# Disposable Identities: A roadmap for Identity creation for people and objects[1]

WORK IN PROGRESS @robvank

If I were called in
To construct a religion
I should make use of water.

Larkin, Philip. The Whitsun weddings. Faber and Faber, 1964.

## Introduction

This Framework introduces the notion of a disposable identity in a world in which the properties of the knowns to us: people, animals, objects and by extension protocols, formats, processes become fluid and mixed into new entities.

In. previous *Salons* on identity by NGI.eu, new models in insurance were described that in the case of an accident with a self–driving car reason as follows: the car gets awarded a temporary identity, the person(s) involved get awarded temporary identities, the rock the car hits before it goes into the water receives a temporary identity, as well as the (pollution in) the water. The combined result of this becomes an ‘event’ identity. This event identity subsequently becomes the basis for negotiating claims.

Uncoupling identity in thinking of “entitlements’ (combined disposable identities of objects and beings) opens up a new field of value and services. In the case of self–driving cars this way of thinking could argue for liability not with real person–identities but with ‘entitlements’; any combination of a particular driver (with particular points on a passport and certain characteristics) and a particular car. This reasoning can be extended to basically any service in the network.

## Identity

Registration of people in China started 278 BC with the first Emperor. In Europe Napoleon started this process in 1800 with the Code Civil. These two cultural trajectories are important to understand the current digital transition in which

[1] Version 2 with comments addressed by Manon den Dunnen

politics and technology are deeply intertwined.

In the old analogue days this hard relationship between a person and a number was defined in one reality (what actually happened, what one could actually see, what one actually did) and harnessed within a rule of law system.
As we move into a hybrid world, it is not just the sum of analogue + the data in digital devices. As every object becomes not only digitally addressable and traceable (item level tagging) but is also collecting data about the (people in) the surroundings, the world of #IoT, Big Data, and AI comes into being. Meaning that whoever owns the relationships of these (objects in the) surroundings with one person's number, currently companies with shareholder obligations and national governments with selected self -interests, is given a large number of extra layers of capabilities. Capabilities and therefor agency that was not included in the original negotiated registration process, not democratically established and non-accountable (non-transparent algorithms). Capabilities that also acquire a pro-active capacity, ie. predictions about behavior, that is not fully shared – or only shared when beneficial to the country or company – with the person whose number is used.

## Disposable identities

The Identity Taskforce in NGI Forward will work on defining the characteristics of Disposable Identities and the requirements for the Trust Framework that certifies conditions to the disposability and verifies and testifies to the disposing of the disposable identity.

Disposable identities are temporary attribute-based identities integrated in a smart contract between a receiver and a supplier of a service, describing: *[actor] may [action] with [actee=disposable identity] under [condition] so that [purpose], services* that demand for context based sharing of data like leasing a car, sharing energy between homes, paying taxes, but basically also any existing service.

Disposable identities can only function in a provable computing environment. That environment is currently not available. It then means that Disposable identities and the Trust Framework are being subject of this ETSI group that is aiming to standardize and make interoperable something that is not yet there.

Disposable identities are thus the only foundation for an eID framework in which all entities (natural, animal, person, man-made, machine-made) can be named and become actionable. The person is no longer the middle and end to end point of services.

## Hardcoding GDPR

The undeniable global push towards a single digital ID protocol is the fruit of converging objectives emanating from corporations and public authorities and increasingly by broad public demand.[2] Furthermore, there is a

[2] WhyID: Protecting Our Identity in the Digital Age
21 OCTOBER 2019 | 4:00 AM
To the leaders of International Development Banks, the United Nations, International Aid Organisations, Funding Agencies, and National Governments:

broad consensus among the same parties that this single protocol should remain the responsibility of national authorities even as they are pushed to agree on a global standard. This means that whatever will materialize as the globally adopted solution both as law and as technology, it is a matter of critical societal and geopolitical importance for the EU. This cannot be decided piecemeal by each member state without coordination or driven by the sole appeal of unproven and poorly defined “digital efficiency”. Furthermore it has to take into account the need for entitlements, combined identities for example in the case of autonomous driving vehicles which will be introduced and explained shortly.

The temptation is great to address this push through an all-encompassing solution responding simultaneously to multiple public policy objectives (from cost efficiency to security) and to the needs of a digitalized business sector (from banking to retail sales). But while options are still open; it is critical to bear in mind that levels of distrusts in both public authorities and the digital sector are higher than they have ever been in the last decades and not abating. A solution that would have the backing of both public authorities and the digital sector but disregarding the long-term consequences for public values and against popular opinion could have very toxic and perhaps lethal effect on the legitimacy of the EU. On the other hand, a solution (both legal and technical) that would offer protection to the essential margin of individual freedom and privacy that has been broadly celebrated about the GDPR would not only shore up support at home and help enforce the GDPR but also help the popularity of EU branded solutions globally

The first challenge to sound policy in this enormously impactful area is adequately scoping the issue.

## Scope

The mindset you need to understand the need for extreme centralization and extreme decentralization *at the same time* is war. War allows us to understand loss of sovereignty by losing agency over the basic assets citizens accept voluntarily (democratically) to fund with their taxes. In 2019 this basic asset is data of people and objects harnessed in platforms plus the capacity to contextualize the initial datasets for proactive capabilities. Simply put, a 500 million zone (made up of relatively autonomous national states) that cannot claim this basic feature will lose the voluntary notion in raising taxes and will break under the current self-organizing agency of individual citizens and groups. We are not in favor of this breakdown.

We are a group of civil society organisations, technologists, and experts who work on digital identity developments across the world. We have worked directly with vulnerable populations, and witnessed the impact that ill-considered, badly designed, and poorly implemented digital identity programmes can have on human lives.

#WHYID: ADD YOUR NAME
You can also sign the letter, join the mailing list, or find out more about our ongoing collective work on digital identity by emailing identity@accessnow.org.

https://www.accessnow.org/whyid-letter/

## Our solution as a moonshot for Europe

Our arguments are ported to this breakdown effectively happening in under ten years. This negative scope is matched with a positive assessment of the economic, social and technical value created by adopting our roadmap of extreme centralization and extreme decentralization as processes running alongside each other.

## Centralization

Governance on 500 million people and billions of devices in Europe is possible by building a triangle of value by enabling VM on chips in travel documents (the current passport will become a device), in routers, applications (NB-IOT SIM VM) like lamps, washing machines, (connected) cars), smart city infrastructure, and (5G) base-stations.

The key triangle is personal device[3] (a supporting service running Estonian e-card in a dedicated European hardware with dedicated European chip (running VML zenroom), the router and the application. Protocols can diverge from and gradually fade out tcp-ip. The image below shows the dots (VM on chip) connecting across the networks that make up #IoT : BAN (wearables), LAN (smart home), WAN (connected car), VWAN (smart city).

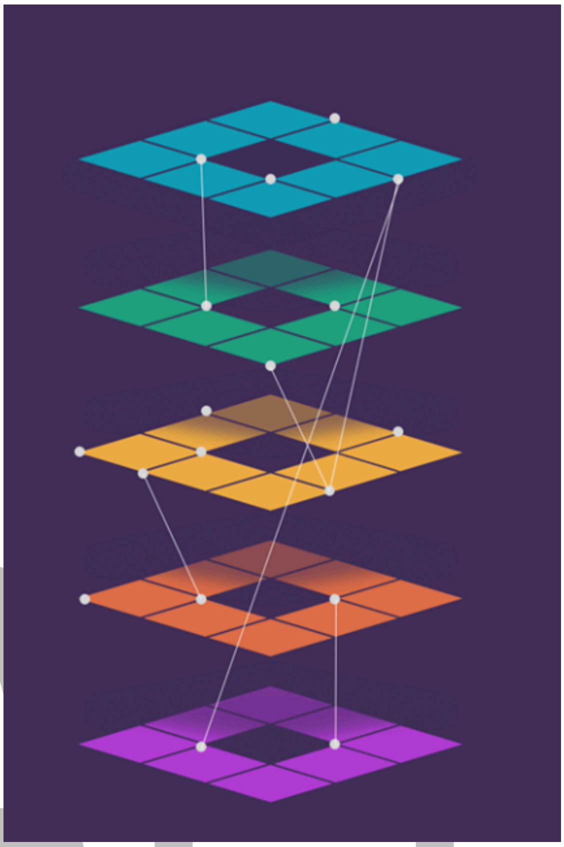

*Figure 1 Image by CIID, Copenhagen in ongoing project, with permission, slightly out of original context*

Our focus is on the space in between the dots. That is where the proactive capabilities of Big Data, analytics, emergent quantum computing and AI come into play. That space is certified by the connecting dots that create Digital Signatures[4]. If the router, application, device triangle is not apparent, then there simply is nothing.

[3] A tablet or phone which becomes the next travel document that any European citizen receives when renewing. His or her national 'passport'. Added free messaging service and horizontal services like health, taxes, payment, social local networking tuned to sharing initiatives.

[4] Digital Signatures for services (banking, payment, energy, education, care, mobility, connectivity…) and Digital Signatures for architectures (virtual and analogue enablers of connectivity) are e-seals, a tool to complement current actions on procurement and local agency as in this kind of SLA it does not matter that the original data sets and analytical platforms are not under your control. In this manner local stakeholders are a priority part of building the next layer of value, naming the new entities that are formed when AI inspired intelligence starts to see patterns unrecognizable before.

In the space between the dots there is no need to identify natural persons or for these persons to expose themselves as natural persons.

## Decentralization

Opposition is mounting, both against a national social credit system and a behavorial tracking (dynamic pricing combined with coelition.org) framework which people experience as control systems that reduces their potentiality.

Yet we cannot go back as individuals, communities and societies to analogue drivers. We can only go forward and then the digital transition towards seamless connectivity is as sound as full resource management is one of the 'solutions' of Climate Change. Full transparency and accountability in services will drastically reduce overhead, corruption and greed. People could benefit from a support system that can give them timely advice on actions and services.

Any system built, however benevolently on the one person –one number framework, will tend to gather and use more and more data. As such it is the heart of the matter that needs to be *'broken'* in order for a seamless connectivity to be not just adopted but welcomed by all generations in society.

## Economic rationales for this approach

Goods, persons, houses, situations[5] and Industrial processes all radiate data and create digital twins. These twins exist as sets of properties in an analytic layer that is in many hands at the moment but not really under multi stakeholder control. Whoever or whatever gains agency in and on that layer (which defines governance of the everyday) must grasp the practice and theory of assigning, withdrawing, validating and defining the very nature of entitlements; who/what/when/where exists how and why? The situation is hybrid in the sense that the digital twins actually begin to actuate back in the 'analogue' objects. This is the moment of ontological change. It demands a new toolset on the notion of identity itself.

The hardest concept to grasp in the Digital Transition is the relative (semi) autonomous gaze of the network itself. This network is a balance of Cloud and edge services, with AI running inside objects in everyday activities (wearables, washing machines, cars). For this network all its users are 'entities', these can be machines, people and processes (templates that predefine scenarios). It becomes clear that 'identity', as in singular identities is no a longer relevant and productive concept.

In the reactive framework we are used to dealing with three groups of actors:

- citizens/endusers
- industry/sme
- governance/legal

[5] The public review of Classification of Everyday Living Version 1.0 CSPRD03, announced in https://lists.oasis-open.org/archives/coel-comment/201805/msg00000.html, closed on 23 May 2018. No comments were received.

These all are characterized by certain qualities, 'a' for citizens, 'e' for industry, and 'o' for governance. In our current (Reference) Models and  (Reference) Architectures we build from and with these actors as entities in mind.

In the proactive vision the data flow of IoT will engender new entities consisting of different qualities taken from the former three groups. There will thus be no more 'users' who need to secure 'privacy' as the concept of privacy has to be distributed over the qualities of the new actor. Privacy then becomes privacies, plural, as in settings of devices in relation to the environment we are in (shopping, dating, working..) We are used to setting up models with entities Eaaa, Eeee, and Eooo. In this conceptual space we have built notions of privacy, security, assets, risks and threats; culminating into a model of relational behaviour: ethics. Can we envisage debate and discuss what ethics by design can look like - what kind of a model can be build with actors Eaeo, Eaao, Eeea[6]?

The most important feature of this approach is that identity becomes an activity dispersed over and managed by the person and his or her attributes profile, the object, machine or robot that performs the service and the enabling connectivity harnessed in an architecture.

Unlike the last decades of austerity and crisis management, this value layer is immensely rich and abundant. Do we really want to leave that with commercial actors aiming to create even more wealth for their shareholders?

## Security

Accountability over anonymity characterizes this approach as it underlies society in the 20th century itself. Tokenized trust is a key feature but only in the actual locality where face to face and communities of people work and live together.

This approach that builds reciprocity not over two, but three actors, is the only way to counter and overcome the incongruities that are currently eroding trust, fake news, synthetic data (information artificially manufactured, created algorithmically) and chimeras (organism contains at least two different sets of DNA), fake passports and passports for sale by national source signers.

This approach builds on the fixed identities of human beings in nationally signed passports, of goods in, GS.1 type of repositories and scenarios of behavior in taxonomies such as coelition.org and face and gait recognition capabilities and reorganizes them as ‘event’ identities.

This approach acknowledges that if we do not go back to before the very notions of Linnaeus classification and encyclopedic organization of Diderot, we will be continuously repairing, legally fighting and running behind realtime agency.

[6] Bill Morrish suggests that maybe it should Raeo, Raao, Reea , R for “reciprocity” which is the goal of disposable identity, to generate many relational lines across space outside of the one body paradigm…I like the idea that disposable identities to help individuals co-inhabit a world requiring many

Identity (and thus security) is distributed over architecture, service and phone/passport, signed in digital signatures, federated and attribute based only.

The new Directorate on Cybersecurity cannot afford to turn a blind eye to the most threatening cyber security risk from within, the sale of paper passports by certain EU countries.[7], further eroding the trust of citizens in EU institutions.

In his article *EU warns of crime risks from governments' sales of passports, visas*[8], Francesco Guarascio writes: "The European Commission said on Wednesday that programs of some EU states to sell passports and visas to wealthy foreigners could help organized crime groups infiltrate the bloc and raise the risk of money laundering, corruption and tax evasion."

### How is this overall roadmap to be achieved?

By regulating the router market, regulating the chip market and setting requirements for embedded computing as VM on chip as well as adding security requirements for #IoT applications in combination with porting security in and on paper documents to digital carriers can be achieved in the revision and updating of three major legislative frameworks: GDPR (review in 2020), the eprivacy draft regulation designed to be applicable to IoT / M2M) and the upcoming public consultation in eIDAS.

Building blocks for the realization of this roadmap are in place (e-estonian) or in development, for example in the Dutch program to realise a national public federated, attribute based Trust Framework and the European DECODE project. In which a provable computing environment is being developed alongside and as we speak and the ongoing work of dyne.org on natural language smart contracts. Zenroom[9] provides the cryptography and the sensitive data manipulation for the whole Decode project, implementing the Coconut credential scheme developed by UCL in 2018.

Validation of the approach commercially is provided by the aqui-hire of Facebook of the UCL team to build LIBRA. "In the absence of any detail on what might comprise a decentralized identity standard

[7] "Malta, Cyprus and Bulgaria are the only EU countries which sell their citizenship, issuing "golden passports" in return for investments ranging between around 1 million and 2 million euros ($2.2 million). Twenty EU states, including those three, sell residence permits, or "golden visas", to foreigners willing to invest in their new host country, with a range of between nearly 15,000 euros ($17,000) in Croatia and over 5 million euros in Luxembourg and Slovakia." https://www.reuters.com/article/us-eu-passports/eu-warns-of-crime-risks-from-governments-passports-visa-sales-idUSKCN1PH13M

[8] https://www.reuters.com/article/us-eu-passports/eu-warns-of-crime-risks-from-governments-passports-visa-sales-idUSKCN1PH13M

[9] https://decodeproject.eu/blog/smart-contracts-english-speaker

from Libra's perspective, some dots can be joined by examining the recent work of George Danezis and his co-founders at Chainspace, a startup acquired by Facebook in May."[10] Recently Microsoft announced their variation on a Coconut credential scheme.

The provable computing framework we envisage for Europe as a 500 million zone of people and 55 billion IoT devices by 2025 (worldwide)[11] is built on the assumption that data frameworks and identity management cannot be separated.

[10] https://www.coindesk.com/buried-in-facebooks-cryptocurrency-white-paper-a-digital-identity-bombshell

[11] https://ec.europa.eu/knowledge4policy/foresight/topic/accelerating-technological-change-hyperconnectivity/hyperconnectivity-iot-digitalisation_en