Privacy issues in border searches of electronic devices[1]

Mary Ellen Callahan, Chief Privacy Officer, U.S. Department of Homeland Security

Since the founding of the United States, border officials have had the authority to search the baggage of citizens and non-citizens alike wishing to enter the country - much as their counterparts have similar authorities in other countries. Now, this authority is carried out by the US Customs and Border Protection (CBP) and the US Immigration and Customs Enforcement (ICE) – components of the U.S. Department of Homeland Security (DHS). At the border, US officials - like the officials of many other democracies - for many years appropriately have had a wider scope of authority to search individuals' property than, for example, law enforcement officers elsewhere within the country's borders. A city police officer, quite rightly, does not ordinarily have the authority to direct individuals on the sidewalk to empty their pockets, their briefcase, or their backpack. DHS' border authorities permit the inspection, examination, and search of baggage, including electronic devices, to determine if there is merchandise subject to duty or being introduced to the United States contrary to law, and to ensure compliance with any of the hundreds of laws or regulations enforced or administered by DHS. In 2008, the Ninth Circuit US Court of Appeals (and the US Supreme Court when it subsequently chose not to review the decision of the Ninth Circuit) reaffirmed border officials' authority and specifically its application to electronic devices.[1] In fact, the US Supreme Court and the US Congress in its lawmaking capacity have long held that there is no expectation of privacy for materials and goods carried over the US border, regardless of one's status in the United States.[2] In recent years, DHS searches of electronic devices, sometimes informed by ongoing criminal investigations, have yielded evidence of illegal conduct such as economic espionage, trade secret violations, and the horrific images of child pornography. However, DHS also recognizes that there are significant privacy concerns raised by the border search of electronic devices, which often contain a volume and range of types of information not found in the traditional briefcase.

On 27 August 2009, DHS Secretary Janet Napolitano announced new directives for both CBP and ICE to enhance and clarify oversight for searches of computers and other electronic media at US ports of entry. As an integral part of DHS policy creation and implementation, my office, the DHS Privacy Office (working collaboratively with the privacy officers in CBP and ICE) played a significant and important role in the internal dialogue on the new directives. Consistent with our tradition of openness and transparency, I released a Privacy Impact Assessment (PIA) entitled Border Searches of Electronic Devices related to the new directives and their impact on travelers that details the significant policy and scope restrictions that DHS has voluntarily put into place.[3] As with all PIAs on nonclassified systems, it is publicly available on our website[4] and the CBP and ICE directives themselves are addenda to the PIA. Most DHS PIAs are derived from the EGovernment Act, which mandates an assessment of the privacy impact of any substantially revised or new information technology system. In the case of border searches of electronic devices, there is no new IT system and therefore the E-Government Act did not apply; the Border Searches of Electronic Devices PIA was conducted as part of my discretionary authority to increase transparency and to enhance public understanding of the authorities, policies, procedures, and privacy controls related to these searches. The Border Searches of Electronic

[1] As published in *data protection law & policy*, October 2009

Devices PIA discusses DHS' general border security mission, definitions of commonly used terms, and the parameters of border searches conducted by CBP and ICE. It details the border search process as it pertains to electronic devices, concentrating on why CBP and ICE conduct searches, how CBP and ICE handle electronic devices, and the policies and procedures in place to protect individuals' privacy. In addition to increasing transparency and disclosure associated with DHS activities, the PIA confirms the DHS' compliance with the spirit and the letter of all relevant laws (including those laws that relate to privacy).[5]

The Border Searches of Electronic Devices PIA is an example of how specific knowledge and expertise are essential to applying privacy protections in a highly specialized area. For example, CBP and ICE are authorized to enforce a broad range of laws at the border, however the exercise of this authority with respect to the search of electronic devices requires the use of discretion in the enforcement of specific laws including but not limited to those pertaining to customs, immigration, child pornography, economic espionage, and money laundering[6]. Any review of electronic devices must focus solely on the laws enforced by CBP and ICE. Therefore, the PIA had to be tailored to the enforcement of these laws while detailing the increased procedural safeguards and supervisory requirements that not only provide guidance to CBP and ICE employees, but also increased transparency to the traveling public.[7] These safeguards include limiting the scope of access and authority for searches and defining strict timelines for the detention of devices.[8]

There are several new elements of the CBP and ICE directives, developed concurrently with the PIA, that provide additional protocols for border searches of electronic devices and are thus worth highlighting. The directives now include certain timeframes as guideposts in which to complete a border search. Searches of electronic devices are generally to be completed by CBP (the interdictory agency) within five days and by ICE (the investigative agency) within 30 calendar days of the date of detention of the electronic device (subject to extensions for law enforcement purposes). The materials can only be detained during the search itself; as soon as the material(s) have been determined to have no law enforcement value for the laws for which CBP and ICE have authority (see footnote 5), the materials must be returned within seven days.[9] These timelines provide clear requirements both for the amount of time the material can be detained and reviewed, as well as the scope of the authorities for CBP and ICE. This information, including timing and appeal rights, is clearly spelled out in documents that DHS is distributing to affected travelers detailing what is happening with the device. The document is also a new initiative to give more information to the traveling public; it will be distributed to anyone whose device is being searched or detained.[10]

Under the new directives, both CBP and ICE added layers of supervisory review and other privacy protections - whether it is CBP requiring supervisory approval for initial detentions or ICE requiring reasonable suspicion before seeking subject matter expertise from outside agencies. In addition to these new procedural layers, Secretary Napolitano has ordered increased transparency relating to border searches and civil rights and civil liberties, and has directed enhanced training for border officers and special agents alike. The DHS Office for Civil Rights and Civil Liberties (CRCL) will also conduct a Civil Liberties Impact Assessment within 120 days of the release of the new directives, and in conjunction with the Privacy Office and CRCL,

CBP will ensure training materials and procedures promote fair and consistent enforcement of the laws and policies relating to searches of electronic devices. Furthermore, ICE is expanding and enhancing its training, including designing a virtual course to be required of all special agents.

The new directives related to border searches of electronic devices are important policy and procedural steps DHS has taken to provide clarity associated with its border authority, and the PIA and new public disclosures significantly improve transparency. With that said, despite the media attention given to 'the laptop search issue,' it is important to recognize how infrequent laptop searches are conducted. The impact on travelers is fairly small: between 1 October 2008 and 11 August 2009, CBP encountered more than 221 million travelers at US ports of entry. Approximately 1,000 laptop searches were performed in these instances-or roughly one laptop search for every 442 jumbo jets full of 500 passengers each. The vast majority of these searches were as simple as asking the traveler to power on the device to show that it is what it purports to be. Of the 1,000 searches, just 46 were in-depth, or one in-depth laptop search for every 9,600 jumbo jets full of travelers.

The mandate of my office, the DHS Privacy Office, is to minimize the impact on individuals' privacy, particularly individuals' personal information and dignity, while achieving the mission of DHS. DHS is charged with ensuring compliance with federal laws at the border including those preventing contraband, other illegal goods, and inadmissible persons from entering or exiting the United States. The Border Searches of Electronic Devices PIA and the directives preserve the flexibility of border officers to achieve their mandated missions while enhancing transparency and oversight. The authority of my office to issue this PIA is important to our nation's dialogue, both domestically and overseas, on the balance of law enforcement and security with civil rights and civil liberties in the context of border searches of electronic devices. Transparency is an important element of the US privacy framework, as evidenced by this PIA. While security agencies in other countries have missions similar to ours and the right to search electronic devices at the border, few if any others provide similar levels of oversight and transparency as that reflected in the PIA.

Debate will likely continue over searches at the border, but the DHS cannot abandon its responsibility to inspect materials that cross our borders just because the information is on an electronic device. To do so would create a protected class of materials, unlike any other, and would lay a path for criminals to exploit our borders in a way never permitted by either the Supreme Court or Congress. It is my job to see that border searches are done in a way sensitive to privacy and I commend ICE and CBP for implementing the directives, training, and policies reflected in this PIA. I welcome an open discussion with other border agencies to share knowledge and experience of each others' security mandates and privacy policies and practices. To only address privacy concerns without considering the realities of border control could leave any sovereign nation vulnerable to those wishing to do harm. I therefore value my role within the Department to affirm and implement privacy enhancements to our important missions.

[1] United States v. Arnold, 523 F.3d 941 (9th Cir. 2008), cert. denied, 129 S.Ct. 1312 (Feb. 23, 2009); see also United States v. Ickes, 393 F.3d 501 (4th Cir. 2005); United States v. Romm, 455 F.3d 990 (9th Cir. 2006); and United States v. Roberts, 274 F.3d 1007 (5th Cir. 2001).

2 See, e.g., 19 U.S.C. §§ 482, 1461, 1496, 1499, 1581-1582; see generally United States v. Flores-Montano, 541 U.S. 149 (2004); United States v. Montoya de Hernandez, 473 U.S. 531 (1985).

[3] www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_laptop.pdf

[4] www.dhs.gov/privacy

[5] E.g., 8 U.S.C. §§ 1225 and 1357, 19 U.S.C. §§ 482, 507, 1461, 1496, 1499, 1581, 1582, and 1595a(d), 22 U.S.C. § 401, and 31 U.S.C. § 5317, as well as the attending regulations of U.S. Customs and Border Protection promulgated at Titles 8 and 19 of the Code of Federal Regulations.

[6] As the nation's law enforcement agencies at the border, CBP interdicts and ICE investigates a range of illegal activities such as child pornography; human rights violations; smuggling of drugs, weapons, and other contraband; financial and trade-related crimes; violations of intellectual property rights and law (e.g., economic espionage); and violations of immigration law, among many others. CBP and ICE also enforce criminal laws relating to national security, terrorism, and critical infrastructure industries that are vulnerable to sabotage, attack or exploitation.

[7] The DHS Privacy Office (my office) addresses major policy decisions throughout the Department; in addition, as part of DHS goal of institutionalizing privacy throughout the Department, each component agency has a privacy officer. Laurence Castelli (CBP) and Lyn Rahilly (ICE) were invaluable in the development and implementation of this PIA and related directives.

[8] DHS cannot and will not disclose information discovered outside the scope of its authorities when conducting a border search of electronic devices.

[9] There may be circumstances where information is copied rather than detaining the whole device. In those circumstances, the same timelines apply for review, and destruction (rather than return) of copied non-law enforcement information.

[10] The new document or "tear sheet" is available at Appendix B of the PIA, providing information related to the reasons for the search, how individuals' data may be used and detailed information about their constitutional and statutory rights.