



# **Crossing the Canadian/US Border: Are Your Electronic and Personal Data and Information at Risk?**

## **The United States Perspective**

**Ontario Bar Association 2009 Institute  
Toronto, Ontario  
Tuesday, February 3, 2009**

### **David P. Sanders**

Partner, International Section  
Williams Mullen  
1666 K Street N.W., Suite 1200  
Washington, D.C. 20006  
(202) 293-8113 (Telephone)  
(202) 293-5939 (Fax)  
[dsanders@williamsmullen.com](mailto:dsanders@williamsmullen.com)



## Topics Discussed

- **U.S. Policy on Laptop Searches**
- **Legislation to Protect Electronic Privacy**
- **A Practical Guide to Protect Your Data**
- **Resources**
- **Questions – After Presentation**



## **U.S. Policy on Laptop Searches**

- **Fourth Amendment Framework**
- **Border Search Exception**
- **Recent Jurisprudence**
- **U.S. Customs Authority to Search**
- **U.S. Customs Policy**



## Border Search Exception

- **4th Amendment**
  - No Unreasonable Searches & Seizures
  - No Warrants Shall Issue without Probable Cause
- **Border Search Exception** – *United States v. Ramsey*, 431 U.S. 606 (1977).
  - National Security at Border Outweighs Privacy
  - Probable Cause or Warrants Not Required
- **Routine v. Non-Routine Searches** – *United States v. Montoya de Hernandez*, 473 U.S. 531, 541 (1985).



## Border Search Exception

- **Routine** – No Level of Suspicion
  - Searches without a high degree of intrusion
    - Examples: vehicles, luggage, outer clothing, personal effects, purses, wallets.
- **Non-routine** – Reasonable Suspicion
  - Searches with a high degree of intrusion that invades the privacy and dignity of the individual
    - Examples: strip searches, X-rays
- **Reasonable Suspicion** – particularized and objective basis to suspect criminal conduct



## Laptops Within Border Search Exception

- **Laptop searches are within border search exception and therefore do not require a warrant or probable cause**
  - *United States v. Arnold*, 523 F.3d 941 (9th Cir. 2008)
  - *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005)
- **No level of suspicion is required**
  - Seven Circuits hold laptop searches are routine
  - Some Circuits avoid issue, finding reasonable suspicion
- **Supreme Court has not addressed whether searches of electronic devices is routine or non-routine**



## Border Search Exception

- ***Where does the Border Search Exception Apply?***
  - **US Border**
  - **Functional Equivalent** – *Aleida-Sanchez v. United States*, 413 U.S. 266, 272-73 (1973)
    - Airports
    - Ports
  - **Inbound and Outbound Traffic**
  - **Extended Border** – *See United States v. Teng Yang*, 286 F.3d 940, 946 (7th Cir. 2002). Example: field on US side next to the Rio Grande River.
    - Requires reasonable suspicion of criminal conduct



## U.S. Customs & Border Protection: Search & Seizure Authority

- Congress granted U.S. Customs expansive authority to search *any* vessel, vehicle, person, trunk, package, or cargo
  - 19 U.S.C. 1582(a)
  - 19 C.F.R. 162.6, 162.7.
- Electronic devices falls within scope of “cargo.” *Ickes*.
- Customs Officers may **seize** property only if there is **reasonable cause** to believe that any law or regulation enforced by CBP or ICE has been violated
  - 19 C.F.R. 162.21



## U.S. Customs and Border Protection Policy, July 16, 2008

- **Policy** – Customs at U.S. border may search electronic devices *absent individualized suspicion*
- ***What Electronic Devices are Covered?***
  - Electronic storage devices, computers, disks, hard drives, Blackberries, PDAs, iPods, cellular telephones, digital cameras
- **Customs May Detain Electronic Device and Data to Conduct Search**
  - Reasonable Period of Time
  - On-site or off-site



## U.S. Customs and Border Protection Policy, July 16, 2008

- **Customs May Transfer Device or Data to Other Federal Agencies to Assist**
  - Translation and decryption to access data
  - Original documents or device detained when *necessary*
  - Agency response time: **15 days** and **7 day** extensions
- **Probable Cause Required to Seize Originals or Copies**
  - Unless ICE matter
- **Customs May Retain Copies of Data For Search**
  - If no probable cause to seize, copies *must* be destroyed



## U.S. Customs and Border Protection Policy, July 16, 2008

- **Business Confidential Information**
  - The Trade Secrets Act, the Privacy Act, and other laws may govern or restrict the handling of the information
- **Attorney-Client Privilege**
  - Although legal materials are **NOT** necessarily exempt from a border search, they may be subject to **special handling procedures**
  - If attorney-client privilege is asserted, Customs Officer **MUST** seek advice from the CBP Associate/Assistant Chief Counsel or the appropriate U.S. Attorney's Office **BEFORE** conducting a search of the document



## Customs' Laptop Search Data

- **In August 2008**
  - 38,050,654 People and Conveyances Crossed Border
  - 169 Resulted in Laptop Search
  - 2 Laptops Searched Resulted in Seizure
- ***What Evidence of Crimes have Been Found?***
  - Child Pornography
  - Terrorist Plans, Martyrdom Videos
  - Intellectual Property Infringement
  - Trade Secrets



# Legislation Protecting Electronic Privacy

- **Traveler's Privacy Protection Act of 2008 – S.3612 (Feingold Bill-proposed)**
  - Reasonable Suspicion Required to Search
  - Probable Cause Required to Seize
  - NO off-site removal for search
  - Record-keeping requirements
- **Border Search Accountability Act of 2008 – H.R. 6869 (proposed)**
  - Record-keeping requirements
  - Require specific retention timeframe
  - Written notification of duplication and third party access 13



## What Can You Do To Protect Attorney Work Product?

- **Label Files “Attorney-Client Privilege”**
  - Customs Officer **MUST** seek advice from the CBP Associate/Assistant Chief Counsel or U.S. Attorney’s Office **BEFORE** conducting a search
  - Labeling puts Customs on Notice
  - Data and/or Laptop could still be detained to make determination
- **Alert Customs Officer to Attorney-Client Privilege**



# What Can You Do To Protect Attorney Work Product?

- **Forensically Clean Computer / Delete History**
  - Overwrite Files
  - Examples: Secure Erase (Macs), ShredU (Linux)
- **External Internet Storage Center**
  - Example: Encrypted VPN (Amazon S3)
  - Warrant **NOT** required for government search
    - Protect America Act and USA Patriot Act



# What Can You Do To Protect Attorney-Client Work Product?

- **Password Protection and Encryption**
  - Customs May Decrypt Data
  - Customs May Not Compel Password Disclosure
    - *In re Boucher*, 2007 LEXIS 87951 (D.C. Vt. 2007)
  - May result in original or device seizure
- **Save Data as Different User**
- **ALWAYS back up your data in event of laptop seizure**
  - Customs has lost information / detained indefinite period
- **Ask for a Badge Number and Receipt if Data Detained**



## Protecting Your Data

- **Summary**
  1. Label Files “Attorney Client Privilege”
  2. Backup Your Data
  3. Forensically Clean Computer and Clear Internet History
  4. Store Data on Secure Private Network
  5. Encrypt Data with Password Protection



## Useful Resources

- Border Search Exception and Laptop Searches
  - Yule Kim, *Border Searches of Laptops and Other Electronic Storage Devices*, Cong. Research Service Report for Congress, Mar. 5, 2008, available at [www.opencrs.org](http://www.opencrs.org).
- U.S. Customs and Border Protection Policy
  - [www.cbp.gov/linkhandler/cgov/travel/admissibility/search\\_authority.ctt/search\\_authority.pdf](http://www.cbp.gov/linkhandler/cgov/travel/admissibility/search_authority.ctt/search_authority.pdf)



**Questions?**

