MORRISON | FOERSTER

Morrison & Foerster LLP
Registered Associated Offices of
Ito & Mitomi

Tokyo Privacy + Data Security Client Alert

March 2017 2017 年 03 月

United States

Can Border Agents Search Your Phone?

By *Miriam Wugmeister, J. Alexander Lawrence, and Rhiannon Batchelder*

Miriam Wugmeister, a partner at Morrison & Foerster LLP's New York City office, is a member of the firm's Global Privacy and Data Security practice.

J. Alexander Lawrence is a partner at Morrison & Foerster in New York and co-chair of its E-Discovery Task Force.

Rhiannon Batchelder is a litigation associate at Morrison Foerster in New York.

There have been numerous reports from individuals entering the U.S. of border agents searching their phones and laptop computers. Many of those individuals are U.S. citizens. Although these events have been in the news recently and appear to be on the rise, this practice is not new. According to CNN, quoting a U.S. customs agency spokesman, border agents searched 4,444 cellphones and 320 other electronic devices in 2015. In 2016, searches of electronic devices at the U.S. borders rose to 23,877, according to the same source. In countries such as China and Russia, border agents have been searching phones and laptops for years, and many companies have developed policies to provide guidance to employees traveling to those countries. Companies are now struggling with how to advise and craft policies for employees traveling to and from the U.S. with electronic devices that may contain sensitive data.

Border Searches: The Constitutional Framework

Courts have held that, under U.S. law, Customs and Border Patrol (CBP) and Immigration and Customs

米国

入国審査官の携帯電話検査はあり？

執筆者：*Miriam Wugmeister、J. Alexander Lawrence、Rhiannon Batchelder*

Miriam Wugmeisterは、モリソン・フォースター、ニューヨーク・オフィスのパートナー。グローバルプライバシー及びデータセキュリティ・グループの一員

J. Alexander Lawrenceは、モリソン・フォースター、ニューヨーク・オフィスのパートナー。Eディスカバリー・タスクフォースを共同統括

Rhiannon Batchelder は、モリソン・フォースター、ニューヨーク・オフィスの訴訟弁護士

このところ、米国に入国しようとして入国審査官に携帯電話やノートパソコンの検査を受けたと多くの人が報告している。その多くはアメリカ国民である。このような出来事が最近よくニュースになりその件数も増えているようだが、実はこれは新しいことではない。CNN は、米国税関当局のスポークスマンのコメントとして、2015 年に入国審査官の検査の対象となった携帯電話は 4,444 台、その他の電子機器は 320 台で、2016 年に至っては米国入国時に検査の対象となった電子機器は 23,877 台に上った、と伝えた。中国やロシアのような国では何年も前から入国審査官が携帯電話やノートパソコンを検査しており、多くの企業で、従業員がそのような国に渡航する際のガイダンスを定めたポリシーを作っている。今般、企業は機密データの入った電子機器を持って米国に出入国する従業員に対してどのようにアドバイスし、どのようなポリシーを策定すべきかについて頭を悩ませている。

入国時の検査： 憲法の枠組み

裁判所がこれまで判示してきたところでは、米国法の下、税関・国境警備局（CBP）と移民税関捜査局（ICE）の係官は、

Enforcement (ICE) agents may ask to search electronic devices at the border and may request individuals to disclose their password so they can conduct the search. These courts have held that a border agent may conduct a manual search of any electronic device without a warrant and without reasonable suspicion. *United States v. Cotterman*, 709 F.3d 952, 963 (9th Cir. 2013). A more intrusive, forensic examination of electronic devices requires that the boarder agent have reasonable suspicion of criminal activity. *Id*. at 968. "Reasonable suspicion" means "a particularized and objective basis for suspecting the particular person stopped of criminal activity." *Id*. (quoting *United States v. Cortez,* 449 U.S. 411, 417-18 (1981)). In the absence of reasonable suspicion, a border agent may still ask for the password and scroll through the contents of the device.

Border agents do not have unfettered authority in this area. For instance, a federal district court recently suppressed evidence found during a search of a laptop at the border after border agents made an exact copy of the laptop's hard drive and searched it with forensic programs. *United States v. Kim*, 103 F. Supp. 3d 32, 52 (D.D.C. 2015). The court held that there had not been reasonable suspicion that the defendant was engaged in ongoing or imminent criminal activity at the time of the border search. Therefore, the search was illegal under the Fourth Amendment. *Id*. at 59.

The precise limits on the authority of border agents in this area remain an open question; the Supreme Court has not yet weighed in on this issue.

入国審査時に電子機器の検査を行うことができ、かかる検査に際して対象者にパスワードの開示を要請することができる。つまり、これらの裁判所は、入国審査官は電子機器についての令状や合理的な疑いがなくても検査対象の電子機器を自ら操作して検査することができると判示している。*United States v. Cotterman*, 709 F.3d 952, 963 (9th Cir. 2013) 。ただし、電子機器に関してそれ以上に踏み込んだ、フォレンジック捜査を行うためには、入国審査官が犯罪行為の存在について合理的な疑いを持つことが必要である。前掲 968 頁。「合理的な疑い」とは、「対象となる特定の者の犯罪行為を疑わせる具体的かつ客観的な疑い」をいう。前掲（*United States v. Cortez*, 449 U.S. 411, 417-18 (1981) から引用）。そして、合理的な疑いがない場合であっても、入国審査官はパスワードの開示を求め、その電子機器に保存されたデータの中を自らスクロールすることはできるのである。

入国審査官は、無制限で検査権限を有するわけではない。例えば、ある連邦地裁は、最近、入国審査におけるノートパソコンの検査において、入国審査官がそのノートパソコンのハードドライブの同一コピーを作成した上で、フォレンジックプログラムを用いて見つけた証拠を排除している。*United States v. Kim*, 103 F. Supp. 3d 32, 52 (D.D.C. 2015)。裁判所はこの事例について、入国審査の時点で、被告人が犯罪行為を現に行っている、又はその危険が差し迫っているという合理的な疑いはなかったと判示し、合衆国憲法修正第 4 条に照らして捜査を違法とした。前掲 59 頁。

この入国審査官が有する権限の正確な範囲は未だ不明確であって、最高裁判所の判断もまだ存在しない。

"When travelling internationally, consider taking only a clean smartphone or laptop computer."

外国への渡航には、データを消去したスマートフォンやノートパソコンだけを携帯することを検討すべきである。

The Department of Homeland Security Guidelines

In a Privacy Impact Assessment for border searches of electronic devices, the Department of Homeland Security addressed procedures for when a device may contain privileged material. U.S. Department of Homeland Security, *Privacy Impact Assessment for the Border Searches of Electronic Devices*, Aug., 2009, at 11, 13.

With respect to searches conducted by CBP, the Assessment states:

国土安全保障省のガイドライン

国土安全保障省（DHS）は、電子機器の入国審査に係るプライバシー影響評価（PIA）において、電子機器が秘匿特権の対象となる情報を含む可能性がある際の対応手続について定めている。国土安全保障省、*電子機器の入国審査にかかるプライバシー影響評価*（2009 年 8 月、11 頁、13 頁）。

CBP が行う検査に関し、PIA は次のとおり定めている。

> [w]here an electronic device is to be detained or seized by CBP, a CBP Supervisor must approve of the detention or seizure, and the CBP Officer must provide a completed CF 6051D or S, respectively, to the traveler. Where a traveler claims that the contents of the electronic device contain attorney-client or other privileged material, the CBP Officer must consult with the local Associate/Assistant Chief Counsel or U.S. Attorney's Office before conducting the examination. *Id*. at 11.

> CBP が電子機器を留置又は押収する際、CBP 監督官は当該留置又は押収を承認し、CBP 審査官は渡航者に対し、それぞれ、CF 6051D 又は 6051S を作成して交付しなければならない。電子機器の中の情報に、弁護士・依頼者間その他の秘匿特権の対象となるものが含まれると渡航者が主張した場合、CBP 審査官は、検査を行う前に、その地域のアソシエイト/アシスタントチーフカウンセル又は連邦地方検事局と協議しなければならない。前掲 11 頁。

With respect to searches conducted by ICE, the Assessment states:

ICE が行う検査に関し、PIA は次のとおり定めている。

> a traveler's claim of privilege or statement to an ICE Special Agent that something is personal or business-related does not preclude the search. ICE policy and certain laws, such as the Privacy Act and the Trade Secrets Act, requires the special handling of some types of sensitive information including attorney-client privileged information, proprietary business information, and medical information. Special Agents violating these laws and policies are subject to administrative discipline and criminal prosecution. Further, when a Special Agent suspects that the content of electronic devices includes attorney-client privileged material that may be relevant to the laws enforced by ICE, ICE policy requires the Special Agents to contact the local ICE Chief Counsel's office or the local U.S. Attorney's Office before continuing a search. *Id*. At 13.

> 渡航者が秘匿特権を主張したり、ICE 特別捜査官に対してプライバシー又はビジネスに関する情報であると述べたとしても、それが検査を妨げるものではない。ただし、ICE ポリシーやプライバシー法、営業秘密法などの法令は、弁護士・依頼者間秘匿特権の対象となる情報、ビジネス上の秘密情報、医療情報など、特定の種類の機密情報について特別の取扱いを要求している。これらの法令・ポリシーに違反した特別捜査官は、懲戒及び刑事訴追の対象となる。また、特別捜査官が、電子機器の中の情報に、ICE が執行する法令に関連する弁護士・依頼者間秘匿特権の対象となる情報が含まれることを疑うときは、ICE ポリシーに基づき、検査を続行する前に、その地域の ICE チーフカウンセル室又は連邦地方検事局に連絡しなければならない。前掲 13 頁。

Therefore, to avail themselves of these DHS protections, individuals should notify border agents of the potential privileged or business-sensitive nature of the data on their electronic devices.

したがって、上記の DHS による保護を利用するため、渡航者は入国審査官に対して、電子機器の中の秘匿特権又はビジネス上の機密情報となり得る情報について申し出るべきである。

Practical Tips: Protecting Sensitive Data at the Border

実務における留意点： 入国審査時の機密データの保護

There are many things you can do to protect sensitive information at the border, below are a few:

入国の際に機密情報を保護するためにできることは数多くあるが、そのいくつかを紹介する。

- When traveling internationally, consider taking only a clean smartphone or laptop computer. If there is no sensitive data on the electronic device, there is no risk that such data will be

- 海外渡航の際は、機密情報を削除した携帯電話又はノートパソコンを持っていくことを検討すべきである。電子機器に機密データが入っていなければ、入国審査官がかかるデータに触れるリスクはないから

exposed to border officials.

- If all sensitive data cannot be wiped from electronic device prior to international travel, only take the information needed and remove all unnecessary sensitive data.
- Inventory all sensitive data contained on any electronic devices that will be taken across the border. That way, if it is accessed, you will know exactly what information was impacted.

- Fully power down all electronic devices prior to passing through customs. Encryption software is most effective when devices are powered down.
- If a request for a search is made, inform CBP or ICE officials if there is privileged or business sensitive data on your devices.

である。

- 海外渡航前に、電子機器から機密データの全部を消去することができない場合は、必要な情報のみにして、不要な機密情報はすべて取り除く。
- 入国の際に持ち込む電子機器の中のすべての機密情報について、目録を作成する。そうすれば、アクセスされた場合でも、どの情報に影響があり得たかが正確に分かる。

- 税関を通過する前にすべての電子機器の電源を完全に切っておく。暗号化ソフトは、機器の電源が落ちている場合が最も効果的である.
- 検査要求があった場合、CBP又はICE係官に対し、電子機器の中に、秘匿特権の対象となる情報又はビジネス上の機密データがあることを伝達する。

For more information on these issues, please contact:

Miriam Wugmeister
New York
mwugmeister@mofo.com

J. Alexander Lawrence
New York
alawrence@mofo.com

Rhiannon Batchelder
New York
rbatchelder@mofo.com

コンタクト

Miriam Wugmeister
New York
mwugmeister@mofo.com

J. Alexander Lawrence
New York
alawrence@mofo.com

Rhiannon Batchelder
New York
rbatchelder@mofo.com