

Reproduced with permission from White Collar Crime Report, 13 WCR 221, 03/16/2018. Copyright © 2018 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

ATTORNEY-CLIENT PRIVILEGE

In an update to an earlier article published in November 2017 with Bloomberg Law, two Seyfarth Shaw LLP attorneys discuss the new 2018 U.S. Customs & Border Protection directive on border searches and how it could potentially impact attorneys' ethical obligations to safeguard client confidences when lawyers travel abroad for work.

More Guidance Please: CBP Issues New 2018 Directive Providing Greater Protection for Privileged Materials During Border Crossings

BY ANDREW S. BOUTROS AND JOHN R.
SCHLEPPENBACH

In late 2017, we wrote for Bloomberg Law about the recent increase in the number of border searches of electronic devices by U.S. Customs & Border Protection (CBP) and the ethical concerns it raised for attorneys, who are obligated to safeguard their clients' confidences. We were not alone in seeing risks for attorneys in CBP's policies; the American Bar Association (ABA) and other organizations publicly called for greater sensitivity to confidentiality and privilege issues during border crossings. In a positive development to start the new year, CBP appears to have heeded those concerns and has issued a new 2018 directive on inbound and outbound U.S. border searches that provides greater protection for client confidences. But notwithstanding this favorable development, attorneys traveling abroad must still remain vigilant as they cross U.S. and international borders.

Ethical Obligations

As a quick reminder, Rule 1.6(c) of the widely-adopted ABA Model Rules of Professional Conduct provides that "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Comment 18 to this Rule lists factors to be considered in determining reasonableness, including:

- (1) the sensitivity of the information;
- (2) the likelihood of disclosure if additional safeguards are not employed;
- (3) the cost of employing additional safeguards;
- (4) the difficulty of implementing the safeguards; and
- (5) the extent to which the safeguards adversely affect the lawyer's ability to represent clients, for instance by making an electronic device excessively difficult to use.

Further, Rule 1.6(b)(6) permits an attorney to reveal information relating to the representation of a client to the extent that he reasonably believes it is necessary "to comply with other law or a court order." Comment 15 to this Rule, however, makes clear that revealing such information cannot be considered necessary until the lawyer has "assert[ed] . . . all non-frivolous claims" against its disclosure and contemplated any available avenues for appeal.

In the widely-discussed Formal Ethics Opinion 2017-5, the Association of the Bar of the City of New York Committee on Professional Ethics construed the

local versions of these rules and concluded that attorneys have an obligation—before they cross any borders—to assess the risk that client information will be breached, the potential harms that could result, and any safeguards that could be implemented. Because any disclosure of client information is presumptively harmful under the ethical rules, the Opinion suggested that attorneys consider not taking confidential client information across the border at all, such as by carrying blank “burner” phones or laptops or using software designed to securely delete information. Where confidential information is carried and disclosure is requested, however, the Opinion concluded that attorneys must take reasonable steps to avoid disclosure, such as by requesting that materials not be searched or copied or asking to speak to a supervisor. Importantly, the Opinion determined that reasonableness does not require attorneys to refuse searches of their devices to the point that they are denied border entry or taken into custody. Finally, the Opinion stated that attorneys have an obligation to promptly notify clients impacted by any disclosures that are made at the border so that clients can determine whether they should file a legal challenge.

The Revised CBP Guidance

Limited Searches Allowed Without Reasonable Suspicion and No Access to Remotely-Stored Information

On Jan. 4, 2018, CBP issued Directive 3340-049A, which provides revised guidance on the topic of inbound and outbound border searches of electronic devices and responds to attorney-client confidentiality concerns in several important respects. Perhaps most importantly, the Directive makes clear the narrow scope of the searches permitted without reasonable suspicion of unlawful activity or a national security concern. Any “advanced searches,” which are defined as those “in which an Officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents,” are barred absent reasonable suspicion.

Critically, the Directive clarifies that border searches may not include using portable electronic devices to access *remotely-stored information*:

The border search will include an examination of only the information that is resident upon the device and accessible through the device’s operating system or through other software, tools, or applications. Officers may not intentionally use the device to access information that is solely stored remotely. To avoid retrieving or accessing information stored remotely and not otherwise present on the device, Officers will either request that the traveler disable connectivity to any network (e.g., by placing the device in airplane mode), or, where warranted by national security, law enforcement, officer safety, or other operational considerations, Officers will themselves disable network connectivity.

The Directive also states that “[o]fficers should also take care to ensure, throughout the course of a border search, that they do not take actions that would make any changes to the contents of the device.”

Heightened Protections for Attorney-Client Privileged Materials

In addition, the Directive provides enhanced procedural safeguards specific to potentially attorney-client privileged materials. It requires officers to consult the relevant CBP Associate/Assistant Chief Counsel’s Office before searching any device as to which a claim of privilege is raised, and to “seek clarification, if practicable in writing, from the individual asserting this privilege as to specific files, file types, folders, categories of files, attorney or client names, email addresses, phone numbers, or other particulars that may assist CBP in identifying privileged information.” Armed with this information, CBP will “ensure the segregation of any privileged material from other information examined during a border search” and the destruction of any copies thereof following the search.

Practical Guidance and Tips

CBP’s Directive is a positive step toward alleviating attorneys’ concerns about safeguarding client confidences during U.S. border crossings, but it is not a substitute for attorneys’ own duties to be careful stewards of that information. The restrictions on the scope of searches in the Directive, for instance, will be of little use if attorneys are not vigilant in making sure they are followed. So, step one for any lawyer crossing the U.S. border is to understand (and remember) the existence and contours of CBP’s latest Directive.

In addition, lawyers must make sure that CBP agents do not use their electronic devices to access remotely-stored information or make copies of information absent reasonable suspicion. This can be as simple as making sure that “airplane mode” is turned on. Similarly, the Directive’s establishment of a protocol for involving the applicable CBP Associate/Assistant Chief Counsel’s Office to help segregate potentially privileged materials is helpful only if attorneys remember to invoke it. Lawyers must still take steps to prove their identities and the existence of the privilege, such as by carrying bar-issued identification cards and being prepared to provide details of those files that should not be searched. And, one constant still remains: Lawyers should never hesitate to ask to speak to a supervisor.

Another important takeaway from CBP’s Directive is the benefit of storing client information remotely, as opposed to locally on a portable electronic device. Because CBP has made clear that remotely-stored information should not be accessed during border searches, attorneys can avoid concerns about disclosing client confidences by uploading needed content to web-based services and carrying “burner” devices that store little or no client information locally. When confidential electronic materials must be carried across borders, they should be clearly identified as privileged (such as with legends asserting the privilege) and if possible, segregated from non-privileged materials. And, attorneys should also have a fully-charged cell phone handy when going through border security so that colleagues can be consulted as needed.

And, of course, careful preparation for border crossings remains key, even under CBP’s revised guidance. Attorneys should continue to carefully evaluate the pros and cons of international travel and in doing so, should consider whether telephone or video conferencing

could achieve the same goals. Where travel is unavoidable, the possibility of search and seizure of attorney-client privileged materials in every country to be visited should be considered and relevant legal materials addressing the issue should be accessible. This is critical because whatever CBP's guidance, other countries may not be as sensitive to the attorney-client privilege and may be unwilling to exercise some of the same restraints as those set out by CBP's latest Directive.

By taking these and other similar steps, attorneys can ensure that they have taken reasonable steps to safeguard their clients' confidences and discharge their own ethical obligations.

Conclusion

CBP's new Directive shows that the agency is sensitive to attorney concerns about protecting client confidences during border searches and is taking positive steps to address them. By clarifying the limits of permissible searches absent reasonable suspicion and stepping up the role of CBP's Associate/Assistant Chief Counsel's Offices in dealing with potentially attorney-client privileged materials, the agency has given attorneys helpful tools to protect their clients and discharge their ethical obligations. These tools are no substitutes for thoughtful preparation, however, and attorneys who travel internationally must continue to take steps to limit the confidential information they carry and invoke the appropriate rights and procedures when the information they must carry is subjected to a border search request—whether in the United States or abroad.

Author Information

Andrew S. Boutros is the National Co-Chair of Seyfarth Shaw LLP's White Collar, Internal Investiga-

tions and False Claims Team and Lecturer in Law at The University of Chicago Law School. A former Assistant U.S. Attorney in Chicago, his investigations and prosecutions spanned the globe and are regarded as among the most extensive and complex multi-district, international corporate fraud and cybercrime cases in the nation's history. In total, Boutros coordinated efforts with international law enforcement authorities in more than 20 countries and charged and prosecuted crimes involving some \$500 million in losses, proceeds, and judgments, while also investigating additional criminal conduct in the several billions of dollars. Boutros represents clients in their most sensitive and important white collar matters, internal and cross-border investigations, including under the Foreign Corrupt Practices Act, and complex litigations. He also provides strategic counseling and advice to clients in a variety of industries and across subject matters, including in the design and implementation of various compliance programs.

John R. Schleppenbach is Counsel in the Litigation Department of Seyfarth Shaw's Chicago office. He is a member of the White Collar, Internal Investigations, and False Claims Team, and has experience representing major corporations in all manner of international internal investigations and litigated matters, including cases involving the Foreign Corrupt Practices Act and the Convention for the International Sale of Goods. A former appellate prosecutor, Schleppenbach has also published more than three dozen articles on emerging issues in litigation and currently serves as the coach to the international arbitration moot court team at Northwestern Pritzker School of Law.