Technology

Borderline Privacy: Electronic Border Searches after Cotterman

BY LOUISA K. MARION

LOUISA K. MARION is an associate in Crowell & Moring's Washington, D.C., office, where she practices in the firm's White Collar & Regulatory Enforcement and International Dispute Resolution Groups.

In what it acknowledges to be a "watershed case implicat[ing] both the scope of the narrow border search exception to the Fourth Amendment's warrant requirement and privacy rights in commonly used electronic devices," the Ninth Circuit Court of Appeals has held en banc that government officials must have "reasonable suspicion" before conducting forensic searches of laptops at the US border. (United States v. Cotterman, 709 F.3d 952, 956–57 (9th Cir. 2013).) The court's ruling in *United States v. Cotterman* presents a dramatic departure from the general rule permitting suspicionless border searches in the interests of national security.

The Cotterman Decision

The *Cotterman* case originated in 2007, when Howard Cotterman and his wife passed through a US border checkpoint on return from a vacation in Mexico. (*Id.* at 957.) When a screen of Cotterman's passport triggered a notification that he carried a 15-year-old conviction for child molestation and, as a "frequent traveler," might be involved in child sex tourism, border agents referred the couple for a secondary inspection. (*Id.*) During a vehicle search, the border agents found three digital cameras containing the couple's vacation and personal photos, as well as two laptops—one of which (Cotterman's) contained one or more password-protected files. (*Id.* at 957–58.) Although separate interviews of the Cottermans revealed nothing incriminating and Cotterman offered (but was denied the opportunity) to unlock the protected files, Immigration and Customs Enforcement (ICE) agents confiscated the laptops and one camera and sent them nearly 170 miles offsite for forensic analysis. (*Id.* at 958.) Forty-eight hours later, ICE uncovered child pornography stored in the unallocated space of Cotterman's hard drive—an area containing data deleted by and unavailable to the average user, yet not overwritten by new data. (*Id.* at 958, n.5.)

Indicted on several child-pornography-related charges, Cotterman moved successfully to suppress the laptop evidence, arguing that the remote forensic search required reasonable suspicion, which the ICE agents lacked. (*See* United States v. Cotterman, No. CR 07-1207, 2009 WL 465028 (D. Ariz. Feb. 24, 2009) (unpublished opinion).) A divided Ninth Circuit panel reversed; although seemingly conceding that the agents lacked reasonable suspicion, the court directed that no particularized suspicion was required under the agents' broad authority to conduct searches at the border. (United States v. Cotter-

man, 637 F.3d 1068, 1074 n.7, 1075, 1079 (9th Cir. 2011).) The Ninth Circuit took up Cotterman's appeal en banc and requested supplemental briefing on the reasonableness of the agents' suspicion. (*Cotterman*, 709 F.3d at 959.)

In its March 9 ruling, the Ninth Circuit bravely revisits "what limits there are upon [the] power of technology to shrink the realm of guaranteed privacy" (*id.* at 956–57 (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)))—this time at the border, where searches have long enjoyed an exception to the Fourth Amendment's warrant requirement (*id.* at 957 (citing United States v. Ramsey, 431 U.S. 606, 621 (1977))). As the Ninth Circuit explains, although border searches are subject to "reasonableness" limitations under the Fourth Amendment, the Supreme Court has "never defined the precise dimensions of a reasonable border search." (*Id.* at 963.) Instead it has called for a case-by-case analysis, balancing individual privacy rights against the strongly favored interests of the sovereign (*id.* at 960, 963), and carving out limited exceptions in which the government may need particularized suspicion—such as for searches involving "highly intrusive searches of the person," conducted in a highly offensive manner, or resulting in the destruction of property (*id.* at 963 (citing cases)). Following these signposts, courts, including the Ninth Circuit, have upheld cursory searches of electronic devices at the border without particularized suspicion. (*See id.* at 960, n.6 (citing United States v. Arnold, 533 F.3d 1003, 1008–10 (9th Cir. 2008), and narrowing its holding to simple searches).)

But a "comprehensive and intrusive" forensic search of a laptop requiring the use of software, the Ninth Circuit asserts, is a different story. (*Id.* at 962, 967-78.) Such a search "implicat[es] substantial personal privacy interests" (*id.* at 964) because individuals today carry "private and sensitive information ranging from personal, financial, and medical data to corporate trade secrets" on their various devices on a daily basis (*id.* at 956). The *nature and volume* of such information renders these devices more akin to the "personal papers" guaranteed special treatment by the Founders—who shared "deep concern with safeguarding the privacy of thoughts and ideas" (*seeid.* at 964)—than the personal property less closely protected by Supreme Court jurisprudence: "Unlike searches involving a [disassembled, searched, and] reassembled gas tank . . . , which have minimal or no impact beyond the search itself—and little implication for an individual's dignity and privacy interests—the exposure of confidential and personal information has permanence. It cannot be undone." (*Id.* at 967 (citations omitted).)

Moreover, the court asserts, a rationale advanced in favor of a broad border search exception—that travelers forewarned of an impending border search may leave behind their sensitive materials (*see, e.g.*, United States v. Ickes, 393 F.3d 501, 506 (4th Cir. 2005))—falls apart because electronic devices "often retain . . . information far beyond the perceived point of erasure." (*Cotterman*, 709 F.3d at 965.) Thus, even those who have invested significant time segregating and deleting such information may find that data remains hidden in their hard drive's slack space, depriving them of the opportunity to "make meaningful decisions" as to government scrutiny of their modern personal papers. (*Id.*) The Ninth Circuit directs: "A person's digital life ought not be hijacked simply by crossing a border." (*Id.*) Absent reasonable suspicion, the government should not have free rein to conduct a "computer strip

search" (*id.* at 966), read a traveler's diary (including erased content) "looking for mention of criminal activity" (*id.* at 962–63), or examine a suitcase for "not only what the bag contained on the current trip, but everything it had ever carried" (*id.* at 965).

Nevertheless, the court concludes, the evidence from Cotterman's laptop need not be suppressed because ICE *had* the reasonable suspicion required: The forensic search was permissible because Cotterman had a sex offense conviction, traveled frequently to international destinations, was returning from "a country associated with sex tourism," carried "paraphernalia of child pornography" (i.e., laptops and digital cameras), and had a device containing password-protected files. (*Id.* at 968–70.)

Assessing the Ruling

The Ninth Circuit's en banc decision is indeed watershed, and joins what one can only hope is a rising tide of cases recognizing the need for increased privacy protections in the modern digital age. The court is right to recognize the risks that consolidation of so much data on personal devices poses to a modern user's personal privacy—especially when over one million such users cross the US border each day. (*Id.* at 956.) A rule that lays bare one's "digital life" to border control leaves travelers with the impossible choice between traveling entirely without electronics (a non-option for most business travelers, students, or employees whose offices require telework), carrying a new or "wiped" device (potentially an expensive, time-consuming, and/or ineffectual process), disengaging from modern life (voluntarily foregoing e-mail, electronic address books, paperless banking, etc.), or surrendering all such personal information to government view. Each is arguably too high a price to pay.

In dissent, Judge Milan D. Smith asserts that by "[m]apping our privacy rights by the amount of information we carry," the majority's rule leads to the "unreasonable and absurd result[]" that those who can afford a large hard drive or sophisticated device receive greater protection than those "presumably less able to afford those more capable devices." (*Id.* at 987 (Smith, J., dissenting).) But that misses a key point: It is the *nature* of the information, a large volume of which the use of modern technology exposes at the border, as well as the lack of meaningful choice that users have about transporting it across borders, that drives the need for special treatment. By contrast, those without technological devices retain the ability they have always had to make meaningful choices about what private materials they carry across the border.

In fact, suspicionless searches may disparately *harm* those who cannot afford to maintain separate devices for sensitive data and for travel, or who lack the technological wherewithal (or corporate technology department) to insulate or properly purge this data. (And, to the extent that they move this data to the cloud in an effort to avoid carrying it across borders, they may be faced with the added concern that their "voluntary disclosure" to a third party cuts off their expectation of privacy in that data. (*Compare* Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.* (permitting warrantless searches of the contents of some electronic communications and remotely stored data), *with* United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) (declaring the Stored Communications Act unconstitutional to the extent it permits the government to obtain, without a warrant supported by probable cause, the content of e-mails stored on third-party servers).)

Although the Ninth Circuit has taken an important step toward improving personal privacy protections at the border, its focus on *methodologies*—the use of computer software for "forensic" searching, rather than manual searching—may create line-drawing problems in its application. For example, should the standard of required suspicion change as analysts become more adept at manually rooting out contraband across a large data set? And, as Professor Orin Kerr asks, what, if any, limits are there on *how much* agents can manually search absent reasonable suspicion? May they guess at passwords without reasonable suspicion, even if they may not crack them through "forensic" testing? And would the use of the device-owner's *own* pre-installed software to recover deleted files constitute a forensic search? (Orin Kerr, *What Is the Ninth Circuit's Standard for Border Searches under* United States v. Cotterman*?*, VOLOKH CONSPIRACY (Mar. 11, 2013), http://www.volokh.com/2013/03/11/what-is-the-ninth-circuits-standard-for-border-searches-under-united-states-v-cotterman/.) This standard will require some clarification by the lower courts.

Finally, it is worth noting, as does Judge Smith in his dissent (*Cotterman*, 709 F.3d at 990–95 (Smith, J., dissenting)), that despite the majority's heavy focus on privacy rights, the bar it sets for "reasonable suspicion" is quite low: The majority relies on a 15-year-old conviction, "frequent" (yet unquantified) travel to a (nearby, popular) tourist destination associated with sex tourism, the carrying of laptops and digital cameras ("paraphernalia of child pornography"), and the existence of a few password-protected files to justify an admittedly exhaustive and intrusive search. Where suspicion is so easily found reasonable, it remains to be seen how much of a watershed the Ninth Circuit's opinion will be.