storage, and virtual meetings. As document sharing and collaboration platforms become the norm for writing and editing all types of legal documents, lawyers and clients must ensure that their processes and technology maintain confidentiality of communications.⁶ When taxpayers and their lawyers use technology to collaborate on a document in real time, for example, this process can include the delivery of information that the client intends to keep confidential and that is being provided in connection with the lawyer's provision of legal advice, thus satisfying three of the four factors for privilege protection. Still, to maintain privilege, such communications must also be confidential. Accordingly, access to such editing must be limited to protect such confidentiality. *Harleysville Ins. Co. v. Holding Funeral Home* provides a cautionary tale.⁷ In that case, a Virginia federal district court considered whether the plaintiff's use of an internet-based electronic file-sharing service operated by Box Inc. waived the attorney-client privilege. Specifically, an employee of the plaintiff's parent company used the same Box site to share certain documents with third parties and, separately, other documents with plaintiff's counsel. The Box site was not password-protected and was accessible to anyone who clicked on the relevant link, or who typed the URL address into a browser; as a result, the defendants were able to access the documents. The court therefore found that no precautions were taken to prevent disclosure and that the plaintiff waived any claim of privilege over the documents that it had loaded onto the Box site. Even basic precautions to limit access to file-sharing sites would likely avoid this result, and taxpayers should implement them, including password-protection and separately accessible folders or sites for third parties and attorneys. Another good practice is to mark any collaboratively edited documents as drafts until the editing is complete and the document is finalized in order to avoid the later accidental disclosure of a document that was downloaded mid-editing but lacked obvious indications to that effect.

Virtual meetings conducted with audio and video represent another source of confidentiality concerns. Beyond any issues arising from the terms of the technology itself, as addressed above, virtual meeting service providers generally provide the option to create records of the meeting with more detail than was previously possible. For example, some providers allow users to capture audio, full transcripts, and video from multiple possible perspectives, including screen-shares made during the meeting. This means that unlike face-to-face meetings, which have been typically memorialized by nothing beyond notes or, at most, an approximate transcript, virtual meetings can capture and record the exact words said as well as the accompanying or reactive facial expressions. Unless covered by privilege (or another exception), these records are generally discoverable and can provide substantial fodder for a tax authority seeking to support an adjustment. For this reason, taxpayers and attorneys should take appropriate steps to maintain privilege. This means being aware of, and approving, all participants to ensure that all fall within the sphere of attorney-client privilege. (See discussion below regarding *Kovel* arrangements, intended to extend privilege to communications with non-attorneys.) Practically, this can include limiting invitation lists, matching up phone numbers and names to the invitation list, and taking reasonable steps to prevent improper disclosure during calls that involve parties outside the attorney-client sphere. In addition, while it is a taxpayer's prerogative to record even privileged meetings, they should put into place safeguards against disclosure to third parties that would break privilege. Further, if such meetings are recorded, all parties should take care not to share potentially sensitive information that may be in the background of their computer screens when screen-sharing. The same concerns apply to other methods of communication that now create records when they didn't previously, such as text-based communication like instant messaging or texts that replace the quick chats or phone calls of old.

In addition to the issues faced by taxpayers in US audits and investigations, the global tax climate is also shifting, with increased aggressiveness from tax authorities around the world. In this context, the multi-jurisdictional use of the types of platforms described above can create added challenges. Even if platform-shared documents are subject to privilege in the United States, those same documents, even when shared with the exact same group of people, may not be privileged vis-à-vis tax or other authorities in foreign countries. For example, the UK corollary to the attorney-client privilege has a much more restrictive definition of the "client" in a company context, limited only to the set of employees who are authorized to instruct the lawyers, and to seek and receive legal advice from them, so that documents shared with other employees will generally fall outside the scope of the privilege in the United Kingdom.⁸ Accordingly, taxpayers and their advisors should assess the protections afforded in a particular country before granting access to employees subject to that country's jurisdiction.

Around the globe, tax authorities have also struggled to keep up with the new way of working. Some tax authorities have reacted more or less by suspending all ongoing audits, but others have continued audits while attempting, often unsuccessfully, to adapt to tools like videoconference platforms. As a result, some tax authorities have switched models, so that instead of discussing an issue with the taxpayer, they simply request a large volume of written information and then reach a position on that basis, even if that position is based on a misunderstanding of the information provided due to a lack of appropriate background, which would have been provided by the taxpayer if the inspector had engaged in discussions. In these cases, taxpayers and advisors face an uphill climb to explain the reality of the case and persuade the inspectors to reconsider their positions, especially if they have already set collection expectations in internal communication. If a taxpayer must deal with a tax authority that has adopted a similar approach, it is essential to provide adequate background when the information is submitted, including by anticipating upfront potential issues that would otherwise be discussed in traditional face-to-face meetings.

Adapting *Kovel* Arrangements in the Age of Collaboration

Complex and multi-jurisdictional planning projects often involve attorneys and non-attorneys working together. In certain circumstances, a client's lawyer can directly engage non-attorney service providers under a *Kovel*⁹ arrangement which operates to extend privilege to the work and communications with non-attorney service providers. These service providers can be engaged on a variety of issues like whether to get local or

subject matter expertise on accounting rules or modeling and computations, to agree on a technical position, or to handle different aspects of implementation on schedule. In such an environment, where much of the communication with a client might not involve an attorney, a *Kovel* arrangement can be a helpful way to protect privilege.

Best practices for *Kovel* arrangements should always be a part of any *Kovel* arrangement to protect privilege. These policies and practices take many forms based on each project, but, in general, they should include procedures, among many, that 1) make clear that the lawyer is the “client” in the *Kovel* arrangement with the non-attorney, and 2) ensure that specific engagement letters and billing procedures are in place, and, 3) as may be needed in the case of preexisting accounting relationships, best insulate the *Kovel* team from, for example, the audit team at the same accounting firm whose services are not under the *Kovel* arrangement.

But how should these best practices be adapted in a world of collaboration platforms and digital information sharing? Each scenario, like any *Kovel* arrangement, will depend on the actual substance of each representation, so while it may be difficult to create bright-line procedures, clients should still consider the extension of privilege in *Kovel* arrangements with care. Just as the practice of protecting privilege is changing, as specified above, parties extending that privilege to non-attorneys in a *Kovel* arrangement should take similar precautions. Practically speaking, this could include limiting the access any non-attorneys have to a collaboration site just to the scope of their hired work and not the entire project. In essence, this could mean creating designated *Kovel* privilege zones on the site. Additionally, the types of rights granted to people on the site could be limited based on their ability to view, edit, or download documents from the site. Such limitations might not be possible in some projects, for example, where the non-attorneys are being asked to assist attorneys throughout the project. These circumstances might justify more expansive access to information on the site. In these situations, attorneys should take care to consider which documents specifically should be considered privileged and mark them accordingly. The excessive designation of documents as privileged, even ones that are not actually privileged or intended to be privileged, may reduce the protection over documents and communications that do merit such protection.

Additionally, just as with conference calls and video calls, the persons granted access should be closely monitored and limited in scope. However, the use of collaboration platforms should be added to the same group of interactions and communications as prior *Kovel* arrangements. Although the use of these sites was growing even before COVID, it seems they are moving rapidly into the new norm for everyday interactions with clients and lawyers.

Tax Raids

Before the pandemic, tax authorities had increasingly utilized a “tax raid” or an unannounced visit and inspection of the office or premises of a company with a judicial warrant to obtain information or documents for an audit. While, in our experience, there has been a slowdown in tax raids during the pandemic, it is anticipated that these tactics could be on the rise again as and when the pandemic comes to its end. The underlying warrant may authorize seizure of not only documents but also electronic information including emails, documents, notes, etc. More important, this can include any documents that an employee has access to or the ability to download from a collaboration site. In general, the handling of raids has been covered in other scenarios,¹⁰ but the rise of virtual working and collaboration platforms brings a new possibility of home raids. For example, previously it was possible, though very rare, that the target of a tax audit raid might be the personal residence of an officer of a company, most often in connection with preexisting concerns related to permanent establishment. However, with large groups of employees now working from home, and in some cases in countries other than their office site, the risks associated with raids can extend across borders. For example, because raiding the company’s servers is the “preferred” option, companies should review their security and accessibility policies and should be conscious of all the information that has been made remotely accessible for employees located in jurisdictions where a raid is a possibility. Without any protection, a document could be accessible from the device that a tax authority has authorization to raid, with the result that the tax authority can seize that document regardless of whether it is stored locally or abroad. Furthermore, even if that document was prepared by US counsel with the expectation of US privilege, for example, the privilege rules in the seizing jurisdiction, rather than those of the jurisdiction where the document is stored, would apply. Therefore, in a world with growing remote work, policies about access to information and the ability to download or otherwise access information need to be considered.

Conclusion

The normal progress of digitization, accelerated by the change brought by the pandemic, has fundamentally changed the way we work. Tax departments and tax authorities are learning how to deal with this new environment, raising the importance of a carefully considered approach to legal privilege in the tax function. Remote or hybrid work arrangements and collaboration platforms are here to stay. Tax departments must now consider how best to protect their communications in the digital world.

Erik Christenson and **Jason Ayer Graham** are partners, tax, at Baker McKenzie LLP.

Endnotes

1. 951A(d)(4)(B), 7701(o), 269(a), 357(b), Treas. Reg. 1.304-4, Treas. Reg. 1.305-5(b)(2)(ii)(B), Treas. Reg. 1.367(a)-3(d)(2)(vi)(d), 1248(a), 894(c), 881, and OECD Action Item 6 and Article 29(9) of the OECD Model, Article 7(1) of MLI. Further, states employ the related but distinct concepts of economic substance, sham transaction, and business purposes. *Sherwin-Williams Co. v. Commissioner of Revenue*, 438 Mass. 71, 778 NE2d 504 (2002) applies all three tests and also notes “[b]ecause the record in this case establishes that the reorganization and subsequent transfer and licensing transactions were genuine, creating viable businesses engaged in substantive economic activities apart from the creation of tax benefits for Sherwin-Williams, they cannot be disregarded by the commissioner as a sham regardless of their tax-motivated purpose.” This most often comes up in the state tax context when a taxpayer wants to deduct otherwise deductible payments made to a related party. Mass. Gen. Laws Ann. ch. 63, Section 31J(b)(i) (Westlaw 2015) requires that taxpayers add back interest expense paid to a related party unless the taxpayer establishes by clear and convincing evidence that the disallowance is unreasonable or that a principal purpose of the transaction was not to avoid payment of taxes; a similar requirement appears in NJ Stat. Ann. Section 54:10A-4(k)(2)(l) (Westlaw 2015).
2. These provisions include but are not limited to the Australian MAAL (Tax Laws Amendment (Combating Multinational Tax Avoidance) Act 2015 (Cth)), the Australian Diverted Profits Tax Treasury Laws Amendment (Combating Multinational Tax Avoidance) Act 2017 (Cth), and the UK Diverted Profits Tax (Finance Act 2015, ss 77–116 and Sch 16 and INTM489590). Also see Section 33 of the Income Tax Act for Singapore’s version of GAAR and Section 33(7) specifically where intent can be used as a defense by the taxpayer to show bona fide commercial purpose of the

transaction and that one of its main purposes was not to avoid or reduce tax. Further, Canada's GAAR legislation in Section 245(2) of the Income Tax Act can apply in the case of an "avoidance transaction," and an "avoidance transaction" is widely considered to examine the subjective motives of the taxpayer when assessing whether that taxpayer engaged in the transaction for "bona fide purposes other than to obtain the tax benefit." Ironically, today's tax planning is often defensive, focused on eliminating uncertainty and the potential for double taxation. Even so, it is not inconceivable that a taxing authority would point to such "defensive planning" as evidence of a subjective intent to achieve a tax benefit, that is, certainty.

3. See, for example, ABA Model Rule 1.6.
4. Restatement of the Law Governing Lawyers Section 118 (Tentative Draft No. 1, 1988).
5. See Fed. R. Evid. 503 (for waiver in federal proceedings or to a federal office or agency).
6. More generally, beyond their own processes, taxpayers and their lawyers must also consider whether the terms of the technology used for such collaboration or even for storing documents pose a risk to the maintenance of privilege in and of themselves. The New York State Bar has concluded, for instance, that while using email services that use artificial intelligence to scan the contents of email for the purpose of generating personalized advertisements is consistent with a lawyer's duty of confidentiality, lawyers nonetheless "must exercise due care in selecting an e-mail service provider to ensure that its policies and stated practices protect client confidentiality" (NYSBA Opinion 820 [2008]). Similarly, it ruled that law firms can provide attorneys with remote access to client files, but should ensure that "the particular technology used provides reasonable protection to client confidential information" (NYSBA Opinion 1019 [2014]). Similarly, if a taxpayer does not take reasonable steps to avoid using technology that shares its confidential information with third parties, it could be considered to have waived privilege.
7. *Harleysville Ins. Co. v. Holding Funeral Home*, 2017 US Dist. LEXIS 18714 (W.D. Va.).
8. *Three Rivers District Council v. Bank of England* (No. 5) [2003] EWHC 2565.
9. See *United States v. Kovel*, 296 F.2d 918 (2d Cir. 1961). Additionally, for state and local tax purposes, although *Kovel* is an interpretation of the attorney-client privilege by a federal court, it is generally understood to apply at the state level. See *Comm'r v. Comcast*, 901 NE.2d 1185 (Mass. 2009), which applies a detailed *Kovel* analysis, and *Mich. v. Paasche*, NW.2d 914 (Mich. App. 1994), which applies the *Kovel* doctrine.
10. For further background, please see Baker McKenzie's work on raids pre-COVID: "Handling Tax Disputes in Europe" (2020), "Handling Tax Disputes in Asia Pacific" (2020); "Handling Tax Controversies in Latin America" (2020), <https://taxshare.bakermckenzie.com/global-tax-share> (<https://taxshare.bakermckenzie.com/global-tax-share>); "Dawn Raids: Dealing With Inspections by Competition Authorities in the UK" (2020), www.ashurst.com/en/news-and-insights/legal-updates/quickguide---dawn-raids-dealing-with-inspections-by-competition-authorities-in-the-uk/ (<http://www.ashurst.com/en/news-and-insights/legal-updates/quickguide---dawn-raids-dealing-with-inspections-by-competition-authorities-in-the-uk/>); "Are You Prepared for a Dawn Raid?" (2019), www.bakermckenzie.com/en/insight/publications/2018/01/dawn-raid; and "Investigative Powers in Practice: Summaries of Contributions" (2018), [https://one.oecd.org/document/DAF/COMP/GF/WD/\(2018\)42/en/pdf](https://one.oecd.org/document/DAF/COMP/GF/WD/(2018)42/en/pdf) ([https://one.oecd.org/document/DAF/COMP/GF/WD/\(2018\)42/en/pdf](https://one.oecd.org/document/DAF/COMP/GF/WD/(2018)42/en/pdf)).

Leave a Reply

Your email address will not be published. Required fields are marked *

Your Comment here...

Name (required)

Your Name*

Email (required)

Your E-Mail*

Website

URL

Save my name, email, and website in this browser for the next time I comment.

Submit

Subscribe
Now! >>



([https://eweb.tei.org/eweb/DynamicPage.aspx?Site=TEIWeb&WebKey=1f125a35-ed08-4e01-](https://eweb.tei.org/eweb/DynamicPage.aspx?Site=TEIWeb&WebKey=1f125a35-ed08-4e01-b99c-3320cb7f6d12)

b99c-3320cb7f6d12)

TRENDING ARTICLES

New Developments in Canada's General Anti-Avoidance Rule

(<https://taxexecutive.org/new-developments-in-canadas-general-anti-avoidance-rule/>) Editor's note. This article was written in early May. In...

Oops! I Did It Again: Practical Implications of Revenue Procedure 2022-39

(<https://taxexecutive.org/oops-i-did-it-again-practical-implications-of-revenue-procedure-2022-39/>) A fact, well known in the tax community: every tax...

TEI Roundtable No. 43: Separate, Combined, and Worldwide Unitary State Filings

(<https://taxexecutive.org/tei-roundtable-no-43-separate-combined-and-worldwide-unitary-state-filings/>) One of the most talked-about education sessions at this year's...

Buying and Selling CFCs Under New Corporate Alternative Minimum Tax Regime

(<https://taxexecutive.org/buying-and-selling-cfcs-under-new-corporate-alternative-minimum-tax-regime/>) As part of the Inflation Reduction Act, Congress enacted a...

Tax Data Takes Center Stage

(<https://taxexecutive.org/tax-data-takes-center-stage/>) As TEI members know all too well, when it comes...

AI, ETL Tools Offer Promising Possibilities

(<https://taxexecutive.org/ai-etl-tools-offer-promising-possibilities/>) Artificial intelligence (AI) and extract, transfer, and load (ETL) tools...



www.tei.org (<http://www.tei.org>) | ©2023 Tax Executives Institute, Inc. All Rights Reserved | [Advertise](https://taxexecutive.org/wp-content/uploads/2022/12/TEI_TaxExecutiveRate-card-2023v3_12.9.22.pdf) (https://taxexecutive.org/wp-content/uploads/2022/12/TEI_TaxExecutiveRate-card-2023v3_12.9.22.pdf)



(https://twitter.com/TEI_Updates)



(<https://www.linkedin.com/company/tax-executives-institute>)