TDL | Trust in Digital Life

Data Protection & Open Banking: Experiences & Expectations

Conference Report

December 2018

Contents

Data Protection & Open Banking: Experiences & Expectations

A one-day TDL conference
with the support of:

Host sponsor:

Platinum sponsor:

Media sponsors:

Side event sponsor:

This two part event organised by Trust in Digital Life, sponsored by NEC Laboratories Europe GmbH and hosted by Jones Day in Brussels over two days in October brought together representatives from the European Commission, businesses, banks, SMEs, vendors and consumer associations to evaluate the experience of implementing, principally two sets of EU regulations, the GDPR and PSD2 from a multi-stakeholder perspective.

The event also played host to two of the Thursday afternoon side events of the 40th International Conference of Data Protection and Privacy Commissioners (ICDPPC).

Speakers, Panelists & Moderators

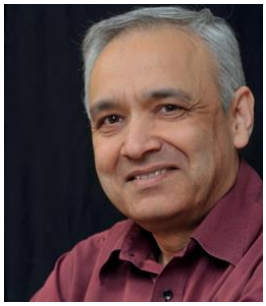
Paul F. Nemitz, Principal Advisor, Directorate-General for Justice and Consumers, European Commission

Paul is Principal Advisor in the Directorate-General for Justice and Consumers of the European Commission. Before, he was Director responsible for Fundamental Rights and Citizenship, the lead director for the reform of the EU data protection legislation, the "Snowden" follow up, the negotiations of the EU-US Privacy Shield and the EU Code of Conduct against hate speech and incitement to violence on the Internet as well as support to exercise fundamental rights, free speech, plurality of the press and democratic engagement.

Before joining DG Justice, he held posts in the Legal Service of the Commission, the Cabinet of Commissioner Nielson, and in the Directorates General for Trade, Transport and Maritime Affairs. He has a broad experience as an agent of the Commission in litigation before the European Courts and he has published extensively on EU law.

Paul was admitted to the Bar in Hamburg and for a short time was a teaching assistant at Hamburg University. He obtained a Master of Comparative Law from George Washington University Law School in Washington, D.C., where he was a Fulbright grantee. He also passed the first and second cycle of the Strasburg Faculty for comparative law, with the support of a grant by the German Academic Exchange Service (DAAD).

He is also a member of the Data Ethics Commission of the German Government and the Global Council in Extended Intelligence; Visiting Professor of Law, College of Europe



Amardeo Sarma, General Manager, Security and Networking Research Division, NEC Laboratories Europe

Amardeo is responsible for research and development in the areas of security, networking and standardization. He is also Chairman of the Trust in Digital Life Association. He has previously worked for Deutsche Telekom and Eurescom and held a Chairman position at the ITU-T. He has published in various areas including software engineering, communication protocols, privacy and identity management. He is an IEEE Senior Member and a member of ACM and AAAS.

Maarten Stultjens, VP Partners Sales, Marketing & Corporate Development, iWelcome

As an entrepreneur in 'scale-up' enterprise-IT companies, Maarten has successfully built international sales and marketing teams from early stage to high growth, scalable and predictive businesses. He is passionate about the potential value of 'digital identities' (IAM) for enterprises.

At iWelcome, he is globally responsible for strategic partners and partner sales, business development, analyst relationships, marketing and product marketing. iWelcome is a game changer in the IAM market. The delivery model of IAM functionality has changed from long lasting on-premise deployments to plug-and-play as-a-service cloud delivery and the focus of IAM has shifted from serving employees to serving consumers and enabling digital transformation. iWelcome today serves blue chip customers across Europe and is acknowledged as product leader in consumer identity and consent management (ranked 'excellent' by Gartner).

Prior to iWelcome, he was co-founder and -owner of BHOLD, a product leader in Identity Governance and Administration. Microsoft acquired BHOLD's technology in 2011 and today it is part of Microsoft's IAM platform.

Jörg Hladjk, Of Counsel, Cybersecurity, Privacy and Data Protection, Jones Day

Leading Jones Day's Cybersecurity, Privacy & Data Protection Practice in Brussels, Jörg advises multinational clients across all industries, with an emphasis on automotive, IT, energy and medical devices. His work covers all areas of EU data protection, such as implementing the GDPR and ePrivacy Regulation compliance programs, data breach preparedness, incident response and handling contentious issues.

Jörg has specific experience in developing strategies for international data transfers, including Binding Corporate Rules and assisting with approval procedures by EU data protection authorities. He chairs the advisory board of Trust in Digital Life and is a co-author of leading EU commentaries. He was a legal expert on a round table during the trilogue negotiations on the GDPR. His practice is recommended in Tier 1 in The Legal 500 EMEA for EU Regulatory: Privacy and data protection (2016-2017) and he is continuously recognized by The International Who´s Who Information Technology Lawyers (2012-2017).

Georgios Kourogiorgas, Data Protection Officer (CIPP/E), Worldline Global

Having trained as a lawyer at the National Kapodistrian University of Athens, Georgios went on to study in Vienna and Leuven before working in government both in Greece and at DG CONNECT in Brussels.

As a Certified Information Privacy Professional/Europe (CIPP/E), Georgios has been Data Protection Officer at Worldline Global, Merchant Services and Terminals for over a year. He is also a member of the BELTUG Privacy Council.

Wendy Grossman, Freelance writer, journalist and blogger,

A graduate from Cornell University, Wendy's credits include work for *Scientific American, The Guardian*, and the *Daily Telegraph*, as well as *New Scientist, Wired* and *Wired News*, and *The Inquirer* for which she wrote a regular weekly *net.wars* column. She edited an anthology of interviews with leading computer industry figures, entitled *Remembering the Future*, published in January 1997 by Springer Verlag.

A Strategic Advisor to Trust in Digital Life, Wendy also sits on the executive committee of the Association of British Science Writers and the Advisory Councils of the Open Rights Group and Privacy International.

Finn Myrstad, Director of Digital Policy and Energy, Norwegian Consumer Council (Forbrukerrådet)

Finn Lützow-Holm Myrstad is the Director of Digital Policy at the Norwegian Consumer Council (NCC), focusing on national and international research and advocacy related to privacy, cyber security, net neutrality, copyright, telecommunication and more. He has led the research and advocacy work relating to terms and conditions in digital services, and has lodged several successful complaints against Apple iCloud, Tinder, Runkeeper and other digital services, exposing security breaches, privacy violations and unfair contract terms.

Finn is also the EU co-chair of the Transatlantic Consumer Dialogue (TACD) Information Society Committee, a network of over 75 leading organisations representing the consumer interest on both sides of the Atlantic. He holds an MSc in Politics and Government of the European Union from the London School of Economics (LSE) and an Executive MBA from Hult International Business School.

Giles Watkins, UK Country Leader, International Association of Privacy Professionals

Giles spent 27 years in finance and technology advisory services, specialising in identity, privacy, security, enterprise architecture and technology due diligence. Giles has held partner positions at both EY and KPMG, building significant global practices in both. Giles also founded the boutique privacy consulting firm, Concentium, in 2010, which was acquired by KPMG in 2014. Giles has sat on the Board of the Open Identity Exchange (OIX) and several identity and security start-ups and was the Technology Chair for the UK Digital Catapult's Personal Data and Trust Network.

Michael Salmony, Executive Advisor to Board of Directors, equensWorldline/Worldline SE/Atos

Michael is Executive Advisor to the Board of Directors of equensWorldline/Worldline SE/Atos, the leader of Europe's payments and transactions service industry and Programme Director of PSD2 programme Founder & CEO Payments Innovation Consulting, specializing in digitisation, payments, digital finance, open banking, PSD2, FinTech, RegTech, InsurTech, cybercrime, transaction strategy, European regulation, innovation management in Europe/Asia/Ocenia Founder and CEO of cross-industry Open Banking forum CAPS (Convenient Access to PSD2 Services).

He was previously IBM Director of Market Development Media and Communications where he managed major projects for the transformation of diverse industries (publishing, TV/radio, utilities, national rail, etc.) through digitisation/eCommerce/ Internet/ multimedia technologies

He is Board-level advisor to major international organisations:

- the German Banking community "Deutsche Kreditwirtschaft"
- industry associations such as the EACB's 3,135 banks and their 209 million customers throughout the EU
- European decision-making bodies, for example

- the European Commission, chairing the Public Hearing on Innovations for the Green Paper on Retail Financial Services with Lord Hill, also part of the Steering Committee to improve European competitiveness/ efficiency by 243 BEUR per annum to the Lisbon Agenda
- the EPC - the decision-making body on payments of the 8000 banks in the 31 countries of Europe to the ERPB

Michael is a frequent keynote speaker, heavily published and networked on Open Banking and related topics

Liisa Kanniainen, Vice President, Senior Strategic Advisor, Nordea

Liisa currently supports Nordea's corporate customers to digitalise their payment processes and her target is to help customers (both B2C and B2B) to create a superior customer experience for their customers, while achieving cost savings through increased process efficiency.

She has wide experience ranging from pioneering mobile financial services business leadership and product development to e-commerce, cash management and innovation. Liisa is the Nordea spokesperson for PSD2 in the Finnish market.

Darek Nehrebecki, Vice President, Strategy and Business Model Development Europe, Mastercard

Darek is an experienced generalist strategy and economic consultant with a proven track record in advising companies on a variety of commercial, operational and competition economics issues.

In the strategic space, he has helped with: pricing and commercial arrangements, entry/exit, operational improvements across the whole value chain (procurement, manufacturing, logistics, distribution), bidding/negotiations - in a number of sectors, in particular FMCG, transport, logistics and TMT.

On the competition side, he has experience in advising on horizontal and vertical abuses of dominance, market definition and market power assessments, mergers and state aid.

Prior to joining Mastercard, he was a senior consultant at Oxera, an associate consultant at Mars & Co. and an analyst with emnos. Darek graduated from the University of Oxford with an M.Phil. in Economics and a BA in PPE.

Romano Stasi, Managing Director, ABI Labs

Romano is managing director of ABI Lab, after having covered several positions in consultancy firms, with a special focus on ICT solutions. Since 2003 he has promoted and coordinated many workgroups regarding security topics, such as business continuity, security governance, information and physical security. He has more than 15 years' experience in the field of ICT research and innovation for the banking sector.

Romano graduated in Mechanical Engineering from the University of Rome "La Sapienza" in 1993 and achieved the MBA in 1998 at the Bocconi University Milan.

Patricia Boydens, Chief Commercial Officer, Harmoney

Patricia has more than 15 years experience of digital communications & business development, mainly for financial services. She is an expert in savings and investments products, MiFID II, KYC and customer journeys. Patricia was just appointed as Vice President of FinTech Belgium.

She joined Harmoney NV in August 2018 after spending four years as the Digital Transformation Manager at The Society. Prior to that, Patricia was Business Development Consultant at MeDirect, a Belgian online bank, having been Head of Product Management at Rabobank.be.

Patricia is an enthusiastic motivator, with a hands-on mentality, getting people to do things; she looks for the win-win situation and after KPI's, sharp, into detail and helicopter view, passionate about start-up projects. Her mantra is 'every problem has a solution'

David Goodman, Consultant & Analyst, Trust in Digital Life

David has over 25 years IT and telco experience in senior management positions across a wide range of companies and organizations in Europe and America. He worked in product management roles in the areas of customer experience and subscriber data management at Apertio, Nokia Siemens Networks and Ericsson including cloud and big data planning for mobile operators. Previously, he worked in sales/ marketing at IBM Tivoli. David is a Principal Consulting Analyst at TechVision Research.

Learning To Live With Data Protection

Keynote: The Surprises of the GDPR and the Lessons for the Regulation of Artificial Intelligence

Paul F. Nemitz
Principal Advisor, Directorate-General for Justice and Consumers, European Commission

Paul opened by referencing the EC's high-level AI group that consists of 42 members, representing civil society, industry and academia. Meeting the previous week in Helsinki, the group were asked to come up with a code based on a statement of ethics for AI and robotics and to give their opinion in March.

Just recently the German government led by the Interior and Justice ministries, set up a similar commission, of which Paul is one of the 16 members. Over the course of a two-year period it is guiding questions on data ethics and has insisted are translated into English so outside opinions can be incorporated[1].

Today's question concerns GDPR and AI, which already has generated a lot of literature from eminent legal scientists and computer scientists. The headline: is GDPR killing AI?

The simple answer is "No" but any AI or machine learning program that works with data falls under GDPR. AI changes the meaning of GDPR because GDPR is technology neutral. If technology evolves, then the meaning of GDPR does too. So what does the application of GDPR to AI imply?
How does technology development, especially machine learning, deep learning artificial intelligence impact on the interpretation and real meaning of GDPR?
Not all data, either now or in the future, is personal data. For example, the weather is never personal data. Sensors on turbines and other instruments generate masses of

[1] https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/datenethikkommission/datenethikkommission-node.html

industrial data, far more so than personal data and it is more valuable and there is more of it. But AI has an impact on what personal data is because the definition is not constrained to data that identifies people but data that makes it possible to identify people, and the scope of that increases with computing power, data availability and the ability to treat that data intelligently.

There is also an increasing number of fields of technology that help controllers and processors manage compliance, such as privacy by design which is also an aim of GDPR.

If we have invested, then we should get a discount when something goes wrong. So we should invest for self-interested reasons as well as to protect customers.

This is another entry point for AI-based systems which can become elements of privacy by design and, when regulation assumes you do more than just comply, by investing in new privacy by design. The question is what is state of the art, what is expected, where does it go beyond?

There is also an obligation to keep data secure with an expectation to apply state of the art methods and stay up to date with the law. So, for example, using AI to improve security of data or making access management easier.

There's a claim that GDPR is being used by people to drag their feet and refuse to say what data they have.

AI can also help with claims management which will also be expected to stay current and state of the art.

The converse perspective is also valid: how should AI be shaped to comply with GDPR? The key points being the right to understand what's happening in automated processing as well as explaining purpose, relevance, method (articles 13-15 and 22).

According to Dr Sandra Wachter, a lawyer and research fellow in data ethics, AI, robotics and Internet regulation/ cybersecurity at the Oxford Internet Institute, information rights don't go very far. Andrew Selbst, a postdoctoral scholar at Data & Society and visiting fellow at Yale Law School's Information Society Project, disagrees and in fact says the opposite

The core challenge is explainability (XAI)

The law is always unclear, which arguably is the nature of democracy. It is nonetheless totally wrong to assume that the law has to move as fast as technology

We have to get out of the engineering view of the world that the law must follow the principles of coding.

Democracy is about deliberation, sometimes leaving things open and undecided, and not enforced perfectly. This lack of clarity is the price of technology neutrality. With the coming of AI there must be some uncertainty with respect to the regulation.

Early presentations simply said that they couldn't explain how conclusions had been reached and many security people who refuse to buy programs don't understand. But there is an obligation to give reasons when public power is exercised. For judges there is a very basic requirement to give reasons when describing an AI-based system. It is important that it is not undermined by technology either: if it's not possible to show what happens when information is added, a human must be able to explain. Now AI developers are increasingly saying it can be done[2].

This is an example of the way early policy statements guide innovation in the right direction, not least because the public sector big buyer and says must have explainability

The law is always unclear, which arguably is the nature of democracy. It is nonetheless totally wrong to assume that the law has to move as fast as technology. Law is good if it has a meaning when the world changes. We have to get out of the engineering view of the world that the law must follow the principles of coding. The machine is stupid which is why you have to update code. On the other hand, the people who interpret the law are not stupid, so the law doesn't need to be updated.

Democracy never produces clear outcomes, it is always a compromise – the GDPR had 4000 amendments! Democracy is about deliberation, sometimes leaving things open and undecided, and not enforced perfectly. This lack of clarity is the price of technology neutrality. With the coming of AI there must be some uncertainty with respect to the regulation. However, when the law is unclear, we should look to the higher law and seek our interpretation in that law. With GDPR, the higher law is clear: protect the individual, give them rights and have institution to give those rights.

It will not impress judges by saying that if they don't enforce the regulation there will be more innovation and profit –

[2] See, for example, Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI), Amina Adadi and Mohammed Berrada, September 2018, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8466590

Google tried this and failed. Judges are never going to be convinced on the contravention of fundamental rights.

In Germany the law was amended to ensure that all procedures must be automated in five years – so it is a big market but they must get used to the rule of law and fundamental rights, even when it doesn't involve personal data. For example, for medications there must be a paper explaining to patients that is a different explanation than that published for professional. It also applies to having full data published from trials.

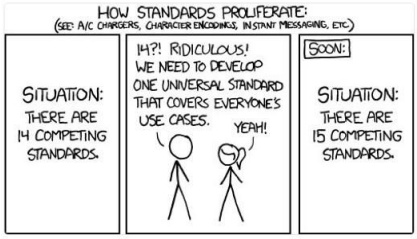
For the first misdemeanour engineers can be forgiven for not knowing, but once it has been pointed out that other models exist, then it should be finished and they should get used to it. We are moving into a world where AI will make decisions for us, so, to make them compliant with basic constitutional settlement etc, they must all be built in by design.

Do we need a new law? Maybe. But this is not an infant industry – AI is being developed by big powerful corporations, and the stakes are high. The Brexit vote was stolen because of lack of foresight and rules – these things are not harmless.

The current work on ethics could materialize into a new set of laws, particularly if it becomes clear that big actors can't be trusted to do (or refuse to do) the right thing.

Negotiated code on incitement to violence on the Internet works OK. Some say that it only works because the Germans made a law on the same subject. It's important to show who rules here: Facebook or democracy?

Now there is another one looming on protecting the 2019 elections and fake news. At the moment it's all voluntary[3]. It raises questions about the role of individual autonomy. Paul believes individuals will rarely use these rights, so it's



From xkcd sucks, 20 July 2011

[3] Constitutional democracy and technology in the age of artificial intelligence, Paul Nemitz, Philosophical Transactions of the Royal Society, 15 October 2018 (http://rsta.royalsocietypublishing.org/content/376/2133/20180089?rss=1)
Also: Governing artificial intelligence: ethical, legal and technical opportunities and challenges, Corinne Cath, Philosophical Transactions of the Royal Society, 15 October 2018 (http://rsta.royalsocietypublishing.org/content/376/2133/20180080?rss=1)

important to empower DPAs and NGOs to act on their behalf.

There was a question about the effectiveness of fines under the GDPR which is already creating an itch on the fines and discourse about them and the laws in some Member States that say always give a warning first – which is not in the regulation.

Paul mentioned is high esteem for the UK's ICO and the sadness that they're leaving because their number two is a policeman. We need more public prosecutors, policemen, investigators etc. – in other words people who know how to make a file that stands up in court. Without mentioning any names, one national DPA head is a former librarian. He was skeptical that we can get public companies with shareholders to do what's right without the threat of fines.

Disruptive innovation is taught in law schools now, including disrupting the law, local transport, etc. There are too many people in Silicon Valley, such as venture capitalists who think they're kings and can do anything. Which does not fit the concept of democracy and the rule of law. Paul asserted that business schools should stop teaching how to disrupt the law. We will not be able to solve the policy issues if the law is not delivering or just being disregarded ... we should move on and break things. The populace is on the other side. Engineers should wake up and decide where they stand on constitutional democracy

Technology investors last week were talking about building investment decisions on the basis of risk of fines. So it is having an impact. Max Schrems, who has a very successful track record to date, lost no time in submitting complaints against Facebook and Google regarding forced advertising and collection of data[4].

The learning curve for competition law appears very low and without substantial fines amounts to effectively nothing. It is unlikely European competition law will be changed, but there is some scope to apply that which takes account of modern development. In her speeches

[4] Max Schrems files first cases under GDPR against Facebook and Google, The Irish Times, 25 May 2018

EC Commissioner for Competition, Margrete Vestager, talks about “hearing the wind blowing”.

There is a huge issue of concentration in technology. Frank Pasquale, a Professor of Law at the University of Maryland, an Affiliate Fellow at Yale Law School's Information Society Project, and a member of the Council for Big Data, Ethics, and Society, writes extensively on the sources of news and the integration of AI, data, etc. These four things together have never seen such a concentration of power like this before which is a problem for markets and democracy. Imagine if Google or Facebook decide to give raw data to only one side ... or were to start going into providing news content.

Panel 1: The Ups, Downs And Surprises Of GDPR So Far

Five months after GDPR came into force, this session reviewed what's been learnt so far and evaluates how all the stakeholders are faring. Despite the noise and speculation earlier this year and the tremors felt well beyond Europe, has corporate or civic awareness of the underpinning issues really changed?

Moderator:
David Goodman
Consultant & Analyst,
Trust in Digital Life

Maarten Stultjens
VP Partners Sales,
Marketing &
Corporate
Development,
iWelcome

Maarten presented the results of an iWelcome survey of consumer attitudes over a 12-month period before and after the launch of the GDPR[5], that encompassed seven countries, six verticals, and 89 companies. Overall the UK, Germany, and Sweden are doing well, with Switzerland, France just behind them and Netherlands not doing as well.

From an industry vertical perspective, retail/e-tail and media are doing well with the BBC lifting UK (if we want to look at consent, the BBC is doing well). Insurance and utilities companies can't switch easily, are further behind.

Key findings are:

- Consumers are not in control
- 33.7% of organizations are not compliant in most areas, only fulfilling some requirements – an improvement from 66.3% in early May
- Basic are requirements in place: the ability to withdraw (92.1%), the right of access (96.6%), the right of rectification (95.5%)
- However, privacy by default, data retention and consent are hardly implemented
- Consent is the least considered with only 12.4% almost or fully compliant.

The overall conclusion is that there is an apparent veneer of legitimate interest, but there is an underlying approach

[5] The state of GDPR-readiness in Europe, A consumer perspective, 5th Edition, July 2018

to circumvent where possible. Do we really care about privacy? Or is the overriding approach to make as little effort as possible, and to try and get away with legitimate interest.

Dr. Jörg Hladjk
Of Counsel, Cyber-security, Privacy and Data Protection Practice, Jones Day

Jörg observed that there is no one size fits all, seeing a lot of organizations after implementing step-by-step struggle with processes and procedures. Implementation is difficult across all sectors. They often complain that handling procedures is not there, so they can't think about adding some for access rights.

Even the best players in the market find that data retention is a big topic and most companies stop there because they don't know how to deal with it as it often means a change in culture, mentality, procedures, especially companies with US subsidiaries.

Georgios Kourogiorgas
Data Protection Officer (CIPP/E), Worldline Global

If one company excels then it impacts the whole sector.

There is legal clarity missing which is limiting opportunities for the single digital market that GDPR promised. Within Worldline, seven countries have still not implemented.

Discussion

Jörg said that, because there is no case law yet, companies are looking at carrying out risk assessment with respect to the GDPR.

Maarten sees discussions that companies say they can't do this or don't know that but by looking at websites of consumer-facing services it becomes clear what is not implemented and lacking. At present, the authorities are not stepping up to give warnings or fines.

Everyone agreed the importance of getting the main things in place and making it extremely clear. For most relevant data it's necessary for companies to store how they got that data – different for each piece and different retention policies for different attributes (and processing purposes).

A question was raised as to whether we need some sort of trust mark that is GDPR-compliant, like a kite mark.

“

Rather than putting the emphasis on compliance, it's more important to build trust, and, by doing that better, it makes companies more competitive.

The response from the panel was that it is very difficult. There are articles on certification mechanisms, but no initiatives are apparent. Rather than putting the emphasis on compliance, it's more important to build trust, and, by doing that better, it makes companies more competitive.

Every data protection authority (DPA) is setting its own procedures for consumers, and the administrative practice is not harmonized. It requires the EDPS to set template procedures.

There was a wave of access requests after May but it has quieted down since. Consent is a very personal thing, so reviewing data consented on is diverse. At the moment consumers simply ask for consent and specific purposes of use.

There was a question about standards like ISO 9000 and 9001? There are a number of companies (for example, the 'EU GDPR Certification Company') that are saying come to a one-day seminar, and we will give you a certificate that says your company is GDPR compliant. These companies are bogus and causing a lot of confusion in marketplace and there doesn't appear to be any mechanism for any authority to intervene. We should in any case be allergic to companies that say they are fully GDPR-compliant. GDPR focuses on processing activities, not end-to-end services.

On the effectiveness of fines, why are so few actions taken?

In a case published recently a hospital received a potential 400 KEUR fine, although most authorities are not ready yet, after five months, to fully enforce – many are still hiring and getting their teams in place. In the short term only a few activists are going to go to the media but that will change.

The draft ISO 9000 standard is trying to do something like that, based on ISO 27001. Driven by CNLI and industry leaders, ISO/IEC 27552 specifies requirements and offer guidance on extending ISO/IEC 27001 and ISO/IEC 27002 for privacy management.

Panel 2:

How Well Is GDPR Working?

Five months after GDPR came into force, this session reviewed what's been learnt so far and evaluates how all the stakeholders are faring. Despite the noise and speculation earlier this year and the tremors felt well beyond Europe, has corporate or civic awareness of the underpinning issues really changed?

Moderator:
Wendy Grossman

Giles Watkins
UK Country Leader, International Association of Privacy Professionals

Giles explained that his is an honorary position at IAPP which has 10,000 certified members and aims to raise the bar on professionalism in approaches to privacy and privacy-related matters. Addressing the theme of the session, it could be said that everything is going wrong with GDPR, which is primarily down to a lack of awareness. Indicative of this is that there is still a need for 27,000 DPOs across Europe a hole that will take some time to fill.

He said that for most businesses that are perceived positives and negatives. On the plus side, the GDPR addresses key business drivers such as generating profits and opening new markets, both of which are based on establishing trust. The perception on the minus side is that the GDPR is a regulation and brings with it barriers, tariffs and business inhibitors in general.

Finn Myrstad
Director of Digital Policy and Energy, Norwegian Consumer Council (Forbrukerrådet)

Finn opened by referring to 'Deceived by Design' a report produced by Forbrukerrådet in June 2018[6], an analysis of Facebook, Google and Microsoft Windows based on their pop-ups with respect to security, privacy and consumer rights. The report analyzes a sample of settings in Facebook, Google and Windows 10, and shows how default settings and dark patterns, techniques and features of interface design are meant to manipulate users and are used to nudge users towards privacy intrusive options. The findings include privacy intrusive default settings, misleading wording, giving users an illusion of control, hiding away privacy-friendly choices, take-it-or-leave-it choices, and choice architectures where choosing the privacy friendly option requires more effort for the users.

[6] https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf . A follow up report 'Every Step You Take' is now available at: https://fil.forbrukerradet.no/wp-content/uploads/2018/11/27-11-18-every-step-you-take.pdf

To demonstrate the complexity of the task facing consumers wishing to understand, Finn explained how the Norwegian Consumer Council had downloaded the terms of service and privacy policies for apps that you would find on an "average" mobile which together exceed the length of the New Testament. And in a well-publicised and broadcast activity, held a public involving 120 people taking turns to read out the terms and conditions from 33 popular apps which lasted … 31 hours 49 minutes 11 seconds[7].

> *"And in a well-publicised and broadcast activity, held a public involving 120 people taking turns to read out the terms and conditions from 33 popular apps which lasted … 31 hours 49 minutes 11 seconds*

Finn also mentioned a study from Princeton which investigated the extent you may be watched when we use the Internet and visit sites which might have hundreds of scripts running in the background, some depositing cookies, others tracking you to other websites[8].

He also drew attention to the ban on facial recognition in 2012 after Max Schrems along with others filed a set of complaints with the Irish DPA (Data Protection Agency) against Facebook, which had been profiling users with emotional analysis from photos, which resulted in Facebook bringing its privacy policies in line with data protection regulations at that time. However, under the GDPR, facial recognition has been brought back.

Finn went on to observe that so far gdpr.org has registered 20,000 complaints in eight EU Member States, and 13,000 breach notifications, resulting in six fines totalling €2350! Despite this GDPR is starting to work and that consumer trust is a factor of realising the data they have and what they do with it.

Discussion

Giles concurred referencing the 2018 Annual Governance Report from IAPP and EY[9] which found that less than 50% of survey respondents reported they are fully compliant with the GDPR. In addition:

- 73% have a formal reporting mechanism to Board level

7 https://www.forbrukerradet.no/side/250000-words-of-app-terms-and-conditions/ and https://www.telegraph.co.uk/technology/2016/05/26/consumer-campaigners-read-terms-and-conditions-of-their-mobile-p/

8 https://techxplore.com/news/2017-11-princeton-website.html

9 https://iapp.org/media/pdf/resource_center/IAPP-EY-Gov_Report_2018-FINAL.pdf

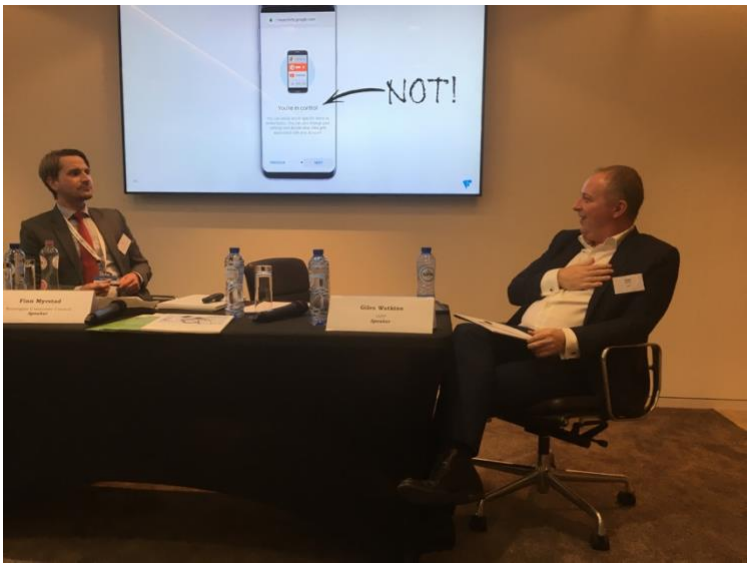
- Only 32% said their privacy was mature
- 56% said they were far from compliant or will never comply.
- 18% 'honest brokers' said they would never be compliant
- 33% are doing on-site analyses, independent audits, of suppliers using

He also pointed out that in the UK the ICO is essentially 'friendly to business.'

Finn stated that Facebook and Google don't dispute the findings of the Forbrukerrådet report but do take issue with the conclusions, believing that what they do is in their legitimate interests – a position that is going to be challenged in court soon.

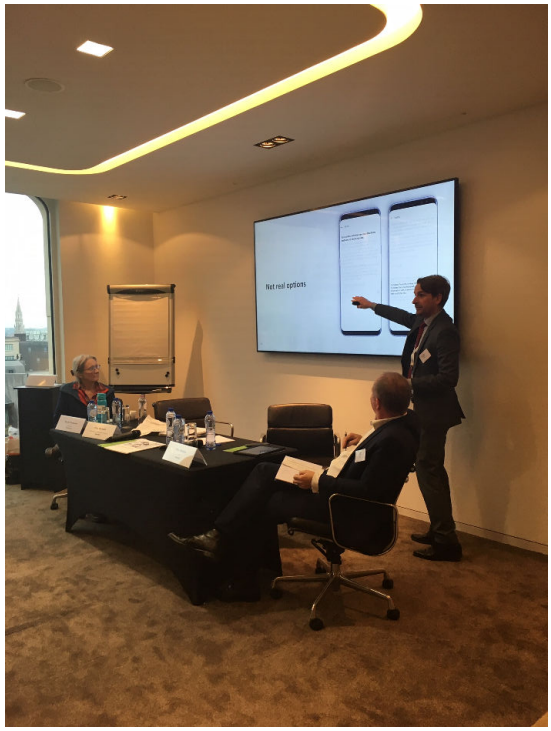
He observed that the guiding principle in the EU is to protect citizens whereas in the US it is to protect business. As long ago as 2010 the Forbrukerrådet filed a complaint about Facebook sharing data with third parties.

They have recently been looking at Microsoft's consent pop-up which did better than the other two investigations. Xbox has not reported any breaches whereas there was a massive breach with Playstation. Microsoft clearly improved their information security.



Following a discussion on the length of time taken to bring actions to court, Giles pointed out the dividing lines between the internal activities around looking at breaches, compiling data inventories and ethical decision making compared with finding the money to carry out training, finding a suitable DPO and implementing privacy-enhancing technologies.


Nordea
Open Banking
Beta test
Developer
Testing


Net real options


Main changes via PSD2 and market progress...
Objectives of PSD2
Scope
Efficient and integrated market
Single market
Security
Strong authentication
Secure connection
Consumer protection
Unauthorized uses
Surcharges
Competition
New payment solutions
Access to accounts - XS2A

Making The Most Of Open Banking

Keynote: Open Banking and PSD2

Michael Salmony
Executive Advisor to Board of Directors, equensWorldline/ Worldline SE/Atos

Having introduced his extensive background in PSD2 and Open Banking, Michael went on to demonstrate that PSD2 is part of a much larger trend to open up banking and the finance community. Its goals are to enhance competition, promote customer convenience and to facilitate innovation impacting all aspects of payments. The key game changer is the provision to allow trusted third parties access to accounts, but at the same time ensuring consumer security.

PSD2 will put pressure on the cards business – Apple has over one billion cards stored on file – which will impact local shops as they store cards on file and draw on them. This is a popular model that may now be replaced by direct payments, so that money can be sent direct without having to use "evil American card schemes". It may be successful because there are a lot of advantages, not least not having chargebacks, although not having a layer of protection from a credit card company could be seen as a disadvantage.

> *... PSD2 is part of a much larger trend to open up banking and the finance community. Its goals are to enhance competition, promote customer convenience and to facilitate innovation impacting all aspects of payments.*

The European Commission is on a rampage to make this happen. The ERPB (Euro Retail Payments Board) defines the rules on how payment initiation will work

Germany planned for five Fintech applications, such as Sofort. In contrast the UK is not interested in payment initiation but in data and transaction history and so is focused on personal financial management model, as in aggregating accounts. Both are modest ambitions: there are no disruptive business models in the UK. This is the regulatory focus and is very modest, particularly as the impact of open banking will be much, much bigger than this: some banks have thousands of people working on new models for customers and the EBA (European Banking Authority) is finding thousands of applicants for licenses

Banking is increasingly becoming an IT business, but a lot relies on expertise and advice, especially in the corporate market

One possible model for the emerging market is 'smart banking' or 'Payment as a Platform' which could be compared with Nokia and smartphones or like the Apple app store – an app model for financial services.

Will banks just become a series of background servers but blown away by Fintechs? Michael didn't think so and expects to see partnerships in the future, as evidenced already by the banks buying up startups.

Non-EU countries are looking at Europe and watching how this evolution is progressing.

One possible model for the emerging market is 'smart banking' or 'Payment as a Platform' which could be compared with Nokia and smartphones or like the Apple app store – an app model for financial services.

There are hundreds of emerging PSD2 ideas such as:

- new options for better checkout solutions,
- social ATM being able to obtain money from people physically close by
- hotel IoT, whereby you just pay for what you consume
- a card-less ATM which gives you access to cash across Europe with one app

And then there are crazy ideas such as a dating/data scientist looking at transactions to match people with similar interests and profiles

Michael believes that B2B is the hidden champion for PSD2. Banks don't serve corporates very well - surveys show banks think they do, but companies say they don't and that they are not flexible enough. PSD2 can change that. Although consumers generate lots of transactions, the value is in B2B – where the money is. Not many people are looking there, but there is a lot of potential disruption there. Fintech attackers are increasingly focusing on SMEs and corporates.

All other industries are opening up: for example, publishers are complaining about European incoming law on open publishing. Making PSD2 work will be difficult - fraud and hacking are big issues but everything is being worked on in the technical, functional, legal, operational spheres.

A few things are not solved:

- identity: how to open up safely and conveniently. It's an absolute mess at the moment. For example, how do you identify that a TPP, accessing a customer and his account, is not rogue?

- GDPR: the key conundrum is how to open up while protecting customer data. There is also the issue of customer consent: if you allow access to a third party, then it's not just your own information but also that of other people.
- reach: how to connect all the TPPs and banks across Europe?
- fraud defence: connected solutions requiring intelligent management, having to satisfy the requirements of the banks and the TPPs

In the emerging digital ecosystem, every industry will provide APIs and open up and then combine to develop new services.

In the emerging digital ecosystem, every industry will provide APIs and open up and then combine to develop new services. For example, Uber takes locations, maps, Paypal, and mashes them up to provide the Uber service. Besides the expected services, we will undoubtedly see surprises.

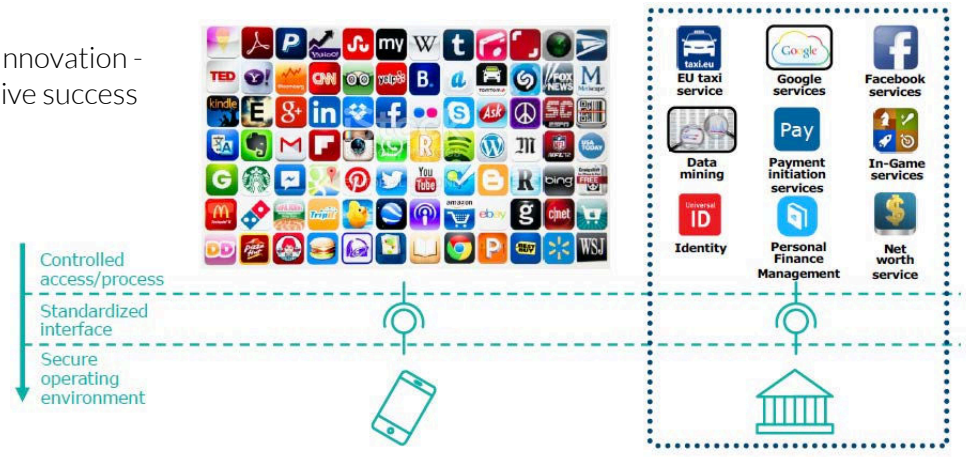
The regulator mandates that there should be no 'API rot' and it's a pity that it had not been made technology neutral.

Given the range of different industries, in addition to the banks and the Fintech community, Michael suggested that it would require service providers – such as equens! - to tie them all together.

The deadline for going live with PSD2 is September 2019, although some banks already have thousands live

There are working groups on standardising APIs for access, such as the open banking working group in the UK, which works in parallel with the Berlin Group – each one thinking that the other has to catch up with them. By contrast, a number of companies have their own working group, a difficult process.

Open Innovation - a massive success



Panel 1:
The PSD2 Experience To Date

Despite the intense interest in the disruptive and transformative impact it would have on the established financial community and emerging Fintech start-ups, it's not apparent how widely the adoption of PSD2 has been felt or made known since it came into effect in January 2018; nor how the different initiatives, such as the UK's Open Banking Group, the Berlin Group and others, are aligned.

Moderator:
David Goodman
Consultant & Analyst,
Trust in Digital Life

Liisa Kanniainen
Vice President, Senior Strategic Advisor,
Nordea

"Some banks consider PSD2 as a huge threat while other banks such as Nordea see it as an opportunity.

Liisa got interested in PSD2 five years ago. There is a clear need for consumer education to know what's safe and what isn't because the model is changing

Liisa described Nordea's business and told that it is the biggest bank in the Nordics and in the top ten in Europe by market cap. She noted that its relationship with its customers defines its impact on society and the environment – there is global warming even in financial policies.

With the customer in the centre, it starts with mobile assuming open banking to be the platform for future services. Nordea is renewing the core of the bank along with payment systems and warehouses, making it the only bank doing this level of change.

Nordea comprises 300 banks through mergers and acquisitions, so with a complex back end, there is no other way to go.

There are 100 robots – which will grow 1000 – to provide robotics. Trade as a blockchain-based platform, also active in wallets, etc – first in Apple Pay

They have started a beta test: 300 Fintechs signed up within three days and within three weeks it shot up to 700. The interest was so great they had to close the portal for a while. There are now more than 2000.

Essentially an "open banking hackathon", 28 beta testers given access to the sandbox and later opened it up for developers, believing collaboration can enable better and richer services.

Liisa particularly works on corporate APIs and how to monetize - unfortunately despite all the benefits the API marketplace provides there is the potential for a perfect man-in-the-middle attack. All that emphasizes that educating the public is a community challenge.

By leveraging the capabilities of the Open Banking platform and their partnerships with innovative Fintechs, Nordea believes it can create value adding solutions for its customers, resulting in a win-win-win situation.

Darek Nehrebecki
Vice President, Strategy and Business Model Development Europe, Mastercard

For Darek, authentication is the biggest issue. The vast majority of transactions are now not authenticated and there is a shift to needing strong authentication. The rate of incidence of requests for more information is going through the roof which for merchants raises the rates of abandonment. Unsurprisingly there is a lot of work going on to protect 'smooth user experiences.'

According to a recent Gartner report, spending on security is rising so fast that it will soon surpass the IT budget.

Banks will have higher liability (fraud transfers). Merchants were able to surcharge card transactions before PSD2 but this should be gone by January 2019, although it will be up to national regulators.

> *"In the old world banks were interacting with corporations and with consumers. In the new world banking and payments are becoming an invisible part of everyday life. The big question here is: what does this mean for banks? How can they distinguish themselves from each other? Banking will always be there, but no doubt in the future banks will be perceived in a different way.*

There are several early open banking use cases. Amongst them, Deutsche Bank is teaming up with IATA to allow direct payments for airplane tickets. Others include instant credit decisions, SME accounting and cash flow management

There are troubling security aspects. Personal finance management involves credential sharing – precisely what banks tell you not to do e.g., Mint distributes login credentials. That goes away, top security upgrade, deposit optimization.

There is a need to find solutions to common pain points, among which are:

- connectivity into banks
- security fraud and liability
- no standards around disputes and complaints
- uncertainty about monetizing data
- poor user authentication experiences
- granting permissions

Banks will either close or find new distribution channels. There are over 5,000 banks in the EU, and most are in compliance land, Nordea being an exception.

When there is a loss of money, banks are required to put money back next day.

What will the consumer uptake be, given that only a small fraction of the population are using it today? Customer understanding is minimal; some banks provide warnings or are generally discouraging (Lloyds and other UK banks).

Banks will either close or find new distribution channels. There are over 5,000 banks in the EU, and most are in compliance land, Nordea being an exception.

Mastercard is creating a set of solutions to address these pain points.

- For trusted third parties: a Global Connectivity Hub
- For banks: an enhanced TPP fraud profiling solution to help decide which requests to accept.

Supporting these are ecosystem solutions relating to dispute resolution, an API distribution platform (which will eventually bring together non-regulated premium APIs), consent management and authentication solutions.

Today is the 155th anniversary of the beginning of the Geneva Convention. The only country where PSD2 is live to date is … UK (always has been on a different timeline to anywhere else!)

A similar regulation is coming to Australia 3Q 2019 and will include telcos. Japan, Hong Kong, Singapore, Canada, Brazil, Mexico all have different flavours of intervention. Nigeria and the US – actually have industry setting standards rather than regulations. Nevertheless, it should be ubiquitous in ten years.

Countries were supposed to have enacted legislation by January 2018, but only 29% of EU companies have done so.

Panel 2:
What Next?

Open banking presents new opportunities for processing financial transactions and introduces a new set of players and rules. It also potentially presents a new set of challenges not previously envisaged. This session looks at use cases, both existing and potential as well as security issues, including alignment with GDPR.

Moderator:
Michael Salmony
Executive Advisor to Board of Directors, equensWorldline/ Worldline SE/Atos
Romano Stasi
Managing Director, Italian Banking Association (ABI Labs)

Romano described ABI Labs as a consortium, working with Italian banks to addressing their pain points. Italy is investing in data, governance and banking is competing with the fintech community. It is focused on regional competition - Italian banks are not ready to focus their strategies on digital services whereas, for example, a Brussels bank can target the Italian market. Contrast this with the main strategy of every Fintech which is to think about Europe and the World. Digital first or digital only to propose to customer, and also a strategy that's international not just domestic.

Banks are national and Fintechs are pan-national which has implications on the role of regulators. Regulatory arbitrage is not good but Fintechs tend to start up where the regulations are most favorable that suit them the best and then expand.

On the other hand, it's a good thing that national regulatory authorities (NRAs) have different approaches in different countries. One country may be security conscious, another less so. Fintechs choose countries where they think they can prosper the best, which creates competition, and leaves them free to passport into other countries when they find a particular model works in the first country.

Regulation comes at a cost and it should/needs to be the same across Europe.

For example, one Fintech found it difficult in Italy so requested a license in the UK from where it continues servicing Italians.

There should be a level playing field, but local markets tend to implement their own markets with their won traditions in mind.

Patricia Boydens
Chief Commercial Officer, Harmoney

Patricia remarked that in Belgium there is a long tradition of a super-efficient payment system and it would be desirable to see a more open dialogue between new players and regulators. At the moment one-way, you must comply. The regulatory authorities and others are being very protective – why should they open up?

It would be better to have an ecosystem where everyone works together, whereas it seems more like that banks are resisting the new competition.

Nordea made the positive decision to embrace the new landscape, seeing how to develop customers they want to serve. Scandinavia is setting a great example for other countries! It will take a bit more time in countries like Italy and Spain. Although already 85% of large Italian banks are looking for partnerships with Fintechs and research and investment.

Discussion

What will the world look like in ten years' time?

The current set of issues and gripes will gradually get resolved. Even though in IT the world can anticipate problems, it can take years to get to standards and a common position. Notably in finance, disputes have to get fixed and security issues need to be addressed. However, not all will be fixed within ten years

"Banks will also survive but are more likely to morph into different versions. Some will disappear. Some Fintechs will survive; many will be absorbed. Lots will fail. Silicon Valley will see opportunities, but will they dominate?

The US takes an industry approach, whereas Europe a regulatory approach, which tends to be different in every country. There will be a role for banks in ten years – they won't go away.

In the IT industry a big company under threat has money and smart people, and will find ways to survive. Banks will also survive but are more likely to morph into different versions. Some will disappear. Some Fintechs will survive; many will be absorbed. Lots will fail. Silicon Valley will see opportunities, but will they dominate?

> *... there are (at least) three possible scenarios*

> *Banks will win and walk with everything because of all the hype etc. Fintechs that do useful things will get absorbed. So mobile, direct banking will be much the same as it is today ...*

> *... there will be total fragmentation: financial service providers will break down into lenders, specialized portfolio managers, banks may break up, some technologies, Fintechs, security bits creating a platform economy where everybody connects to everything ...*

> *... a halfway where digital giants take all. Amazon, Google, Facebook can set standards and tiny Fintech in Belgium will have no power to challenge it.*

Banks have legacy systems whereas Fintechs start from scratch, so Fintechs have a competitive advantage with modern technologies.

Ultimately, it's all about extreme customer centricity and those companies that have it will win in ten years

Michael summarized observing that there are (at least) three possible scenarios:

- banks will win and walk with everything because of all the hype etc. Fintechs that do useful things will get absorbed. So mobile, direct banking will be much the same as it is today
- there will be total fragmentation: financial service providers will break down into lenders, specialized portfolio managers, banks may break up, some technologies, Fintechs, security bits creating a platform economy where everybody connects to everything
- a halfway where digital giants take all. Amazon, Google, Facebook can set standards and tiny Fintech in Belgium will have no power to challenge it.

It could be said that this is conflating payments and banking but it may simply come down to who has the biggest and most important piles of data. There are PSD2 APIs for banks, but not Facebook or Google. There will be a few big trusted players. Amazon are not going to be a bank themselves but are more likely to plug in everything. Fintech have no marketing power or branding, so the ones who have trust – and on all devices – will be the winners. Fintechs will be enablers.

Anyone offering financial services will be a bank.

Patricia sees banks today taking over businesses. Her daughter has never set a foot in a Belgian bank branch and would have no idea what to do. Bank is on the phone. We are nibbling away at pieces of Europe ecosystem.

Where are the incentives to change? Two piles of players – banks and Fintechs. What currently are the incentives for banks to be compliant? If there were 3,000 different APIs, they'd have to change some every week...

Confusion of language - when people say Fintech it can mean many different things. Consider the situation as a 2x2 diagram: bank/regulated/licensed vs technology competent.

Most banks are regulated but operate in the old system although some have adopted state of the art approaches. Banks may manage to re-platform if their CEOs have the guts. Many are but most are not.

But it is amazing, to have an unregulated company that will source services from regulated third parties and create an ecosystem of services off the back of it. The front door doesn't need to be regulated!

Google can be a gateway to financial services tomorrow with partners by creating an extra consent box. People are unaware: for most the prospect of a smooth app will get them over the line. In the user experience lies the set of winners

Romano mentioned 'CBI Globe', a global open banking ecosystem. Consorzio CBI has been appointed by the Italian financial community to develop a cooperative international solution working to facilitate interconnections between ASPSP and TPP in order to reduce investments and technical complexity for participants thanks to the centralization of some 'shared services'

David Goodman
Consultant & Analyst,
Trust in Digital Life

David explained that, to tackle open banking security concerns, the European Commission is planning on awarding a 42-month project to a consortium comprising 43 partners from 22 EU Member States, including Trust in Digital Life (TDL), with the objective of create competence networks across Europe with a hub European cybersecurity research and competence centre.

There was a question as to why ENISA is not involved, the reason being that ENISA is not allowed to get involved in project proposals because as an EU institution it must remain neutral. However, once a project is underway, it is a different matter.

The project, led by Goethe University Frankfurt, will cover nine vertical sectors and 11 technology elements and one of the ten work packages will feature industry demonstration cases in the following areas:

- finance – incident reporting; open banking security
- health – medical data exchange
- smart cities – citizen participation/e-Government; critical infrastructures; education

- transport – maritime (port critical infrastructure); supply chain assurance

TDL and ABI labs together with Université Paul Sabatier Toulouse (UPS-IRIT), Intesa Sanpaolo, and JAMK are leading the task on open banking security.

The initial areas that have been identified are:

- Social engineering & malware attacks
- Certificate verification
- GDPR & PSD2
- APIs
- Circles of trust

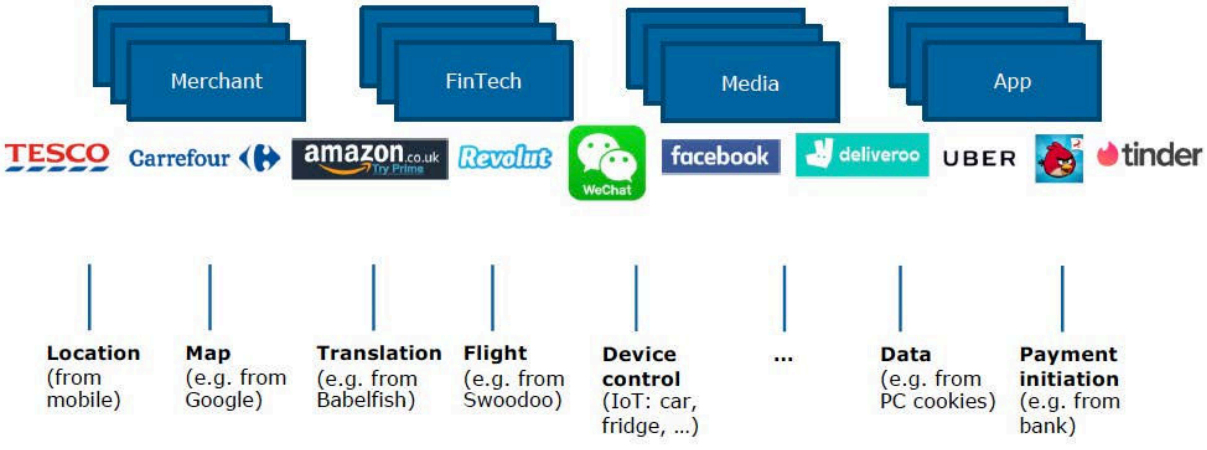
Without clarification, banks will err on the side of safety especially because of GDPR

What is the relationship between a bank and a third-party subcontractor they can't see? You would have to go back to the third party to withdraw consent, it can't be done via the bank, unlike today, where it can be done from either side.

A question came on how to handle consent and access requests under GDPR, with the proviso that consent in the GDPR and PSD2 are different. Fintechs embrace the GDPR because they generally start off by thinking from a customer perspective. A lot of banks however are exploring blockchain which has a number of GDPR-related challenges, not least of which is the right to be forgotten.

One idea suggested was that in the future every bank will have a consent dashboard

Emerging Digital Ecosystem



Glossary of Terms

AI	Artificial Intelligence
AISP	Account Information Service Provider
ASPSP	Account Servicing Payment Service Providers
CRM	Customer Relationship Management
DPA	Data Protection Authority
DPO	Data Protection Officer
EC	European Commission
EU	European Union
GDPR	General Data Protection Regulation
IAPP	International Association of Privacy Professionals
ICO	UK Information Commissioner's Office
NRA	National Regulatory Authority
OBWG	UK Open Banking Working Group
PSD2	Payment Services Directive 2
SME	Small and Medium-sized Enterprise
TDL	Trust in Digital Life Association
TPP	Third Party Provider

'Are you aware that you can now do all of this online?'

TDL's vision is that trust must become an intrinsic property of any online transaction involving personal information, incorporating legal, business, and technical advances. By supporting cyber security policies, and integrating societal considerations, we believe that citizens and end users will recognize trustworthy services, transactions, and data, and be prepared to pay for them. Trustworthy ICT will increase confidence and trust in modern society, bring new and attractive ways of living and working, and further strengthen Europe's democratic and social values.

The association's mission is to provide its members with a European business development platform in order to stimulate development and user acceptance of innovative but practical trustworthy ICT. Guided by its strategic research agenda, TDL acts as an incubator for a portfolio of sprint projects intended to validate new and innovative technology concepts, promotes cross-sector collaboration, and aggregates the results into industry recommendations for policy makers and the European Commission.

trustindigitallife.eu

trustindigitallife.eu

Trust in Digital life Association
Maurice Dekeyserlaan 11 /
Avenue Maurice Dekeyser 11
1090 Jette, Brussels
Belgium

office@trustindigitallife.eu
+44 141 588 0892

TDL | Trust in Digital Life