Privacy in Cross-Border Preservation

Erin Tripp, Business Development Manager
CNI Spring 2018
San Diego, California
Thursday, April 12
Session Notes: https://bit.ly/2GJJG42
Twitter: @eeohalloran
Privacy in Cross-border Preservation

- Introduction
- Digital Preservation
- Privacy and Data Protection
- DuraCloud
- Research
- Lessons Learned
- Next Steps
- Discussion

Image Credit: GDJ
Introductions: Erin Tripp

- Librarian working in project management and business development in OSS for six years
- Began at DuraSpace as its new Business Development Manager in May 2017
- Experienced legal researcher and witness from the Parliamentary Standing Senate Committee on Official Languages
Introductions: DuraSpace Stewards OSS

We steward the software and standard ontology for representing scholarship, called VIVO and two open source repository software: DSpace and Fedora.

We also steward DuraCloud, a content and preservation storage software.
Digital Preservation

Multiple independent copies of digital material stored in different geographic locations

What jurisdictions are allowed according to privacy and data protection regulations?

Image Credit: belthsazar_liem
In Canada, I observe reluctance to use U.S.-based storage providers due to privacy and data protection regulations and/or concerns.

Similar sentiments are expressed by peers in Germany, the Netherlands, the UK and other jurisdictions.
Privacy and Data Protection

Example: UK-based digital preservation tender

- Information security guidelines did not include storage location
- Inquiries found U.S. storage would not be considered
- The UK data protection act says data can’t be transferred outside of Europe “without adequate protection.”
Privacy and Data Protection

“All transfers of information create legal issues, particularly where the transfer is to a third party across borders”

(Banks, 2013).
DuraCloud

- Suite of Open Source Software
- Storage mediation system
- Comprehensive REST API
- Provides duplication and bit-level integrity checks
DuraCloud

- No established community of developers outside of DuraSpace (yet!)
- Working to:
  - Attract new contributors
  - Develop more welcoming and accessible docs
  - Encourage and support new installations and services

Image Credit: colinda
DuraCloud

- Joined Mozilla Open Leadership Training Program with DuraCloud community building objective
- Worked with the Texas Digital Library to install and support DuraCloud
- Worked with 4Science, to improve documentation, audit install, and provide training for DuraCloud Europe service
Research Required
- As we worked to build the DuraCloud community, questions emerged:

  - Is there flexibility to change DuraCloud’s dependencies to address privacy and security requests?

  - What are our obligations under law if the US government requested data stored through our services?
Research Required

- We researched cross-border privacy and data protection

- We spoke to:
  - Our general counsel
  - Our hosting provider (AWS)
  - Members of our community seeking referrals for specialized legal counsel

Image Credit: Gerald G
Research Required

We consulted with attorneys:

Joe McClendon who focuses on commercial and technology transactions, leveraging his decade of experience as an IT professional

Matt Lee advises on compliance issues under the USA Patriot Act
Lessons Learned

- Global trend shifting to greater transparency with regard to how organizations handle data

- Europe’s General Data Protection Regulation (GDPR) is considered the most important change in data privacy regulation in 20 years and cloud storage providers plan to comply

- Large U.S.-based cloud storage providers (AWS and Microsoft) publicly state they will not disclose customer information, unless ordered to by valid court order, subpoena
Lessons Learned

U.S. Justice Department is entitled to data hosted with U.S.-based providers in other jurisdictions. It may execute a search warrant or issue a subpoena.

Mutual Legal Assistance Treaties (MLATs) are also used. They’re “agreements between two or more countries, which create obligations under international law for governments to assist one another in criminal investigations and prosecutions” (MLATs, n.d.)
Lessons Learned

Case Study: Microsoft v U.S. DOJ

- Microsoft is first American company to challenge a domestic search warrant seeking data held outside the United States
  - Company has 100 data centres in 40 countries

- Challenge based on
  - Protection of laws and interests of other countries
  - Concern that customers will go elsewhere if they think the US government’s reach extends to data centres around the world

- New York-based court of appeals, sided with Microsoft in 2016

- U.S. Government appealed ruling to the supreme court
Lessons Learned

- Federal prosecutors asked that the case with Microsoft be dismissed (Reuters, 2018)

- U.S. President signed a provision into law, known as the Clarifying Overseas Use of Data (CLOUD) Act

- U.S. judges can issue warrants for data stored in other jurisdictions

- Companies can object if the request conflicts with foreign law.
Next Steps

- Staying abreast with international privacy developments
- Develop documentation on how we will handle data requests
- Develop a privacy and data protection policy that outlines our obligations and data protection best practice with our partners
- Be flexible to accommodate the privacy regulations internationally

Image Credit: danilo
Discussion

● What are your experiences with privacy, data protection and data storage?
● Does this topic interest you?
● Do you have additional areas of interest not covered here?
● Contact: etripp@duraspace.org or @eeohalloran

Image Credit: hs
Thank You for Coming!

Erin Tripp | etripp@duraspace.org | @eeohalloran