**Relevance of COEL to OASIS sponsor organisations**

The organisations that support existing IoT and Privacy-by-Design standards initiatives have interests in several areas:

* Security (IT and more generally)
* Intelligence & risk (in the IT area)
* Digital identity
* Connected devices
* Connected physical infrastructure
* IT / cloud infrastructure
* Compliance & trust
* Connectivity & telecommunications
* Data & data analytics

All in business-to-business applications such as health, smart cities, digital business, energy, military, government & education.

To show the relevance of our work, we must describe the benefits of COEL to their organisations and the other technical committees they support using the terms above. We should also demonstrate the links to the overall OASIS mission.

The other OASIS IoT and Privacy-by-Design standards initiatives focus on the following topics:

* Machine to machine business messaging
* Security
* Intelligence
* Identity
* Privacy models

COEL is uniquely person-centric in this mix and represents a complete privacy model use case. In many cases, COEL-encoded data will represent content (or payload) for these other standards. In the area of identity, our pseudonymisation framework is highly relevant to secure key mechanisms and we provide a universal mechanism coding behavioural attributes. Overall, we will need to emphasise the role of COEL in connecting real-world, observable events about people into this digital (IT) sphere.

We must focus on the normative elements of the specification from an engineer's perspective. Coelition tends to talk about the non-normative elements of privacy-by-design while COEL must explain how the normative sections support privacy-by-design. Coelition talks about business impacts and the creation of an ecosystem – COEL must be more technical and address wider integration / interoperability.

The ultimate benefit of data portability has driven the creation and development of the specification but has been under-represented in recent copy.

**First drafting notes**

COEL is a business-to-business technology specification that helps organisations to understand what we do as humans and what we might do next. The specification promotes behavioural data portability as means to drive innovation, reduce costs and maximise the value of data in a framework that can be trusted by individuals and is compatible with the needs of regulators in a wide range of jurisdictions around the world.

The COEL specification will be relevant to any organisation that collects and/or analyses data about individuals including their interactions with digital infrastructure and IoT devices. This may be in the provision of personalised services to the individual or for the assessment of identity and security risks.

Key features of the specification:

* The COEL roles framework provides a privacy-by-design governance structure for pseudonymous data about people's real-world, observable behaviours. The purpose of both the pseudonymisation-at-source and structured role definitions is to enhance security.
* The COEL event coding (Atoms) provides a syntactic structure for recording, transmitting, analysing any observable human behavioural event. The resulting data is micro-structured – preserving the insight potential of unstructured data while providing the audit and compliance benefits of structured data. Each Atom is an independent record of an event, facilitating the creation insight from multiple sources with no data transformations required. These Atoms, and the real-word events they encode, become behavioural attributes in identity systems and evidence in intelligence systems.
* The Classification of Everyday Living (COEL) data model is a unique and extensible hierarchical taxonomy of human behaviours. It provides the basis for semantic interoperability across platforms, languages and cultures.
* The interfaces allow platforms to integrate using JSON over HTTPS for all interactions. The specification allows for many types of data storage constructs – centralised, personalised or distributed. The delivery of data from IoT devices and connected infrastructures is as lightweight as possible to ensure bandwidth, connectivity or local processing power are not limitations for adoption.
* The specification has a number of embodiments in the form of dedicated devices, mobile apps, web interfaces and data warehouses which provide evidence of use. Sample code in the specification is drawn from these real world implementations.

**Other OASIS IoT/MM Committees**

[OASIS Advanced Message Queuing Protocol (AMQP) Bindings and Mappings (AMQP-BINDMAP) TC](https://www.oasis-open.org/committees/amqp-bindmap)

Defining bindings and mappings of AMQP wire-level messaging protocol for real-time data passing and business transactions

[OASIS Advanced Message Queuing Protocol (AMQP) TC](https://www.oasis-open.org/committees/amqp)

Defining a ubiquitous, secure, reliable and open internet protocol for handling business messaging.

[OASIS Message Queuing Telemetry Transport (MQTT) TC](https://www.oasis-open.org/committees/mqtt)

Providing a lightweight publish/subscribe reliable messaging transport protocol suitable for communication in M2M/IoT contexts where a small code footprint is required and/or network bandwidth is at a premium.

[OASIS Open Building Information Exchange (oBIX) TC](https://www.oasis-open.org/committees/obix)

Enabling mechanical and electrical control systems in buildings to communicate with enterprise applications

**Other OASIS Privacy-by-Design Committees**

[Cyber Standards Council](https://www.oasis-open.org/committees/cyber-council)

The voice of the cybersecurity user community

[OASIS Biometric Services (BIOSERV) TC](https://www.oasis-open.org/committees/bioserv)

Developing open standards that facilitate the use of biometrics and biometric operations over a service-oriented architecture

[OASIS Cross-Enterprise Security and Privacy Authorization (XSPA) TC](https://www.oasis-open.org/committees/xspa)

Enabling the interoperable exchange of healthcare privacy policies, consent directives, and authorizations

[OASIS Cyber Threat Intelligence (CTI) TC](https://www.oasis-open.org/committees/cti)

Supporting automated information sharing for cybersecurity situational awareness, real-time network defense, and sophisticated threat analysis

[OASIS Electronic Identity Credential Trust Elevation Methods (Trust Elevation) TC](https://www.oasis-open.org/committees/trust-el)

Defining a set of standardized protocols to elevate trust in an electronic identity

[OASIS PKCS 11 TC](https://www.oasis-open.org/committees/pkcs11)

Enhancing PKCS #11 standard for cryptographic tokens controlling authentication information (personal identity, cryptographic keys, certificates, digital signatures, biometric data)

[OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC](https://www.oasis-open.org/committees/pbd-se)

Enabling privacy to be embedded into IT system design and architecture

[OASIS Privacy Management Reference Model (PMRM) TC](https://www.oasis-open.org/committees/pmrm)

Providing a guideline for developing operational solutions to privacy issues

OASIS is a nonprofit consortium that drives the development, convergence and adoption of open standards for the global information society.

OASIS promotes industry consensus and produces worldwide standards for security, Internet of Things, cloud computing, energy, content technologies, emergency management, and other areas. OASIS open standards offer the potential to lower cost, stimulate innovation, grow global markets, and protect the right of free choice of technology.

OASIS members broadly represent the marketplace of public and private sector technology leaders, users and influencers. The consortium has more than 5,000 participants representing over 600 organizations and individual members in more than 65 countries.

**Founder & sponsor organisations**

|  |
| --- |
| * [Cryptsoft](http://cryptsoft.com/)
* [IBM](http://www.ibm.com/)
* [360 Enterprise Security Technology Corporation ltd.](http://www.360.net)
* [Accenture, LLP](http://www.accenture.com/us-en/security-index)
* [Adobe Systems](http://www.adobe.com)
* [ADP Global Security Organization](http://www.adp.com)
* [Alfresco Software Inc.](http://www.alfresco.com/)
* [Anomali Incorporated](http://www.anomali.com)
* [Arbor Networks Inc.](http://www.arbornetworks.com)
* [CA Technologies](http://www.ca.com/)
* [CIB labs GmbH](http://www.cib.de)
* [Cisco Systems, Inc.](http://www.cisco.com/)
* [Connectis](http://www.connectis.nl)
* [Dell](http://www.dell.com)
* [Dutch National Cyber Security Centre (Dutch NCSC)](http://www.ncsc.nl)
* [EclecticIQ](http://www.eclecticiq.com)
* [FireEye, Inc.](http://www.fireeye.com)
* [ForeScout Technologies, Inc.](http://www.forescout.com)
* [Fornetix](http://www.fornetix.com)
* [Fujitsu](http://www.fujitsu.com/)
* [GrammaTech](http://www.grammatech.com)
* [Hancom Secure](http://en.hsecure.co.kr)
* [Hewlett Packard Enterprise (HPE)](http://www.hpe.com)
* [Hitachi](http://www.hitachi.com)
* [Huawei Technologies](http://www.huawei.com)
* [iboss, Inc.](http://www.iboss.com)
* [Intel](http://www.intel.com/)
* [IXIASOFT](http://www.ixiasoft.com)
* [Jahia Solutions Group SA](http://www.jahia.com)
* [KRYPTUS Information Security S/A](http://www.kryptus.com)
* [Logius](http://www.logius.nl)
* [LookingGlass Cyber Solutions](http://www.lookingglasscyber.com)
* [McAfee, LLC](https://www.mcafee.com/us/index.html)
* [Micro Focus](http://www.microfocus.com)
* [Microsoft](http://www.microsoft.com)
* [NC4](http://www.nc4.com)
* [NEC Corporation](http://www.nec.com/)
* [NetApp](http://www.netapp.com)
* [Netcracker Technology](http://www.netcracker.com)
* [New Context Services, Inc.](http://www.newcontext.com)
* [Oracle](http://www.oracle.com/)
* [P6R, Inc.](http://www.p6r.com)
* [Progress Software](http://www.progress.com/)
* [PTC](http://www.ptc.com/)
* [QuintessenceLabs](https://www.quintessencelabs.com/)
* [Red Hat](http://www.redhat.com/)
* [RIPS Technologies](http://www.ripstech.com)
* [SafeNet](http://www.safenet-inc.com/)
* [SAP](http://www.sap.com/)
* [SDL International](http://www.sdl.com/)
* [Software AG](http://www.softwareag.com/)
* [TELUS](http://www.telus.com)
* [Thales e-Security](http://www.thales-esecurity.com)
* [ThreatQuotient, Inc.](http://www.threatq.com)
* [Trend Micro, Inc.](http://www.trendmicro.com)
* [TruSTAR Technology](http://www.trustar.co)
* [Tyler Technologies](http://www.tylertech.com)
* [UnboundTech](http://www.unboundtech.com)
* [US Department of Defense (DoD)](http://www.disa.mil/)
* [US NIST](http://www.nist.gov)
* [US Veterans Health Administration](http://www.va.gov)
* [VeriSign](http://www.verisign.com)
* [VMware, Inc.](http://www.vmware.com)
 |

**Sponsor organisations on multiple IoT / Privacy-by-design committees**

|  |
| --- |
| [Cisco Systems](http://www.cisco.com/) |
| [Veterans Health Administration](http://www.va.gov/) |
| [360 Enterprise Security Group](http://www.360.net/) |
| [Dell](http://www.dell.com/) |
| [IBM](http://www.ibm.com/) |
| [Microsoft](http://www.microsoft.com/) |
| [NIST](http://www.nist.gov/) |
| [Red Hat](http://www.redhat.com/) |
| [Thales e-Security](http://www.thales-esecurity.com/) |
| [Cryptsoft Pty Ltd.](http://www.cryptsoft.com/) |
| [Intel Corporation](http://www.intel.com/) |
| [LookingGlass](http://www.lookingglasscyber.com/) |
| [McAfee](https://www.mcafee.com/us/index.html) |
| [NC4](http://www.nc4.com/) |
| [New Context Services, Inc.](http://www.newcontext.com/) |
| [Oracle](http://www.oracle.com/) |
| [Software AG](http://www.softwareag.com/) |
| [TELUS](http://www.telus.com/) |
| [ThreatQuotient, Inc.](http://www.threatq.com/) |
| [Trend Micro](http://www.trendmicro.com/) |
| [US Department of Defense (DoD)](http://www.disa.mil/) |

**COEL Overview from OASIS website**

The OASIS COEL specification provides a privacy-by-design framework for the collection and processing of behavioural data. It is uniquely suited to the transparent use of dynamic data for personalised digital services, IoT applications where devices are collecting information about identifiable individuals and the coding of behavioural data in identity solutions. The specification pseudonymises personal data at source (IDA) and maintains a separation of different data types with clearly defined roles & responsibilities (RPE) for all actors. All behavioural data are defined as event-based packets (BAP). Every packet is connected directly to an individual and can contain a summary of the consent they provided for the processing of the data. A combination of a taxonomy of all human behaviours (COEL) and the event-based protocol provide a universal template for data portability. Simple interface specifications (MMI & PQI) enforce the separation of roles and provide system-level interoperability.

**Original Charter**

Statement of Purpose

The purpose of the COEL TC is to create the standards necessary for the successful formation and growth of a business ecosystem aimed at providing personalised services.

Personalised services, such as those that emerge from loyalty card schemes or branded wearable devices, form a large and growing market. However, these solutions exist only as narrow, vertically-integrated propositions. As such, information exchange between various domains is hampered and the cost of creating complete vertical solutions restricts uptake to large players, excluding the small to medium enterprise market and the public sector (where personalised services could offer the greatest human value). All these solutions share one thing, the need to understand what we do as humans and what we might do next. This behavioural aspect of personalised services is at the core of the COEL TC aims.

Any system or device that collects data for the provision of personalised services is likely to be handling information that individuals would classify as personal or sensitive. The objective of the COEL TC in this domain will be to create transparent technical frameworks that respects the data of individuals, can be trusted by individuals and are compatible with the needs of regulators in a wide range of jurisdictions.

Building the infrastructure for these services requires many distinct capabilities, including capture of behavioural data, a comprehensive framework for describing behaviour, secure transmission and storage of this data, maintenance of a separation between this data and directly identifying personal information, the development of complex data analytics to interpret the data, and imaginative strategies to deliver value to both business and the end user through personalised service offerings. Standards and best practices are required to address each of these so that an ecosystem can function in which each actor focuses on their strengths providing value to the rest of the ecosystem.

The COEL TC will develop and publish the standards necessary to realise an ecosystem for personalised services. The specific projects targeted by this TC are:

* development of a taxonomy of human activity (the Classification of Everyday Living),
* a format and protocol for the representation, transmission, storage and referencing of individual instances of human behaviour (called Behavioural Atoms) and their associated context,
* an ecosystem architecture delineating the roles and responsibilities of ecosystem players, and
* a set of technical requirements for implementing this architecture.

In an ecosystem of this type, business-to-business interactions can be defined and conducted to share data in appropriate ways about personal behaviours (such as consumer brand consumption). The source of this model for a business-to-business ecosystem of this kind is Coelition <coelition.org> (see the Contributions referenced below). Within such an ecosystem, participants could agree to share and/or license consumer-facing brand and behaviour instance data (Behavioural Atoms). A complete specification for the necessary processes for such an ecosystem may include defining intermediary roles, the patterns for interactions among participants, and methods for determining compliance with these specifications.

Audience

The audience for this TC includes any party interested in defining the nature of the Coelition ecosystem, and consensual, privacy-respecting exchanges of human behaviour generally. Most particularly, these projects should be valuable to parties interested in implementation of Behavoural Atom information stores; the development of devices and systems that can identify and create Behavoural Atom data; and those looking to develop services around the data flow of individual and aggregate Behavoural Atom data gathered. Within the scope of the COEL taxonomy, social scientists and psychologists from industry, government or academia may also be interested in participating in this TC.

**Position statement for W3C**

The COEL-TC (<https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=coel>) manages the development of an OASIS Open Standard that implements a privacy-by-design framework for the collection and processing of behavioural data. The standard provides a means to improve interoperability for organisations that seek to create working privacy-by-design systems. Applications built using COEL deliver data privacy and data self determination for individual citizens and consumers, in a way that is fully auditable and easy to check legal compliance.

There are four key technical insights that have been used to build COEL as the basis for the transparent use of dynamic data for personalised digital services, IoT applications where devices are collecting information about identifiable individuals and the coding of behavioural data in identity solutions:

[1] For privacy-by-design applications, we have found that a minimum requirement is to ***pseudonymise personal data* *at source*** and then maintain a strict and auditable separation of different data types with aligned roles & responsibilities for all actors involved.

[2] We have defined new data types based on the expertise of COEL-TC members in digital capture of human behaviourial data. The well defined data types in COEL standard are one of the core means to deliver interoperability for users of the standard. All ***behavioural data are defined as event-based packets***. Every packet is connected directly to an individual and can contain a summary of the consent they provided for the processing of the data. This provides a means to store and process context specific consent using e.g. Kantara CISWG-TC protocols (<https://kantarainitiative.org/groups/ciswg/>) or other consents standards.�

[3] The ***Classification of Everyday Living*** is a holistic, hierarchical taxonomy that sits at the heart of the COEL Standard. For applications that require granular data on everyday human behaviour, we believe the COEL taxonomy provides ***a unique and extensible knowledge base that can deliver semantic harmonisation for personalised services***. The first version of this asset already delivers a high level of harmonised knowledge, and the COEL-TC framework provides a structured means for this to develop in years to come to a broader and richer ontology derived from use cases. An interactive visualisation of the current COEL JSON artefact has been created by ***Coelition*** (<https://coelition.org/>) �to showcase this asset base (<https://coelition.org/business/resources/visualising-life/>). We believe that the combination of the COEL taxonomy of human behaviours, and the event-based data type and data handing protocols, provide a universal template for data portability. We have consciously kept the knowledge that is encoded in the COEL taxonomy independent of the technical infrastructure used for the COEL standard.� �

[4] Privacy-by-design applications cannot be achieved with a pure technical solution. In parallel with the well-defined data types and taxonomy, the COEL approach also ***defines roles & responsibilities for actors who want to use the COEL standard in privacy-by-design implementations***. The COEL Standard describes simple interface specifications that help enforce the separation of roles and provide system-level interoperability.