Three statements, and three main issues

Data Protection and Security on the Web

ESWC-2014

Heraklion,

pompeu.casanovas@uab.cat

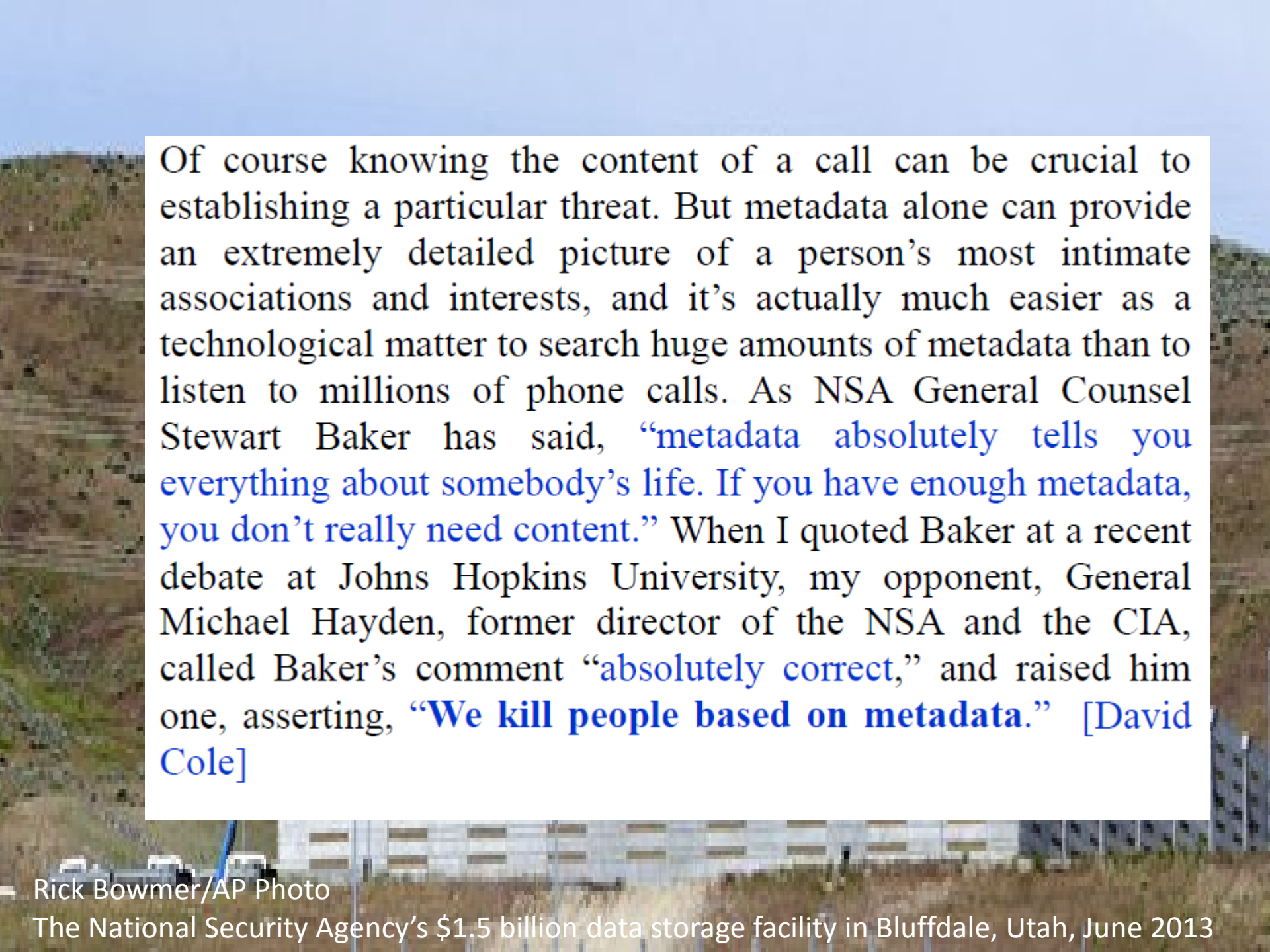
pompeu.casanovas@rmit.edu.au

IoT Commission Expert Group: Six Challenges for the Development of the IoT

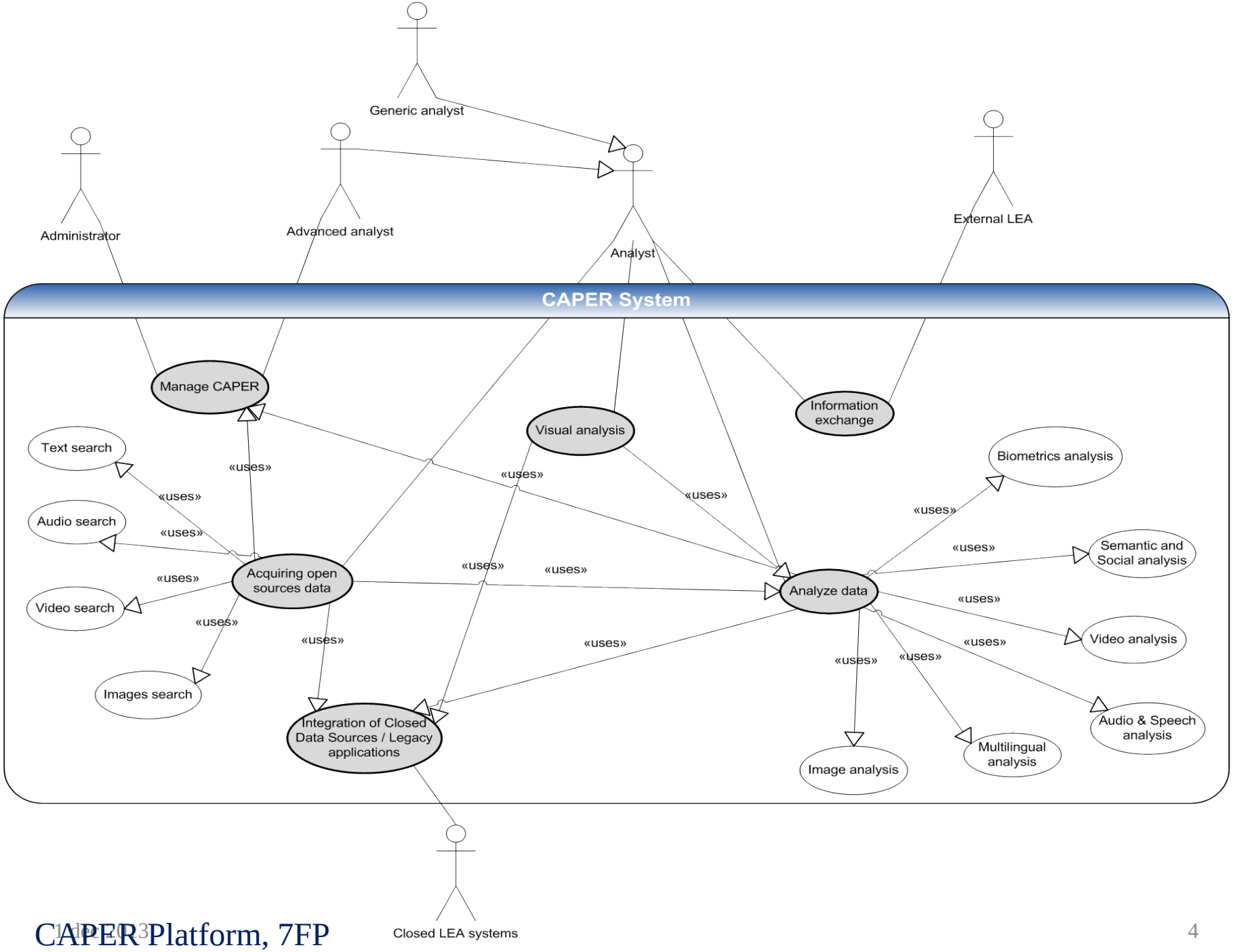
1. Identification
2. Privacy and data protection and security
3. Architectures
4. Ethics
5. Standards
6. Governance

Europe's policy options for a dynamic and trustworthy development of the Internet of Things SMART 2012/0053 (Rand Corporation)

Of course knowing the content of a call can be crucial to establishing a particular threat. But metadata alone can provide an extremely detailed picture of a person's most intimate associations and interests, and it's actually much easier as a technological matter to search huge amounts of metadata than to listen to millions of phone calls. As NSA General Counsel Stewart Baker has said, "metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content." When I quoted Baker at a recent debate at Johns Hopkins University, my opponent, General Michael Hayden, former director of the NSA and the CIA, called Baker's comment "absolutely correct," and raised him one, asserting, "**We kill people based on metadata**." [David Cole]



Rick Bowmer/AP Photo
The National Security Agency's $1.5 billion data storage facility in Bluffdale, Utah, June 2013


Generic analyst
Administrator
Advanced analyst
Analyst
External LEA
CAPER System
Manage CAPER
Visual analysis
Information exchange
Text search
Audio search
Video search
Images search
Acquiring open sources data
Integration of Closed Data Sources / Legacy applications
Analyze data
Biometrics analysis
Semantic and Social analysis
Video analysis
Audio & Speech analysis
Multilingual analysis
Image analysis
«uses»
Closed LEA systems

Three hot topics

- legal treatment and effects of metadata (identity meta-system layer of the Internet)
- the idea of a global citizenship or digital neighborhood approach to assign, protect and manage fundamental rights (refining the traditional "subject of rights" drawn under the national rule of law)
- Implementing Protection by Design Principles (PbD) into security issues (Security by Design)

PRINCIPLES OF FAIR INFORMATION PRACTICES (FIPs)

1. *Openness and transparency*	There should be no secret record keeping. This includes both the publication of the existence of such collections, as well as their contents.
2. *Individual participation*	The subject of a record should be able to see and correct the record.
3. *Collection limitation*	Data collection should be proportional and not excessive compared to the purpose of the collection.
4. *Data quality*	Data should be relevant to the purposes for which they are collected and should be kept up to date.
5. *Use limitation*	Data should only be used for their specific purpose by authorized personnel.
6. *Reasonable security*	Adequate security safeguards should be put in place, according to the sensitivity of the data collected.
7. *Accountability*	Record keepers must be accountable for compliance with the other principles.

i-SWRM, n-SWRM

FIPs. Source: Langheinrich (2001)