

in **FUSION** 11

Cross-Border E-Discovery: Navigating Rules and Regulations Across Multiple Jurisdictions

Kenneth N. Rashbaum, Esq.



FUSION11 Session Agenda

1. Privacy and data protection concepts beyond the U.S.

- How they affect ability to gather electronic evidence for U.S. litigation, regulatory proceedings and business processes

2. Recent developments in privacy and data protection:

- Tightening (Spain and France) and loosening (U.K.) of barriers to transfer personal data outside the E.U.

3. Practical suggestions for collection, review and disclosure or discovery of offshore data



FUSION11 Caveats

- Inconsistencies between countries:
 - Privacy and data protection laws vs. need to expedite global business; historical antecedents that inform privacy and data protection
- Many gray areas:
 - Protections can differ between countries and even provinces
- Law is evolving
 - (2/11/09 Article 29 Working Party Document; *Christopher X* (France); *Digicel* (U.K.); the Sedona Conference® *Framework for Analysis*, cited by European Commission); **Cloud issues**

FUSION11 Data Transfer and Disclosures

- Data retention and disclosure rules vary by:
 - Region (EU),
 - Country (enabling legislation), and
 - Sometimes province or state within a country (German Lander, for example)
- **Key Concept: “Personal Data” is protected.**
 - ***Emails are personal data, as they can be traced to an identifiable individual***



FUSION11 Cross Border Laws: The E.U. Privacy Floor

- **EU Data Protection Directive (95/46)** - Member nations must implement laws to restrict all manner of “processing” of “personal data” meaning “any information relating to an identified or identifiable natural person” (see EU Directive Article 2)
 - Prohibits transfer of personal data outside the EU unless the country to which it is transferred provides “adequate protection” of personal data (EU Directive Article 25)
 - Only Canada, Argentina, Switzerland and Israel meet E.U. “adequate protection” standard



FUSION11 E.U. Data Protection

- **Rule:** Any transfer of personal data to a third party requires a justification and – in case of countries outside EEA – additional safeguards
- The concept of “pre-trial discovery” is unfamiliar to most EU countries (except UK)
 - **Rule:** Each party may use only own documents as evidence
 - ⇒ These legal and cultural differences are relevant in the data protection assessment
 - Consent may be of doubtful validity in some countries
- Statutory exemptions
 - “Transfer necessary to safeguard legitimate interests of parties to litigation and no overriding interests of affected individuals”
 - “Transfer necessary for exercise or defence of legal claims in court”

Don't Assume U.S. Terms Have Same Definitions Elsewhere

- “Privacy Law” in U.S. = “Data Protection” in EU
- “Data Subject” is usually an individual but can also be a legal entity (Italy)
- “Data Processing” can be storage or mere accessing of data.
 - Preservation (litigation hold) may be considered processing if it involves manipulation of data, such as moving data to a secure server or even preserving in place
- “Discovery” in U.S. = “Disclosure” in civil law jurisdictions
- E-Mail in U.S. is “Personal Data” in EU and elsewhere

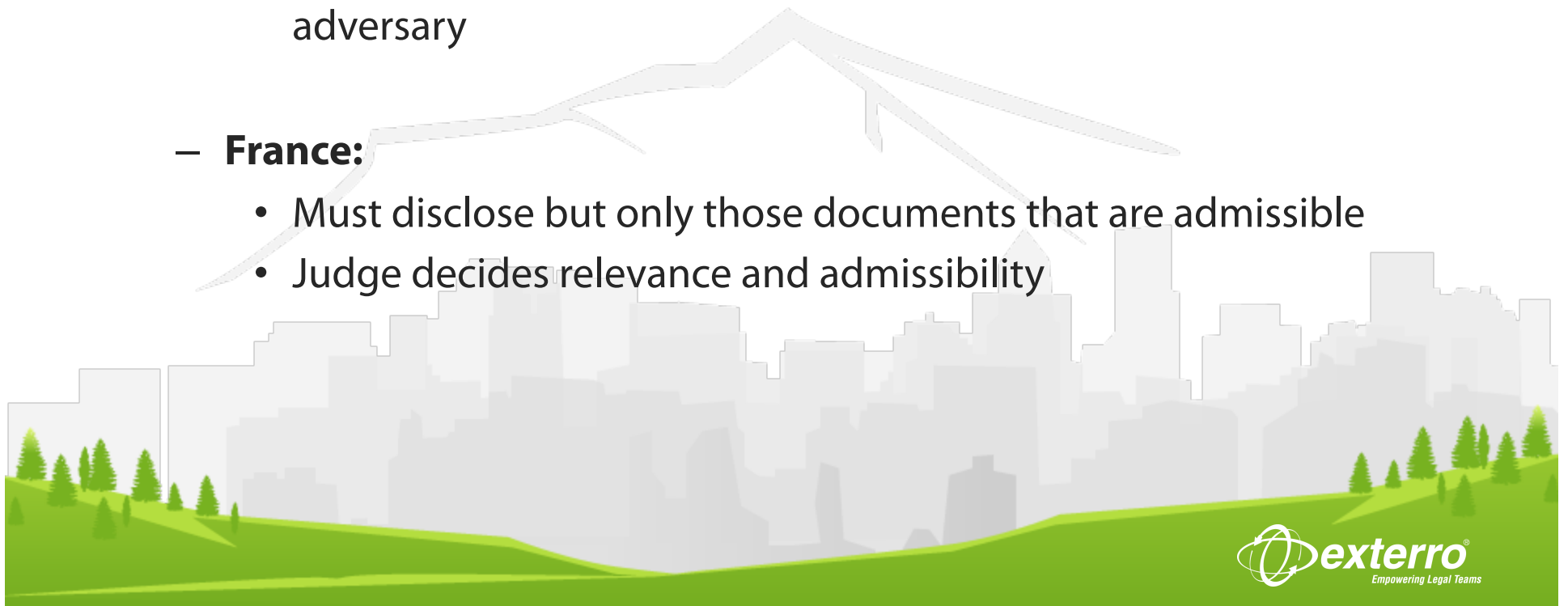
FUSION11 Discovery vs. Disclosure

- Common Law Jurisdictions: wide-open pre-trial exchange of information
 - **US**: Fed. R. Civ. Proc. 26(b): “**discovery** *reasonably calculated to lead to admissible evidence*”



FUSION11 Discovery vs. Disclosure (cont'd.)

- Civil Law Countries: **Disclosure** limited to trial evidence
 - **Germany:**
 - Litigants not required to produce documents
 - Need only produce to court that which supports its litigant's case
 - Judge decides whether to order document produced to adversary
 - **France:**
 - Must disclose but only those documents that are admissible
 - Judge decides relevance and admissibility



inFUSION11 Privacy Laws With Criminal Liability

- Blocking statues prohibit transfer of economic, commercial or technical data for use in foreign judicial proceedings.
- Personal nature of the data not relevant
- France and Venezuela (general); Switzerland (banking); limited blocking statutes in Canada, U.K., South Africa, Russia
- Privacy statutes have criminal penalties in Switzerland, Italy (recent Google conviction) and Venezuela



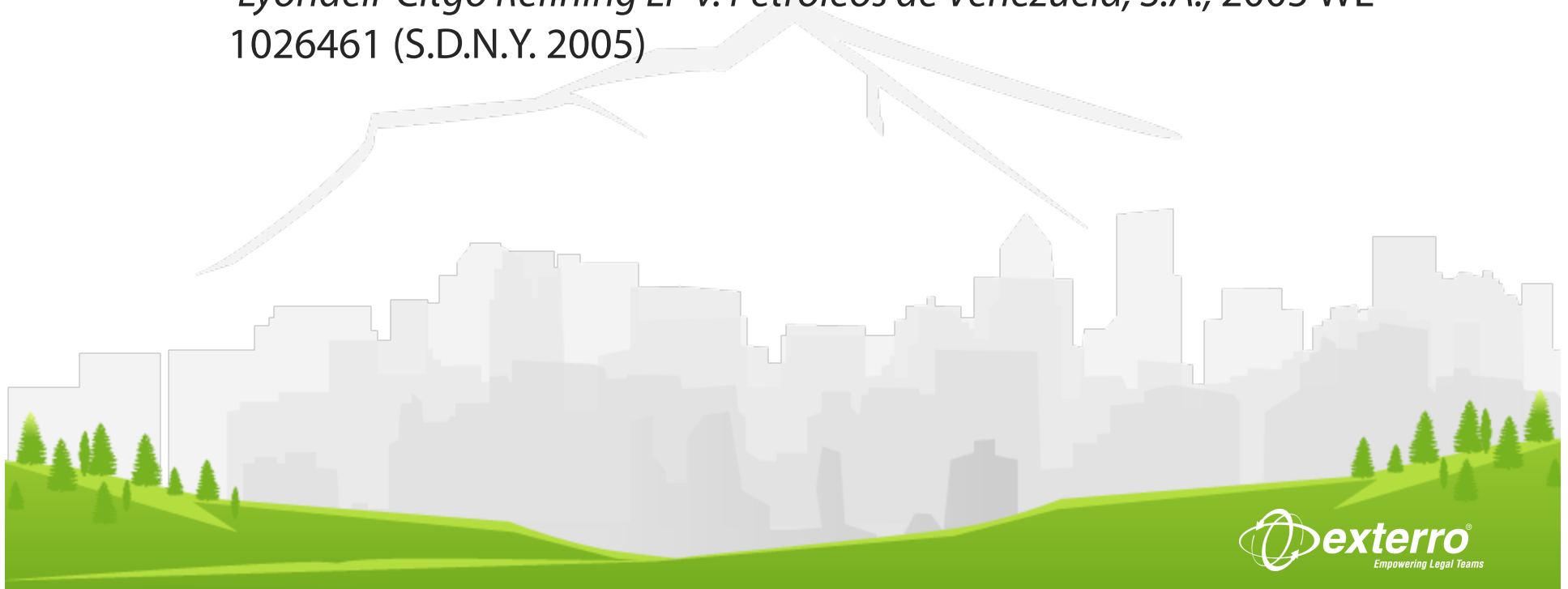
FUSION11 South America: Habeas Data

- Concept of Habeas Data
 - A constitutional right first embodied in Brazil's new constitution, 1988.
 - Followed by Paraguay (1992), Peru (1993), Ecuador (1996), and Colombia (1997)
 - **Individual can obtain information on what data are kept on him/her, and request corrections, amendments or destruction**
- Argentina and Chile have EU-style data protection
 - Argentina is one of four countries EU considers equivalent in privacy protection



FUSION11 South America: Habeas Data (cont'd.)

- Be aware of local variations in this concept and data protection
 - Example: Not all countries permit request for destruction (in effect, precluding disclosure in litigation or investigation)
- Real-World Consequences: Adverse inference instruction accepted rather than violate privacy provisions with criminal sanctions
 - *Lyondell-Citgo Refining LP v. Petroleos de Venezuela, S.A.*, 2005 WL 1026461 (S.D.N.Y. 2005)



- Japan's Personal Information Protection Act of 2003:
 - **Rule:** Consent required for transfers of “personal information” to third-parties (Art. 23, Par. 1)
- Data subject may request his/her personal data and must be provided an opportunity to correct, supplement or delete it (Art. 26)
- Entity holding personal data must specify the purposes of its use (Art. 15, Par. 1)
- Data subject may request cessation of use of the data if the data is used beyond the purposes in the Notice (Art. 27)

FUSION11 Disclosure and Discovery in Asia

- Korea:
 - **Rule:** Data to be *deleted when no longer needed for intended purpose of processing* (APPII Art. 17 (3)).
 - Data needed later for U.S. litigation may no longer exist, resulting in sanctions (cf., *Adams v. Dell, re Taiwan*)
- Australia:
 - Practice Note 17 (meet and confer)
- Hong Kong:
 - Practice Direction 5.2 (exchange of documents)
- Singapore:
 - Direction No. 3 (discovery of electronic documents)

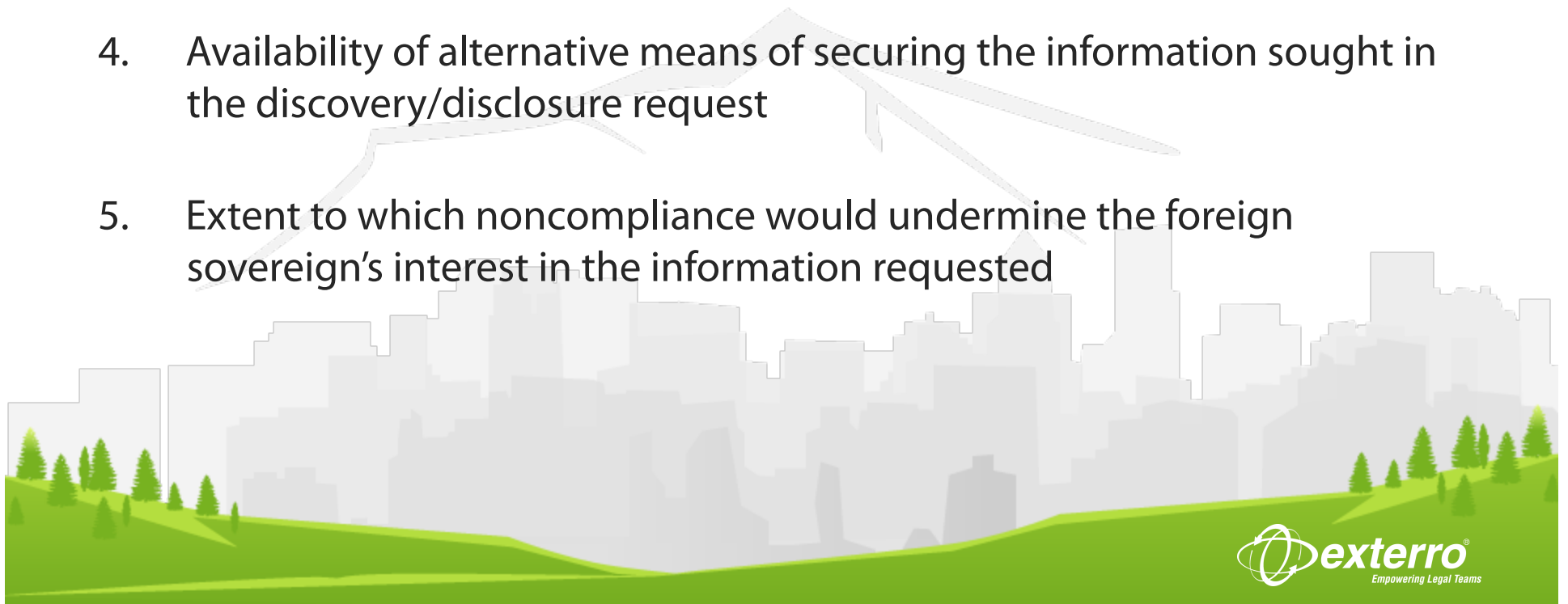
FUSION11 Hague Convention vs. FRCP

- The five factor test in The Restatement (Third) of Foreign Relations Law Section 442(2)(a) is :
 - 1) “Relevant to any comity analysis”
 - 2) In determining whether federal courts should utilize Hague procedures rather than the Federal Rules
 - *Societe Nationale Industrielle Aerospatiale v. Iowa U.S. District Court*, 53 U.S. 522, 556 (1987).



FUSION11 Five-Factor Test

1. Significance of the discovery/disclosure to issues in the case
2. Degree of specificity of request
3. Whether the information originated in the jurisdiction from which it is being requested
4. Availability of alternative means of securing the information sought in the discovery/disclosure request
5. Extent to which noncompliance would undermine the foreign sovereign's interest in the information requested



FRCP Presumption May Be Changing – Or Not

- Until 2008: Most U.S. courts held that the Federal Rules were to be followed, in the face of Protective Order motions citing Blocking Statutes, on the ground that these provisions were rarely enforced.
 - See, *Straus v. Credit Lyonnaise*, 242 F.R.D. 199 (E.D.N.Y. 2007)
- January, 2008: *In re Avocat Christopher X*: French Supreme Court affirms criminal conviction arising from California *Executive Life* litigation
- But see, *In re Global Power* (2009):
 - Delaware court holds no real threat of Blocking Statute enforcement (without citing *Christopher X*). Contra: *In re Payment Card* (EDNY)

FUSION11 Hope for Common Ground?

- European Commission Working Party 29 “1/2009 Working Document” On Pre-Trial Discovery For Cross-Border Civil Litigation” (WP158):
 - Acknowledges need for understanding between common law and civil law jurisdictions
- CNIL Opinion August 2009 on data transfer
- Working Document 158 cites, in several places, *The Sedona Conference® Framework for Analysis of Cross-Border Discovery Conflicts* (available at www.thesedonaconference.org)
- Sedona International e-Discovery Best Practices Commentary is in draft



FUSION11 WP 158: Minimizing the Intrusion?

- Filtering activities before disclosure in U.S. is to be carried out in Europe (p. 11)
 - Separate infrastructure required (hardware + software)
- Filtering carried out by independent trustee instead of other parties (p. 11)
 - Redaction of “sensitive” personal data and irrelevant material (requires input of U.S. counsel)
- Anonymizing personal data in a first step if practicable
- Early involvement of internal data protection officers (p. 11)
- *See Also*, CNIL (France) Opinion August 2009 by same author

U.S. - Form Legal Hold in Europe? Not So Fast

“There may however be a further difficulty where the information is required for additional pending litigation or where future litigation is *reasonably foreseeable*. *The mere or unsubstantiated possibility that an action may be brought before the US courts is not sufficient.*” (WP 158 at 8; emphasis supplied)



FUSION11 There's More

- Many countries (i.e. Brazil, Korea, Japan) require deletion of personal data after the purpose for which it was collected has been completed
- Concept of “Discovery” does not exist in Civil-Law jurisdictions. Preservation for discovery, then, is an alien concept
- Broad US-style legal hold notice offends Civil-Law concept of narrowly-tailored disclosure
- Tracking legal holds, where names of custodians and their responses are forwarded to US, may violate local E.C. privacy directive enabling legislation



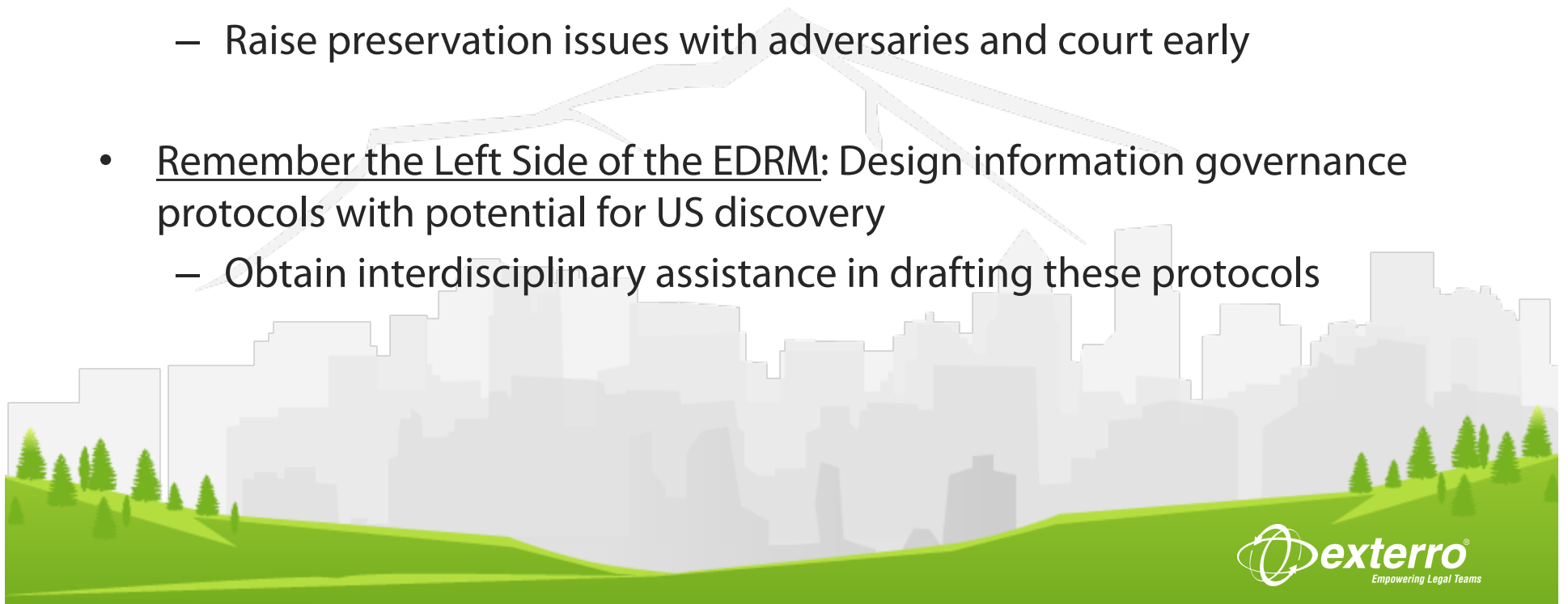
inFUSION11 Best Practices: Path Through the Thicket

- Assemble the legal hold team:
 - Local counsel
 - Experienced US counsel
 - Local IT/records management resources and counsel
- Tailor the legal hold notice and scope to local requirements



Further Along the Path Through the Thicket

- For Defensibility:
 - Assess how tracking hold notices may be accomplished in compliance with privacy laws while meeting Pension Committee, ER. AL., standards
- Be Proactive:
 - Raise preservation issues with adversaries and court early
- Remember the Left Side of the EDRM: Design information governance protocols with potential for US discovery
 - Obtain interdisciplinary assistance in drafting these protocols



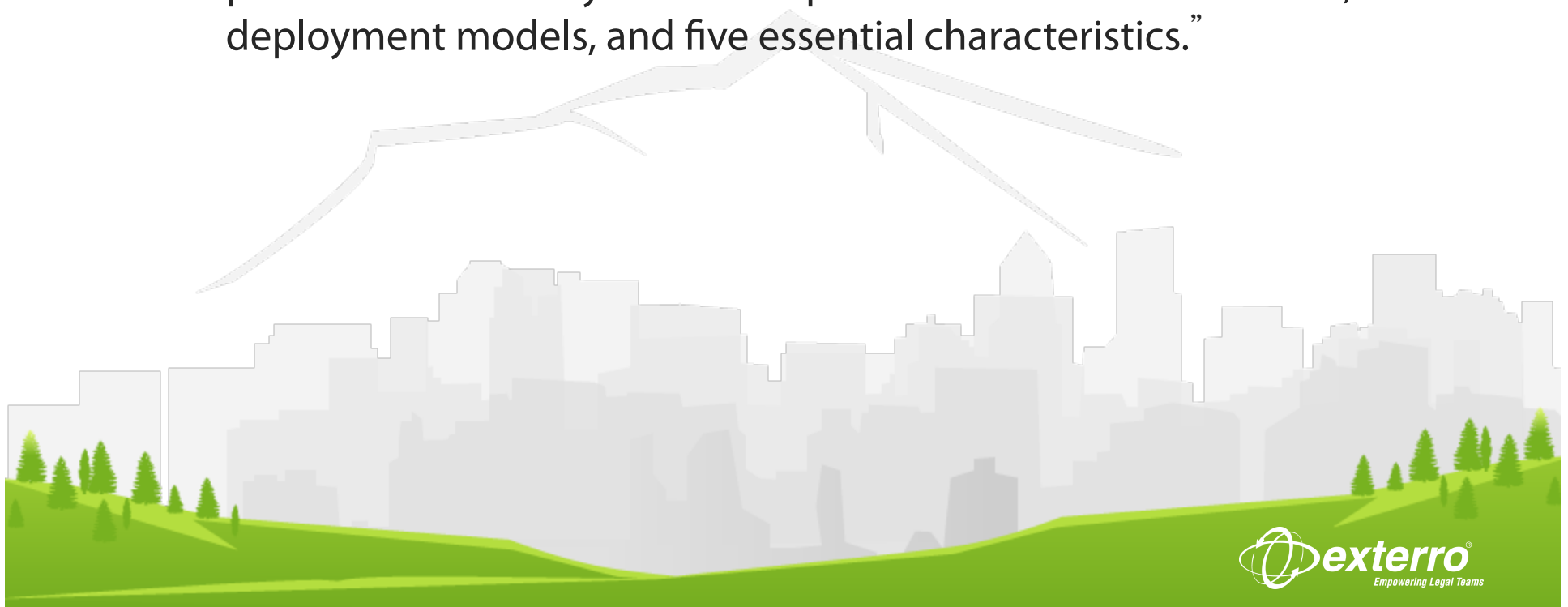
What are Permissible Cross-Border Transfer Methods?

- Consent of Data Subject/Notice (where permissible)
- U.S. Safe Harbor: Certification that entity will abide by certain privacy principles
 - Approved by all EEA states
 - Yearly re-certification required
- Model Contract Clause Agreements: EC Privacy Protocol Clauses
- Binding Corporate Rules: Global code of conduct (recently approved as “toolkit”) by EC

*Caveat: May not suffice for personal data used in litigation (i.e., Blocking Statutes)

FUSION11 The Cloud

- NIST Definition:
 - “Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of three service models, four deployment models, and five essential characteristics.”



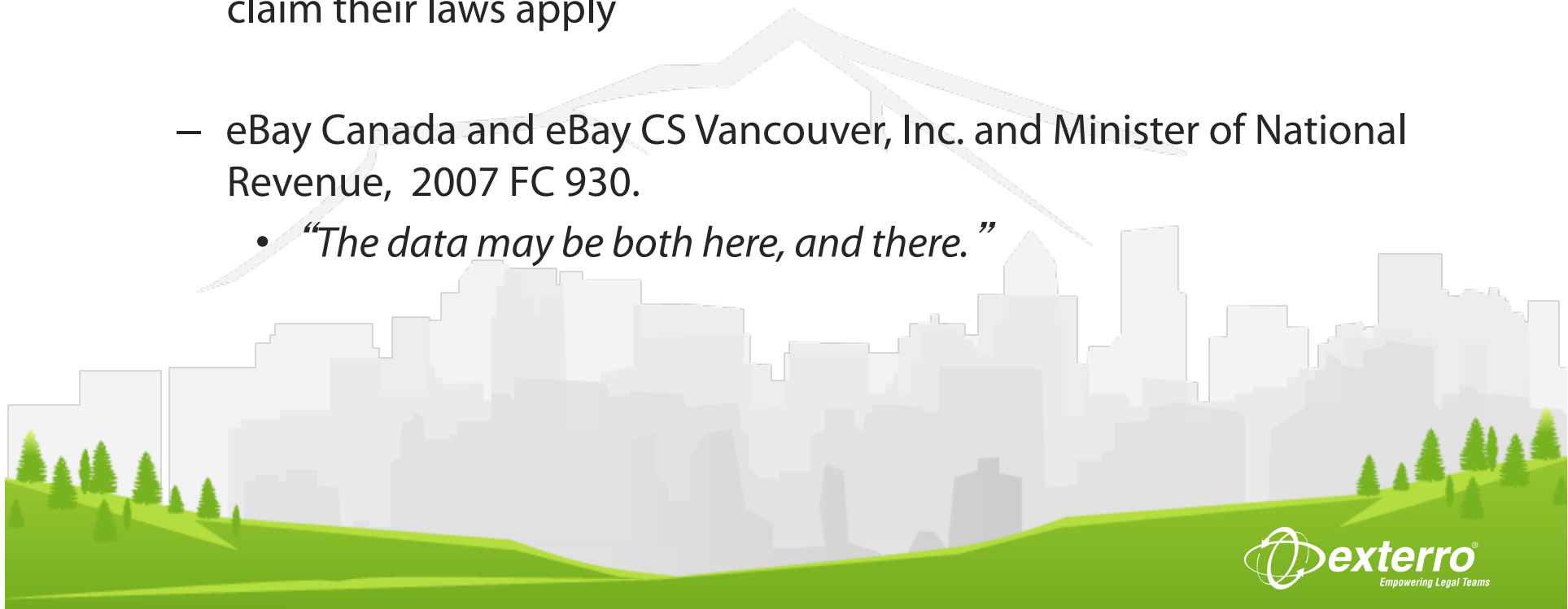
inFUSION11 Cloud: English Definition

- Computing services available from anywhere
 - Applications are accessed from the Internet; use can be metered
 - Applications and/or storage reside outside the four corners of the machine



FUSION11 Cloud: Whose Law Applies?

- Answer: Unknown
 - In cloud, server locations are not known; servers may be in many locations
 - Data is often in many places simultaneously; many countries may claim their laws apply
 - eBay Canada and eBay CS Vancouver, Inc. and Minister of National Revenue, 2007 FC 930.
 - *“The data may be both here, and there.”*



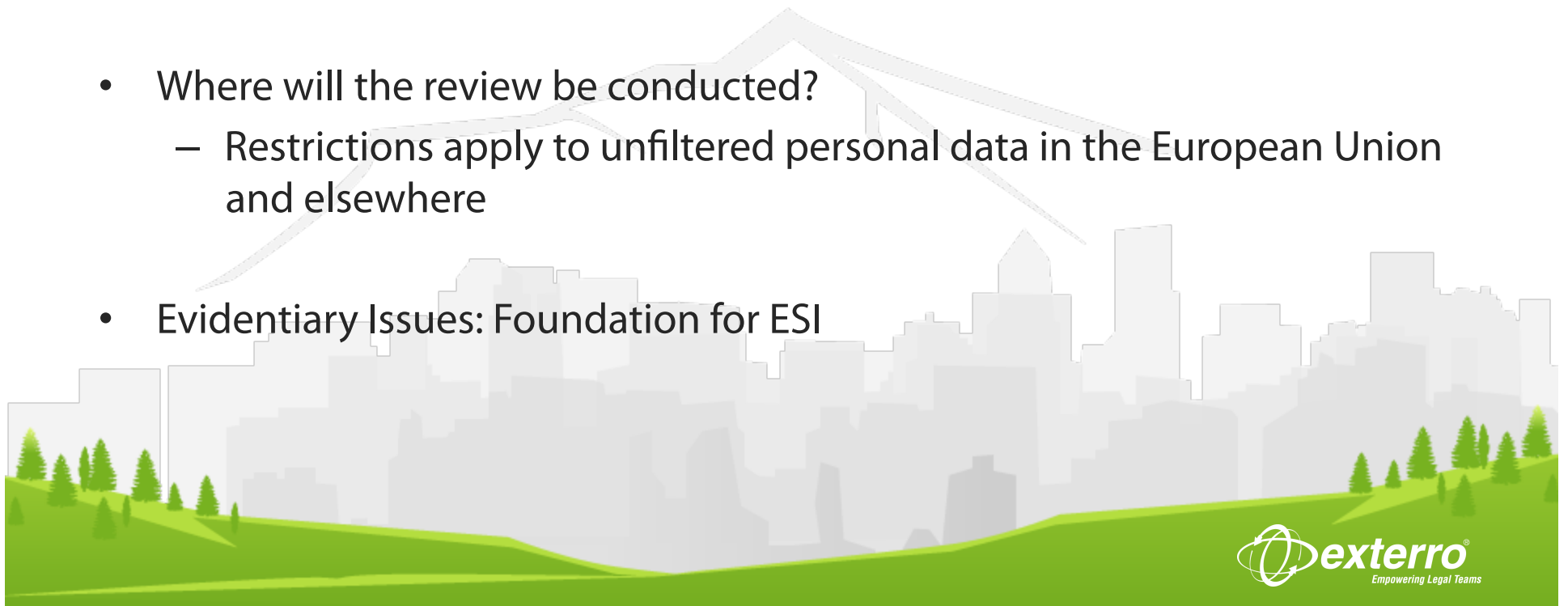
Discovery of Cloud Data Originating Outside US

- Privacy laws, data protection laws and blocking statues may impede discovery
 - Server locations may be an issue.
 - See, *Columbia Pictures v. Bunnell* (data with company in Netherlands but servers in U.S.)
- Germany:
 - DPA of Schleswig-Holstein announced sending data to cloud violates German Data Privacy Act **unless** servers are within borders of Germany



FUSION11 Collection and Review

- How collect data from the provider?
- Does the SLA provide for collection methods and timing?
 - Examples: Format (Native vs. TIFF), metadata preservation
- Identification of data and search modalities
- Where will the review be conducted?
 - Restrictions apply to unfiltered personal data in the European Union and elsewhere
- Evidentiary Issues: Foundation for ESI



FUSION11 Additional Concerns

- Complex pre-trial discovery slows down the case
- Judges frequently have outdated equipment, reduced staff and little real-world experience with ESI
- “The technology of the digital revolution is forbidding to most lawyers, who after all went to law school because they could not do math or science.” Goode, Steven, *The Admissibility of Electronic Evidence*, 29 Rev. Litig. 1 (2009)
- Most lawyers as a result, **DO NOT ADEQUATELY EDUCATE THE COURT;** they do not give the court the basis for favorable rulings



FUSION11 So Now What?

1. Plan Before Collection

- What is needed?
- Where is it (Cloud? Servers? Laptops?)
- Is it protected?
- Are there data protection agreements?
- What are the language issues?
- Permissions/notifications needed?
- Is it here already and, if so, is onward transfer permitted?
- Where should data room be established?
- What are the protocols needed for on-site initial review?



FUSION11 So Now What?

2. Assemble the Collection Team

- Client representatives in U.S. and host country
- Local counsel
- Experienced cross-border discovery U.S. outside counsel
- Third-party consultant

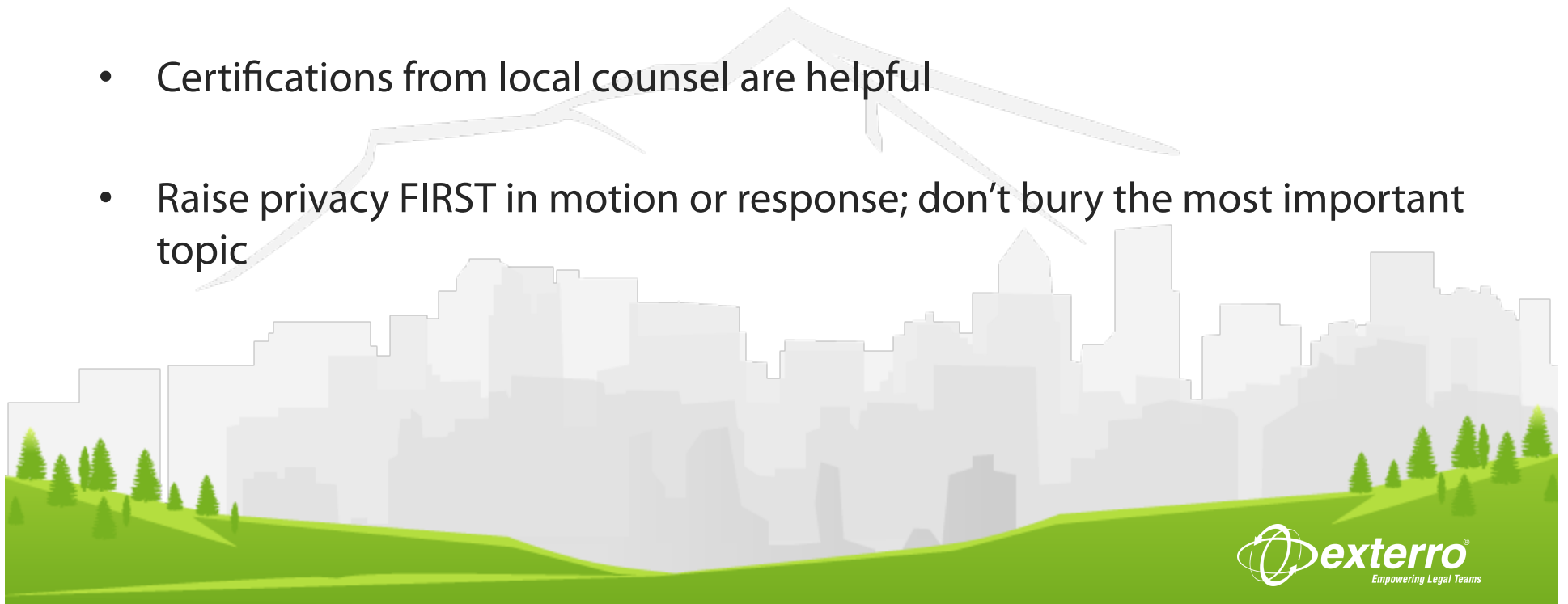
3. Make the process defensible here and in the host country

- Local counsel should advise whether local data protection authority requires permission, notice, or neither
- There will usually be some risk but, with adequate protocols and documentation of process, it can be reduced to an acceptable level



FUSION11 Leave a Legacy: Educate the Court

- Do NOT assume judges are knowledgeable about non-U.S. law or your client's dilemma, "Do I go to jail here or there?"
- Raise cross-border issues early
 - R. 26(f) Conference, *and* Rule 16 Scheduling Conference.
 - Resolution may be possible without motion practice
- Certifications from local counsel are helpful
- Raise privacy FIRST in motion or response; don't bury the most important topic



FUSION11 Questions?

For more information, contact:

Kenneth N. Rashbaum, Esq.

Rashbaum Associates, LLC

(212) 421-2823

krashbaum@rashbaumassociates.com

www.rashbaumassociates.com

© 2011 Exterro, Inc. All rights reserved.

THIS DOCUMENT IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY AND IS NOT INTENDED AS ADVERTISING. ALL WARRANTIES RELATING TO THE INFORMATION IN THIS DOCUMENT, EITHER EXPRESS OR IMPLIED, ARE DISCLAIMED TO THE MAXIMUM EXTENT ALLOWED BY LAW. THE INFORMATION IN THIS DOCUMENT IS SUBJECT TO CHANGE WITHOUT NOTICE.

