TDL | Trust in Digital Life

A TDL Working Group Meeting
hosted by
Verizon Enterprise Solutions
Wenckebachweg 123, 1096 AM Amsterdam

verizon

Event Programme

19:30 – 22:30 Wednesday 1 February
Grand Café Ovidius, Spuistraat 137-139, 1012 SV Amsterdam (+31 20 620 8977, ovidius.nl)

09.00 – 10.00 Thursday 2 February
TDL Board Meeting
Wenckebachweg 123, 1096 AM Amsterdam

10:00 – 17.00 Thursday 2 February
TDL Working Group Meeting
Wenckebachweg 123, 1096 AM Amsterdam

Time	Subject
10:00	**Members Update** · Report on discussion and output from November Strategy Review · Feedback from extraordinary General Assembly in January
10:30	**Working Group: Blockchain** · Feedback on the report from the June workshop in The Hague · Discussion on the finalisation of the document Blockchain: Perspective on Research, Technology and Policy · Planning for 2017 including work on papers focusing on specific issues (e.g., privacy; performance, IoT control, or enterprise use, etc.) as well as the next one-day event
11:30	**Coffee**
11:45	**Working Group: Blockchain** *continued*
12:15	**NEW Working Group: Creating Awareness of the Regulatory Landscape Impacting Personal Data for SMEs** *(see below)* Planning for the 2017 work programme including: · A paper setting out guidance and advice for citizens and businesses, particularly SMEs, on how to operate in a best practice approach in a privacy-driven world. · Educational materials that can be taken to industry, startups, SMEs and others to help establish a common and balanced understanding of these critical issues.
12:45	**Lunch**
13:45	**NEW Working Group: Creating Awareness of the Regulatory Landscape Impacting Personal Data for SMEs** *continued*
14:45	**NEW Working Group: Securing Internet-Connected Devices** *(see below)* Planning for the 2017 work programme including: · Collaborative work on a paper setting out insights and recommendations for businesses, governments and citizens · A demonstrator platform for testing IoT devices The results of a small number of technical solutions
15:30	**Coffee**
15:45	**NEW Working Group: Securing Internet-Connected Devices** *continued*
16:30	**Wrap-up**
17:00	**Close**

New Working Group: Creating Awareness of the Regulatory Landscape Impacting Personal Data for SMEs

Problem Statement

The use of personal data in recent years has prompted disruption, initiated digital transformations, increased competition and raised awareness of the issues associated with security, privacy and identity as never before. The market is quickly changing and the responsibilities of companies and their service providers are becoming not only ever more explicit but also are demanding a more balanced approach to the management of personal data. This presents a number of challenges in terms of assigning responsibilities, not least due to new and far-reaching EU legislation that includes the General Data Protection Regulation (GDPR), the Electronic Identification and Trust Services regulation (eIDAS), Anti-Money Laundering 4 (AML4) and Payment Services Directive 2 (PSD2).

The introduction of GDPR in May 2018 will have a significant impact on all companies, including many outside Europe, involved in the processing of EU citizens' personal data. Supervisory authorities will have a number of broad powers including the ability to impose severe penalties for non-compliance. Nevertheless, it's not all doom and gloom, as with new obligations also come opportunities for businesses, especially where there are new data sources. This is especially the case with the role of Fintech and PSD2, and improvements to data portability and mobility, self-sovereign identity and access to global services. In addition, eIDAS presents great opportunities to streamline identity verification and the legally-binding use of e-Signatures.

These legislative changes in the EU have further heightened the need for awareness and focus on the management, security and protection of personal data, especially in a regulatory context. From recent 'right to be forgotten' cases through to data mobility and privacy, these topics are inextricably linked and affect both consumers and businesses alike.

Despite the best efforts of lawyers, consultants, journalists as well as specialist vendors and service providers to spread the word, remarkably few companies are taking steps to prepare, especially for GDPR. Most very large companies either have their own CPO or access to external advisors who can help them with advice. However, this is not the case with SMEs which could remain blissfully unaware of the changes and the consequences until it is too late.

Proposed Solution

Understanding how, why, when and who should leverage personal data is critical especially as new sources of personal data start to open up. Moving beyond social into mobile operators and indeed financial data the opportunities to leverage better, richer, more accurate sources of data than traditionally provided by data bureaux is now here. Empowering consumers and citizens with their personal data is a trend that will only increase over the next few years and will be essential for trust between all these parties.

Working Group Approach & Output

The focus is to be on a practical approach to dealing with the new requirements and responsibilities, designed to support SMEs and innovators dealing with these issues but unfamiliar with the changing legal landscape. Deliverables are to include:

- A paper setting out concise guidance and advice for citizens and businesses, particularly SMEs, on how to operate in a best practice approach in a privacy-driven world.
- Educational materials that can be taken to industry, startups, SMEs and others to help establish a common and balanced understanding of these critical issues.

New Working Group: Securing Internet-Connected Devices

Problem Statement

The recent DDOS attack on Dyn servers by a botnet of ICDs highlighted the vulnerability of unprotected smart devices from malware and other forms of cyber attacks. For many this is just the tip of the iceberg, highlighting the likelihood of many such nightmare scenarios in the future.

The projected massive growth in IoT, from door locks to traffic lights, is both exciting and extremely daunting. By the year 2020, it is estimated that there will be 24 billion connected 'things' worth $1.7 trillion globally with the promise of previously undreamed of convenience which is very enticing. But imagine the consequences as (or when) thousands of driverless 'connected cars' get hacked. Or a smart shower cannot be turned off.

Proposed Solution

While it is apparent that ensuring the correct software is installed on sensors and small devices, this is not an especially useful piece of advocacy. Far more important is to ensure that all devices are running the latest software that support the latest protection. The one huge gap with all these small devices is whether or not they are well-managed; so that if they are not kept up to date, they should be isolated.

Other industry initiatives and technical solutions in this area will abound with the core issues being associated with authentication, consent and compliance . For example, 5G PPP are addressing issues of authentication and when working with SIM manufacturers, no one talks about 'lightweight crypto', although there may be a role for some loss of functionality depending on whether the objective is velocity, size, security, performance, latency etc

One solution would be to provide security quantification for such devices, i.e., making security measurable, using methods based on computational trust. Long term this could lead to an alternative/extension for current certificate authority-based solutions.

Another idea entails providing a means for making mobile devices more trustworthy and controllable representatives of their owners as compared with having them controlled by hardware/operating system/application suppliers and telcos. An extension to this would be to explore the trend towards managing the 'swarms' of devices or the 'mesh of things', not only individual smartphones, surrounding each of us. This approach – coined 'AlterEgo' by TU Darmstadt – is a challenging vision that requires a socio-technical design approach and comprises all the challenges of developing such devices in a secure, trustworthy and transparent manner.

Working Group Approach & Output

This working group will focus on practical recommendations for how businesses, governments and citizens can restore trust in ICDs and prevent the future of IoT being scuppered by hackers.

The intention is to neither provide advice to developers or manufacturers nor produce a gap analysis but rather address some technical solutions as well as broader societal, policy and legislative issues, such as the problems or pain points customers would encounter.

Among the technical solutions would be an exploration of security quantification and the ideas associated with 'AlterEgo'. Deliverables are to include:

- A paper setting out insights and recommendations for businesses, governments and citizens
- A demonstrator platform for testing IoT devices
- The results of a small number of technical solutions

TDL Working Group Meetings

All members of the TDL community are invited to meetings to discuss the content and plans of working groups face-to-face, to define next steps and action points so that content creation can proceed between meetings. Working group leaders are responsible for the agenda, charter, plenary presentations and progress reports as well as the agreed deliverables. These meetings also provide the opportunity to:

- Interact, network, share ideas and visions with the leading organisations in the field of security and trust in ICT, mobile communication and modern technologies;
- Follow presentations from keynote speakers who are specialists in the research of security and future plans of the core elements of TDL;
- Get recognition for the results of the research on a European scale;
- Influence the decisions of European policies concerning TDL through active participation;
- Be part of a dialogue on use cases, law and technology, requirements and technology and business cases.

Venue

Verizon Business address

H.J.E. Wenckebachweg 123, 1096 AM Amsterdam

Contact person

Rob Kroneman, office +31 207116711, mobile +31 6 55787289, rob.kroneman@intl.verizon.com

Accommodation

For hotels and visitor information in Amsterdam, we recommend you go to the IAMSTERDAM - IAMVISITING website.

Directions to Verizon

A taxi from Schiphol airport takes between 15 to 30 minutes depending on traffic and costs approximately €45-50, unless of course you prefer to use Uber. It is considerably less expensive by train *(see below)*.

By public transport

From Schiphol airport, the Intercity train to Amsterdam Central station takes about 14 minutes and costs €5. Then take tram 51 or 54 six stops and get off at Spaklerweg from where it is a ten minute walk to Verizon's office. Alternatively, simply take a taxi from the station to Wenckebachweg 123.

By car

Coming north from the A2 / E35 or from the south east on the A1, take exit 11 – Amesterdam-Amstel and follow Johannes Blookerweg and Wenckebachweg to Duivendrechtsekade in Amsterdam-Oost.