Unit 5- Privacy Policy Languages

- **Most consumers are sensitive to privacy issues when conducting business online. Protecting information by enforcing security and privacy practices internally is a way for organizations to increase business by building trust with such consumers.**

- **Many privacy languages are available for representing policies, but they tend to use formats convenient to their implementations, and there is no single framework or metric to analyze and evaluate the effectiveness of these languages**.

- **Privacy policy languages can help with several of the stages involved in managing privacy policies (writing, reviewing, testing, approving, issuing, combining, analyzing, modifying, withdrawing, retrieving and enforcing policy) .**

- **Privacy policy languages were designed to express the privacy controls that both organizations and users want to express. Most of the privacy policy languages were designed for specific purposes with specific features and characteristics. Most of the initiatives for designing these languages have occurred in the last ten years.**

- In 1997, the World Wide Web Consortium (W3C) began development of the **Platform for Privacy Preferences Project (P3P)** to express website privacy policies in machine-readable format

- A **P3P Preference Exchange Language (APPEL)** was also designed by W3C in 1997 to express an individual's privacy preferences, to query the data represented by P3P, and to make decisions accordingly

- **CPExchange** was developed in 2000 to facilitate business-to-business communication about privacy policies

- Later, the industry felt the need for languages to express the internal privacy policies of the organizations themselves.
    - With that goal IBM designed the **Enterprise Privacy Authorization Language** (EPAL) in 2003 [18].

- During the same period a consortium of organizations joined to design the **eXtensible Access Control Markup Language (XACML)** for expressing both privacy and security policies in a machine readable format.

- There were other initiatives such as DPAL [3], and XPref [1] in 2003 and 2004.

ACL→ Access Control Language

SAML → **Security Assertion Markup Language-** an XML-based markup language for security assertions (statements that service providers use to make access-control decisions).

XACML → eXtensible Access Control Markup Language → The standard defines a declarative fine-grained, attribute-based access control policy

XACL→ XML Access Control Language → aims at providing XML documents with a sophisticated access control model and access control

P3P→ Platform for Privacy Preferences Project (P3P) → an obsolete protocol allowing websites to declare their intended use of information they collect about web browser users.

APPEL-- P3P Preference Exchange Language

Sophisticated ACL	Enterprise	SAML, XACML, XACL
	User	XACML
Web	Enterprise	P3P
	User	APPEL, XPref
Enterprise		CPExchange, PRML, E-P3P, EPAL, DPAL
Context Sensitive	Enterprise	Geo-Priv, Rei
	User	Geo-Priv

Figure 1: Classification of the privacy policy languages based on the situation in which the languages can be used. Where E represents the Enterprise and U represent User category. We present the enterprise languages separately

1. *Sophisticated Access Control Languages* (SACL): SACL includes languages that were designed and developed based on Role Based Access Control (RBAC). SAC languages are mostly implemented for security policies and maintained by system administrators (e.g., XACML). In addition to representing security policies, SAC languages can also represent privacy policies.

2. *Web Privacy Policy Languages*: This category includes the languages which are helpful in representing some form of human-readable privacy policies on the Internet in machine-readable formats (e.g., P3P).

3. *Enterprise Privacy Policy Languages*: A number of languages have been designed to represent the internal policies of an enterprise, which would help the organization to perform the actions as stated in the privacy policies (e.g., EPAL). These languages are mostly used for internal purposes and they are more fine-grained than the web privacy policy languages.

4. *Context Sensitive Languages*: Since the context information can provide a personalized service, some languages were designed to represent policies that take into consideration context information. The information that is used for providing these services is very sensitive. These languages make use of the semantic web technologies for representing the policies (e.g. Geopriv).

Three of the above categories (except for enterprise privacy policy languages) can be further sub-categorized on the basis of 'whose information is being represented in the machine-readable format?'Using this information we classify the languages further into two categories:

1. *User*: This class of languages helps in representing user's privacy preferences in a machine-readable format (e.g., APPEL, XPref). Through these languages, users can express their preferences in a set of preference rules (called a ruleset), which can then be used by their user agent to make automated or semi-automated decisions regarding the acceptability of machine-readable privacy policies.

2. *Enterprise*: This class of languages helps in representing the enterprise privacy policies in a machine-readable format (e.g., XACML and EPAL).