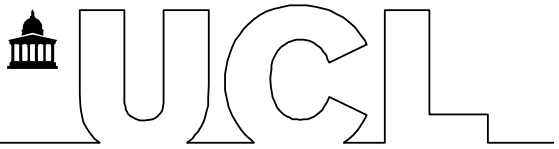
UCL DEPARTMENT OF ELECTRONIC AND ELECTRICAL ENGINEERING



MSc Telecommunications with Business

Project Dissertation

Will the Phone Number Disappear? What Will Replace it and How Long Until Then?

Sacha Nacar

August 4th 2016

Report submitted in part fulfilment of the requirements of the MSc Telecommunications with Business

UCL DEPARTMENT OF ELECTRONIC AND ELECTRICAL ENGINEERING

MSc Telecommunications with Business

Declaration

This report is submitted as a part of the MSc course in Telecommunications with Business.

I declare that this work has not been submitted for assessment in any other degree course.

I also declare that all material described in this report is substantially my own work except where explicitly and individually indicated in the text. This includes ideas described in the text and figures.

Name: Sacha Nacar

Signature: ……Nacar……

Date: August 4th 2016

Abstract

Facebook's announcement in February 2016 stating that the number one trend in 2016 would be the disapearance of the phone number has renewed interest for the future of the long-lasting E164-formatted number. Experts have been speculating on its demise for decades and with the widespread emergence of communication OTTs, it is likely that it the phone number may lose its original functionality: a communication endpoint on the PSTN. However, the phone number is not set to completely go extinct. In fact, this research demonstrates that it holds a large potential to evolve into an adequate digital identifying technology for online services. This research paper delves into the various driving trends that are leading to the dissociation of the phone number from the PSTN and its potential as a digital identifier through an analysis of its fit with requirements for digital identity systems. From this research emerges an important initiative from GSMA called Mobile Connect which links the current ubiquity and universality of the phone number with the web-centric availability of the OpenID initative. Though phone number will be around for a while in its evolutive form, this research illustrates a few scenarios and timelines that emphasize on the fact that the future of digital identity is set to evolve through digital mapping, decentralization, and the fact that a universal identifiers will become obsolete in the future, hence the potential demise of the phone number once again. Recommendations for various stakeholders of the industry include repurposing of IP backbones into IP services (eg. Messaging & Video) for Virtual DID Providers, development of Identity Brokering technologies for Online Directory services, distribution of bundled "bot" services and integration with Mobile Connect for MNOs, focus on decentralization technologies for Working Groups (GSMA & OpenID) government agencies and regulators, and integration with IP 2-factors authentication technologies for GSMA's Mobile Connect.

Acknowledgment

I would first like to thank my thesis supervisor Dr. Clive Pool of the Electronic and Electrical Engineering School at University College London. Prof. Poole provided me with great support, contacts, and insights on the topic I wanted to research. While he steered me in the right the direction whenever he deemed appropriate, he consistently allowed me to make this research paper my own.

I would also like to thank the industry experts who were involved in the interviews for this research project who have provided with tremendous guidance and have opened my mind to new subjects of studies. Without their passionate participation and input most, if not all, of the ground-breaking topics would not have been discovered for this research:

- Infobel CEO, Alain Wahba.
- TADS Community Founder, Alan Quayle.
- Tokbox/Telefonica Senior Director of Business Development, Chris Koehncke.
- GSMA Web Working Group Director, Istvan Lajtos.
- Truphone Head of R&D, James Body.
- Matrix.org Founder, Matthew Hodgson.
- Telefonica Vice President Europe, Mike Short.
- UK Cabinet Head for ICT Resilience, Nigel Brown.
- Neustar VP of Research and IETF Modern Charter Chair, Tom McGarry

I would also like to acknowledge Prof. Andy Valdar of the Telecommunication with Business MSc. programme at University College London as the second reader of this thesis, and would like to thank him for his valuable tiem spent commenting on my research.

I am very grateful to all the discussions I have had on the topic with friends, professors, family members, and other industry professionals who have opened my mind to new areas of research and discussion.

Finally, I would like to express my gratitude to my parents for providing me with their continous support and encouragement throughout my degree and throughout this research. This accomplishment would not have been possible without their support. Thank you.

Sacha Nacar

Contents

I Introduction & Background **13**

II Research and Methodology **15**

1 Research Objectives **15**

2 Interviews & Discussion Topics **16**

3 Secondary Sources **16**

4 Research Limitations **17**

III Analysis & Discussion **18**

5 Driving Forces & Factors **18**

5.1 Next-Generation Networks and Nationwide Number Portability 18

5.2 The Importance of Certification & The Dissociation of Numbering from the Network 19

5.3 The Rise of Social Media and Social Profile Verification 20

5.4 Real-time Communication APIs and the Rise of Contextual Identity 21

5.5 The Growing Penetration of Mobile Broadband & Smartphones - A Threat to the PSTN . . . 22
5.6 Teens Shape the Way We Communicate & The Decline of Voice . . . 23
5.7 Fragmentation of Devices & the Need for Convergence . . . 24
5.8 Virtual & Disposable Numbers - Contextual Identity for the PSTN . . . 25
5.9 Concerns About Data Protection, Security, Privacy, and Anonymity & Emerging Solutions . . . 26
5.9.1 Security & Data Protection . . . 27
5.9.2 Privacy & Anonymity . . . 27
5.10 The Rise of e-Government . . . 27
5.11 Bringing Emergency Services to the Digital Age . . . 28
5.12 Internet Giants Become MVNOs: Google Fi, Apple SIM & Facebook's Internet.org 30

6 Extinction or Evolution? 31

7 Requirements for Next-Generation Digital Identity Systems & How the Phone Numbers Fits 32

7.1 Ubiquity & Universality . . . 32
7.1.1 Description . . . 32
7.1.2 Relevance of the Phone Number . . . 33
7.2 Federation & Interoperability . . . 34
7.2.1 Description . . . 34
7.2.2 Relevance of the Phone Number . . . 36
7.3 Security . . . 37
7.3.1 Description . . . 37
7.3.2 Relevance of the Phone Number . . . 38
7.4 Privacy, Trust & Control . . . 39
7.4.1 Description . . . 39
7.4.2 Relevance of the Phone Number . . . 40

7.5 Contextual Identity . . . 41
7.5.1 Description . . . 41
7.5.2 Relevance of the Phone Number . . . 42
7.6 Spamming, Spoofing & Reputation Management . . . 42
7.6.1 Description . . . 42
7.6.2 Relevance of the Phone Number . . . 43
7.7 Legislation, Regulation & Governmental Impact . . . 44
7.7.1 Relevance of the Phone Number . . . 44
7.8 Constraints & Challenges . . . 45

8 Scenario Planning 46

8.1 Use of Disposable Numbers Delay the Eclipsing of the PSTN . . . 46
8.1.1 Impact - 2 . . . 46
8.1.2 Likelihood - 4 . . . 47
8.2 Voice & Messaging OTTs Become Primary Means of Communication for Most . 47
8.2.1 Impact - 5 . . . 47
8.2.2 Likelihood - 5 . . . 47
8.3 WebRTC Becomes Widespread Across Browsers and Platforms . . . 48
8.3.1 Impact - 4 . . . 48
8.3.2 Likelihood - 5 . . . 49
8.4 Mobile Internet Ubiquity Led by "Social" MVNOs . . . 49
8.4.1 Impact - 5 . . . 49
8.4.2 Likelihood - 3 . . . 50
8.5 The Smartphone Becomes Central to the Internet of Things . . . 50
8.5.1 Impact - 3 . . . 50
8.5.2 Likelihood - 4 . . . 51
8.6 Decentralization, Convergence & Mapping Lead to the Obsolescence of a Universal ID . . . 51

8.6.1 Impact - 5 . . . 51
8.6.2 Likelihood - 4 . . . 52

IV Conclusion & Recommendations 53

9 Prediction Timeline 54

9.1 Short Term (2-3 years) . . . 54
9.2 Medium Term (3-7 years) . . . 55
9.3 Long Term (7-20 years) . . . 56
9.4 Very Long Term (20+ years) . . . 57

10 Will the Phone Number Disappear? What Will Replace it and How Long Until Then? 57

10.1 Will the Phone Number Disappear? . . . 57
10.2 What Will Replace it? . . . 58
10.3 How Long Until Then & The Problem with Predicting the Future . . . 58

11 Recommendations 59

11.1 Commercial . . . 59
11.1.1 Online Directories . . . 59
11.1.2 Virtual Number (DID) Providers . . . 59
11.1.3 Mobile Operators . . . 60
11.1.4 Internet Companies with Telco Infrastructure . . . 60
11.2 Regulatory . . . 61
11.3 Governmental . . . 61
11.4 Working Groups . . . 62
11.4.1 OpenID . . . 62
11.4.2 IETF . . . 62
11.4.3 GSMA . . . 62

11.4.4 ITU 63
11.5 Winners & Losers 63

V Appendices **64**

Glossary of Abbreviations, Initiatives, Hacks, and Services

- **Blockchain:** The Blockchain is a distributed database that maintains a continuously-growing amount of data records secured from modification or revision. The Blockchain enables the security and decentralization of a transaction's accountability.
- **Connect.gov:** Similar to Gov.UK Verify, Connect.Gov enables individuals to use a third-party Sign-In Partners to access agency applications.
- **Consensus Protocol:** Consensus protocol allows the verification of transaction and identity by reaching computerized consensus instead of going through centralized authoritative systems. The Stellar Consensus Protocol provides a way to reach consensus without relying on a closed system to accurately record financial transactions and is a construction for federated Byzantine agreement (FBA).
- **Covert Redirect:** Covert Redirect is a vulnerability of the OAuth and OpenID mechanisms which allows attackers to gain information from users' profiles.
- **CNAM:** Caller ID Name databases allow VoIP services and applications to identify callers and differentiating real peopl from telemarketers or robocallers.
- **Ethereum:** Ethereum is a decentralized platform that runs smart contracts based on the blockchain: applications that run exactly as programmed without any possibility of

downtime, censorship, fraud or third party interference.

- **Facebook Account Kit:** Similar to Mobile Connect, Account Kit allows people to quickly register for apps and log in using just their phone number or email address. Account Kit is based on Facebook's binding of phone numbers to profile information and their implementation fo OAuth.

- **FIDO:** The FIDO Alliance addresses the "lack of interoperability among strong authentication devices as well as the problems users face with creating and remembering multiple usernames and passwords". The FIDO Alliance plans to change the nature of authentication by developing specifications that define an open, scalable, interoperable set of mechanisms that remove reliance on passwords to securely authenticate users of online services.

- **Free Basics:** Free Basics is one of Internet.org's initiatives which provides people with access to basic websites for free including news, job postings, health and education information, and communication tools like Facebook.

- **FutureID:** The FutureID project is a European initiative based on the European Commission's Single Digital Market strategy to "build a comprehensive, flexible, privacy-aware and ubiquitously usable identity management infrastructure for Europe". It integrates the eID technology, trust infrastructures, emerging federated identity management services, and modern credential technologies.

- **Gov.UK Verify:** Verify is the UK's initiative to provide online identity certification through trusted third-party identity brokers for access to government services. Certification parties range from banks and the royal mail, to mobile operators through Mobile Connect.

- **Hashgraph:** Hashgraph is an alternative to the Blockchain. It consists vastly of the same concept except for the fact that all new transactions, whether conflicting or not with the

existing "chain", are kept. The Blockchain is like a growing tree that constantly grows and sees all but one of its branches chopped off. In hashgraph, no branch is discarded.

- **ID4D:** The ID4D initative from the World Bank Group aims to facilitate access to services and rights for all by supporting progress toward identification systems using 21st century solutions. The initiative aims to help countries reach the Sustainable Development Goal target of "providing legal identity for all, including birth registration, by 2030".

- **Internet.org:** Internet.org is Facebook's initiative to provide internet connectivity to the whole world through the use of high-altitude long-endurance planes, satellites and lasers.

- **Matrix.org:** Matrix is a an open standard for decentralized persistent communication which aims at allowing any entity to run their own identity servers which is interoperable with any other service that implemented Matrix's open standard. This means that users on OTT A could chat with users on OTT B.

- **Mobile Connect:** Mobile Connect is a "secure universal log-in solution. Simply by matching the user to their mobile phone, Mobile Connect allows them to log-in to web-sites and applications quickly without the need to remember passwords and usernames." Mobile Connect works by allowing users to register to services through OpenID & OAuth technologies through their phone number. The verification is performed through the use of SMS 2-factor authentication.

- **MODERN:** The MODERN working group will define a set of Internet-based mechanisms for the purposes of managing the acquisition and resolution of telephone numbers (TNs) in an IP environment. The Working Group has investigated the use of the blockchain to decentralize the distirbution mechanism of telephone numbers along with the use of X509-like credentials for verification of this distribution and further communication.

- **NGNP:** Non-Geographic Number Portability is part of IETF's Modern draft and allows the portability of numbers across the United States through the deployment of IP tandems and the creation of non-geographic area codes.

- **NSTIC:** The U.S. National Strategy for Trusted Identities in Cyberspace is a US government initiative that aims to improve the privacy, security and convenience of online transactions through collaborative efforts with the private sector, advocacy groups, government agencies, and other organizations. The strategy had four guiding principles: privacy-enhancing and voluntary, secure and resilient, interoperable, cost-effective and easy to use.

- **OAuth:** The OAuth 2.0 authorization framework enables third-party applications and services to obtain limited access to an HTTP service provided by an online platform. These HTTP services are usually database containing information about a person's profile. The online platforms offering OAuth authentication to third-party services are usually social media platforms like Facebook, Google, LinkedIn, or Twitter.

- **OpenID Connect:** Connect is the technology powering the OpenID initiative. OpenID Connect is an identity layer on top of the OAuth 2.0 protocol. It allows Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User.

- **OpenID:** OpenID allows an online user to use an existing account to sign in to multiple websites, without needing to create new passwords. At the front-end, the experience feels similar to OAuth authentication. However, OpenID is a central platform that services connect to, while OAuth requires individual implementation ont he service platform's end. The particularity of OpenID is that it is a decentralized system of providing identity on the web - users can choose their providers and no entity owns OpenID privately.

- **OpenID MODRNA:** OpenID's MODRNA working group stands for "Mobile Operator Discovery, Registration & autheNticAtion" and is intended to mobile network operators (MNOs) providing identity services for online individuals such as the Mobile Connect initiative.

- **OTT:** Over-The-Top content is the delivery of audio, video, and other media over the

Internet detached from an operator in the control or distribution of the content. In this research, OTT is used to specifically describe voice/video/messaging communication applications such as WhatsApp or Viber.

- **Project Loon:** Loon is Google X's initiative to provide internet connectivity to the developing world through the used of helium-filled balloons navigating in the air.

- **Social Graph:** The social graph is a graph that illustrates personal relations of internet users. Facebook's Graph API allows developers to build relations between people through the various attributes (whether interests, location, education, workplace, etc.) in their applications.

- STORK & eID: STORK & eID are technologies powering the FutureID initiatives in a cross-border manner. The objective of the STORK project is to establish a European eID Interoperability Platform that allows citizens to establish new e-relations across borders, just by presenting their national eID.

- **TOR:** Tor is a software and an open network that allows individuals to stay anonymous on the web when browsing. TOR uses Onion routing to conceal a user's location and IP address.

- **WebRTC:** WebRTC is an open project intially developed by Google and Mozilla Friefox that provides browsers and mobile applications with Real-Time Communications (RTC) capabilities via simple APIs built in right into the browser. This way, no plugins (such as Flash or Chrome Extensions) or applications are needed to be downloaded to have a real-time audio, video, or messaging conversation on the Web. Developers can easily build online platforms that leverage WebRTC to provide audio, video, and messaging services inherently interoperable with any device out of the box.

Part I

Introduction & Background

The phone number has been around for over 150 years and over that period it has provided a ubiquitous way for people around the world to be identified and to communicate on the PSTN. In the last decade, voice calls have gone from devices, the phone, to applications and are now becoming mere embeddable features in applications through APIs.

The advent of IP technologies and the transition to NGN platforms has given rise to many new opportunities for communication and identification. For example, Voice over IP, OTT messaging apps, or WebRTC have allowed for communication to become cheap and fragmented. As interest grows over free/cheap communication, fragmentation of identity, anonymity and privacy, new generations rarely choose the regular PSTN voice calls as their primary means of communication.

David Marcus of Facebook recently advocated that 2016 would see the disappearance of the phone number as the number one trend. The demise of the phone number has long been an intense discussion topic and one that draws from many areas of expertise making the debates even more heated. With the introduction of the Internet and IP technologies, ICT industry experts have long thought that the PSTN's main endpoint technology would be replaced by IP addresses, emails, third-party IDs, and more recently decentralized technologies like the blockchain. Though the E164 has been through many cycles of innovation in terms of numbering with the ITU - with the example of tollfree numbers, shortcodes, or emergency services - the recent revolution in digital identity and web authentication has allowed the phone number to take on a new role: a digital identifier for online services. In fact, most OTT applications today leverage the phone number to establish some kind of identity and perform profile verification and authentication of their user base. It is undeniable that the heavily-anchored numbering system's ubiquity and availability is highly attractive for parties looking to implement centralized authentication and identification systems.

This research attempts to determine whether the phone number is set to disappear and be replaced or whether it has a future based on its evolution as a digital identifier. As communication systems switch to IP and fragmentation of identity over the web rises, is the phone number still relevant as a means of identification for IP communication platforms? Will it disappear? What will replace it and how long until it is replaced?

Part II

Research and Methodology

1 Research Objectives

The research objective was to analyze the most important driving trends leading to the phone number's extinction or evolution to predict its future as a digital identifier and develop scenarios that would benefit industry players ranging from Mobile Operators to Working Groups. It is important to note what this research is not about: determining the most suitable online identifier of the future. This is a much broader topic which requires intensive technical and commercial research and knowledge of all technologies available today. This research focuses on the relevance of the phone number as a digital identifier and the various trends, factors, and technologies that affect its relevance.

Trends in both the evolution of identity and communication were investigated as they are intrinsic to one another: without identity, communication is practically impossible; without communication, identity is pointless.

The research body consists of 3 parts: the analysis of the driving trends of the phone number's evolution or extinction, the analysis of requirements for digital identifiers along with the evaluation of the phone number as a digital identifier, and finally scenario planning based on strong trends and evolution of digital identity.

2 Interviews & Discussion Topics

ICT industry experts were self-selected to weigh in on some of the topics that ranged from the "Driving Trends of Communication & Identity" to "Candidates for Identity Management" or the various commercial opportunities.

Figure 1 below illustrates the selection of interviewees that contributed to the findings and guidance of this research.

- Consultants
  - Chris Koehncke
  - Alan Quayle
- Internet/VoIP/Directories
  - Alain Wahba - CEO Infobel
  - Matthew Hodgson - Founder Matrix.org
- Working Groups
  - Istvan Lajtos - Director WWG GSMA
  - Tom McGarry - VP Neustar/IETF
- UK Cabinet
  - Nigel Brown - Head of ICT Resilience
- Operators
  - Mike Short - VP Telefonica
  - James Body - Head R&D Truphone
- Academia
  - Peter Cochrane - UCL
- Regulatory
  - Greg Mook - Vodafone

Figure 1: List of Interviewees

3 Secondary Sources

Secondary sources included OECD, GSMA, Whitehouse.gov, and Gov.UK public reports along with consumer reports from Ofcom, Ericsson Lab, and McKinsey. Additionally, IETF and W3C drafts were reviewed and investigated to understand the technology behing the evolution of identity and community and the web. Figure 2 illustrates the various secondary sources that played a crucial role in providing either direct content or guidance and understanding in drafting this research paper.

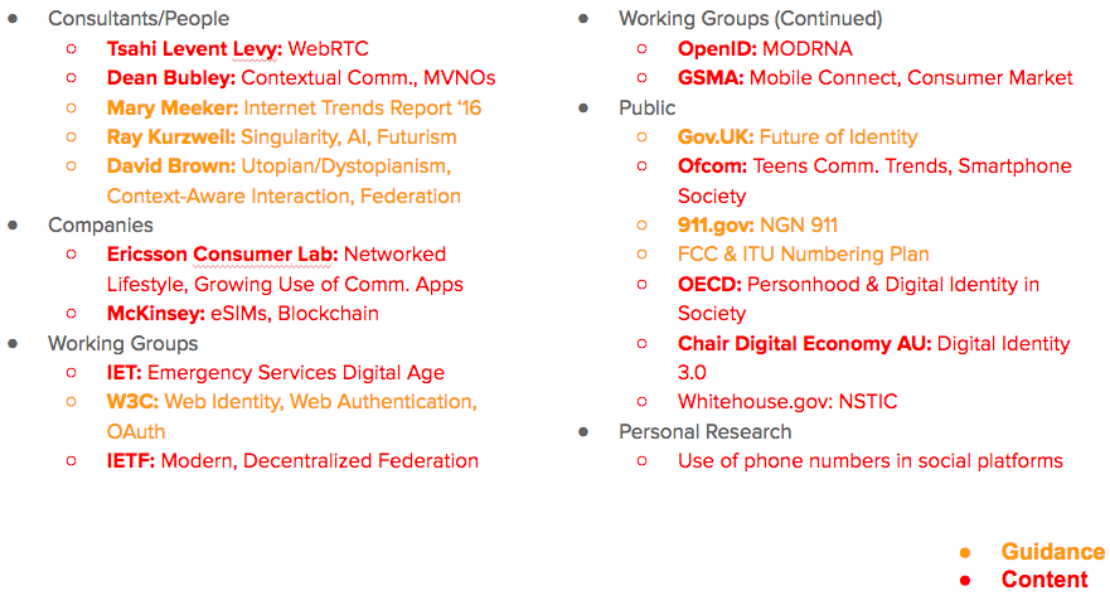


Figure 2: List of Secondary Sources

4 Research Limitations

This research holds a few limitations, specifically in the choice of approach to the topic. The future of the phone number depends on the future of identity and communication, both of which are very large topics to cover and touch upon many factors that will influence the future of the phone number. This research attempts to focus specifically on factors that directly affect the evolution of the phone number as a digital identifier. However, this focus also lead to omissions in trends, factors, or scenarios that could affect the future of digital identity in general and hence affect the future of the phone number. For example, political and human behavior factors towards identity will deeply impact the future of digital identity. These topics have not been covered in detail in this research.

Additionally, this research focuses on the identification of humans. Though the topic of the Internet of Things is covered, it is centered around the identification of people through various central devices such as the smart phone or other autononous interfaces.

The views of the individual interviewees are largely cohesive with findings from the secondary

research but leaves an inherent biased because the experts' results are self-selected.

Due to the time constraints, most interviews were conducted at a very early stage in the research which led to many arbitrary predictions on scenarios' impact and likelihood. Should this research be extended, it would be wise to conduct a second round of interviews to gather expert opinions on the scenario planning and the timeline developed.

Finally, predicting the future is a difficult task as the same rate of change is often assumed when in fact change is happening at an exponential rate. This makes predictions beyong 15-20 years almost certainly inaccurate.

Part III

Analysis & Discussion

5 Driving Forces & Factors

5.1 Next-Generation Networks and Nationwide Number Portability

The development of next-generation, all-IP, platforms has allowed network operators to move away from circuit-switched networks and conduct all types of communications, whether voice, video, or messaging over IP-based networks. With the emergence of IP platforms to replace circuit-switched networks, telephone numbers do not have to have a presence (or connection) to a particular switch on the PSTN anymore and it means that Nationwide Number Portability is achievable. Neustar's Tom McGarry explains that with the development of IP-based networks, telephone numbers are assignable on a non-geographic level and ported nationwide in the USA through the development of NGNP[46] (See Appendix P [V]). NGNP means that phone numbers no longer need to be associated to particular switches, are portable and usable as unique identifiers of people rather than switches (or places). NGNP will allow mobile carriers that only operate in a small region, e.g., one state to port numbers across LATA even with no point

of interconnection in the local access of the network. This means that individuals get to keep their phone numbers even if they move to different states which renders these numbers just as immutable as physical addresses.

NGNP could also benefit the international market. Rodrigue Ullens, founder of SIP Trunking company Voxbone, voiced the concern that "with the advent of IP technology, the marginal cost of transport of a voice call is close to zero"**[45].** Hence, inter-area call charges should be dropped to reflect this marginal cost. With the development of NGNP and non-geographic numbers, this could one day be a reality. Such a trend is already observable with Europe's Single Digital market strategy to force network operators to eradicate roaming charges and termination costs which will deeply affect the international use of the PSTN for voice calls.

5.2 The Importance of Certification & The Dissociation of Numbering from the Network

The emergence of E-Commerce and an economy driven by online individuals has called for the need of adequate verification of identity and certification of profiles [1]. Companies like VeriSign focus on providing such services and these services often base their verification mechanism on information tied to the phone number provided by businesses.

As a matter of fact, the phone number is a binding that ties an individual to billing information, an address, and ultimately a person that is reachable on their device (See Appendix W [V]). For example, social and dating profiles use two-factor authentication to verify users. Additionally, online number directory services like Infobel become identity brokers as they can verify business profiles based on information linked to the phone numbers provided.

Alain Wahba, Infobel's CEO, illustrates that there have been cases when certification company Thawte only certifies a business profile once it is first published and certfied on Infobel (See Appendix V [V]) - the phone number becomes an element of certification. This is where the future of the phone number lies, it is becoming less of a communication endpoint (or address) and more of a unique identifier tied to a profile. CNAM databases (See Glossary) become more

valuable to the future of the phone number than the E164's original use as a communication endpoint.

The result is that the numbering system becomes dissociated from the PSTN network and can be used as an identifier in various cases independent of the PSTN, such as identity verification.

5.3 The Rise of Social Media and Social Profile Verification

Wahba describes the paradox that people have been removing themselves from directories but increasingly registering with social networks by adding much more personal information as used to be available on directories. The challenge for the Digital Identity industry became to link the social information to the phone number because when linked, it becomes a very powerful, personally-connected, and highly verifiable identity (See Appendix V [V]).

The massive adoption of social media has opened these platforms to the opportunity of becoming identity brokers. Up until now this was mainly powered by the use of username and password along with integration through OpenID (See Glossary) and OAuth (See Glossary). However for the last few years, social platforms have leveraged the use of the phone number to create and verify user profiles through 2-factor authentication based on SMS. Though Facebook advocates for the disappearance of the phone number in 2016[47], their Messenger application heavily leverages the use of the phone number to create an ubiquitous ecosystem (See Appendix A - [V]). Another recent and powerful example includes Facebook's recent launch of Account Kit[2] which allows developers to build applications that authenticate users using solely their phone numbers which are linked to Social Graph (See Glossary) - the technology that powers profile discovery. Account Kit is the most recent initative to join a group of new identity management systems leveraging social graph technologies, the phone number, and 2-factor authentication like Twitter's Digits [3].

5.4 Real-time Communication APIs and the Rise of Contextual Identity

Throughout the last decade, not only did voice and messaging go from being the most important applications of a telephone device to becoming one of many applications on a smartphone, voice and messaging have now become embeddable features in these applications [4].

In the late 1990s and early 2000, traditional telephony had moved to IP with the rise of voice-over-IP services. In the 2010's, voice had moved to the Web thanks to the development of new real-time technologies that powered this change. Technologies like Flash, telecom APIs, and later WebRTC (See Glossary), all enabled voice, video, and messaging to become easily embeddable in all sorts of web pages, sites, and applications. Application and web platform developers no longer had to create dedicated applications for real-time media usage, it was now accessible as embeddable features through the implementation of real-time communication APIs. Examples include Facebook with chats, voice, and video calls right on the Facebook platform or online video bank clerks right in a user's online bank account page.

Static web and real-time communication are merging to become almost indifferentiable and web or login credentials can also be used as communication identities.

James Body believes with the rise of these technologies it has now become extremely easy and cheap to build a communication path to anyone (See Appendix R [V]). Coupled with today's value for independent but integrated online personas, the development of these technologies led to the multiplication of communication platforms and OTT's (See Glossary) and, hence, to the rise of contextual identity.

This fragmentation of identity has given individuals the power to reveal different aspects of their identities depending on context. For example, someone using to a job interview video-conferencing platform would log in using his or her LinkedIn profile rather than Facebook, resulting in the platform having access to this person's LinkedIn information which may differ to some extent from that individual's Facebook profile information.

The rise of contextual identity on the web has also been powered by the development of

single sign-on authentication technologies like OAuth (See Glossary) and OpenID (See Glossary) which allow for users to decide on their identity brokers when authenticating to service platforms as well as the level of information that the service can access from that identity broker. For example, authenticating to the job interview platform could be done via the Facebook, LinkedIn, or Google identity brokers and the user signing on could filter what type of information the platform would have access to. For example: age, education, occupation, address book, etc.

5.5 The Growing Penetration of Mobile Broadband & Smartphones - A Threat to the PSTN

Mobile is overtaking the use of fixed lines and we now live in a "Mobile First" society. The mobile industry continues to scale rapidly, with a total of 3.6 billion unique mobile subscribers at the end of 2014 (See Appendix B [V]). Half of the world's population now has a mobile subscription—up from just one in five 10 years ago. An additional one billion subscribers are predicted by 2020, taking the global penetration rate to approximately 60% (See Appendix C [V]). There were 7.1 billion global SIM connections at the end of 2014 [5].

Sub-Saharan Africa has seen the benefit of implementing mobile instead of wired-networks. These regions have seen tremendous innovation on mobile technologies even with SMS services like mobile banking. In these regions, the PSTN is still very prominent especially with SMS-based industries like mobile banking. However, regions built on mobile technologies will see a growing penetration of mobile broadband and smartphones and SMS economies will also be threatened by the rise in OTTs and other smartphone applications.

GSMA Intelligence predicts that more than four out of five people will have access to 3G networks by 2020, up from 70% today[5]. The report also states that 4G networks are being rolled out at a faster pace than what was the case for 3G. While it took 10 years for 3G network coverage to reach half of the global population, it will take 4G networks eight years after launch to reach the same milestone, therefore reaching this level in 2017 [5].

Mobile has been a staple of the developing markets but smartphone adoption has been

extending beyond developed markets. Smartphone adoption rate is expecting to reach an average of 65% across the globe by 2020 (See Appendix D [V]).

While an increase in the adoption of smartphone and mobile subscriptions globally means the phone number is reaching closer to full ubiquity, mobile broadband and smartphones have allowed for the possibility of OTT/IP communication apps to replace the PSTN use for voice and messaging. As their penetration rate continues to grow in the rest of the world, more regions will have access to these technologies and the PSTN, along with the traditional use of the phone number, will become ever more threatened. In fact, WhatsApp has recently announced that their application alone sees 100 million voice calls every day. This is highly significant knowing that WhatsApp had launched the voice calling feature only a year ago.

In fact the SMS market is also experiencing a hit due to messaging OTTs. Until now, only the general consumer SMS market was affected due to the plethora of messaging applications and embedded features. However, with the introduction of application-to-person messaging routes in applications like WhatsApp or Viber along with IP-based 2-factor authentication applications like Authy, the SMS market as a whole is seeing its usage decline[50].

5.6 Teens Shape the Way We Communicate & The Decline of Voice

Ofcom Chief Executive Ed Richards stated that the 'millennium generation' is shaping the communications habits for the future [7].

The Ofcom study of nearly 2,000 adults and 800 children found that six year olds have the same understanding of communications technology as 45 year olds. Also, more than 60% of people aged 55 and over have below average 'DQ' scores, the resulting "Digital Quotient" index (See Appendix F [V]).

The study also demonstrates that 12-15 year olds are developing fundamentally different communication habits than older generations. Children aged 12-15 are least likely to have a conversation on the telephone. Only 3% of their communications time is spent making voice calls, while the vast majority (94%) is text based - like instant messaging and social networking.

In contrast, UK adults average 20% of their communication time on the phone. UK adults do embrace digital text-based communications but the traditional email, which is used for 33% of their time spent communicating compared to just 2% among 12-15s, is their most popular means.

Not only are younger generations abandoning the use of the PSTN but also voice in general. Text-based messaging is overtaking voice and the decoupling of the phone number from the PSTN network, and from its original voice use in general, to become solely a unique identifier becomes even more apparent.

5.7 Fragmentation of Devices & the Need for Convergence

Device ownership per consumer is increasing in both personal connected devices like smartwatches, as well as connected household devices like smart TVs and remote home monitoring systems. Based on research in 12 countries, it was found that the average number of devices connected to the internet has increased to 4.1 devices in 2015 [9].

Wahba describes that our current situation is one of "one-to-many", one main device (being the smartphone) with many applications (or endpoints). However, the increasing amount of personal devices could move this situation to one of "many-to-many" where a single individual is reachable on multiple application endpoints and on multiple devices (See Appendix V [V]).

Additionally, some argue that the future of computing seems to be about a set of platform and device-independent services that can run on very simple devices. We are entering a post-device era[52], one fueled by the Internet of Things and the power of Deep Learning.

As the fragmentation communication endpoints (whether on applications, locations or devices) will bring the need for convergence to happen. As individuals register with more applications and add them to their various devices it becomes evident that to stay connected with each other, individuals in their communication circles will either have to do the same (which might become inconvenient) or upcoming technologies like Artifical Intelligence will allow for this convergence to happen.

James Body raises the point that with the emergence of AI, intelligent bots could well be the solution to this fragmentation problem. We would be "allowing the bot or the agent that is sitting between the network and you to make some kind of decision about what to do with that call or message based on purpose and precedence" (See Appendix R [V]). Apart from

Artificially intelligent assistant could be setup by both individuals and set up the connection in some sort of hand-shake format that considers the identity and location of the communicators and their preferences for communication. For example, Sally would tell its assistant to contact Bob. At this point, Sally's assistant finds Bob's assistant based on some sort of directory. Bob's assistant knows what Bob is doing and what his preferences are and shares these with Sally's assistant to establish the communication channel based on these parameters (eg. voice, message, or delayed, or not at all). Of course, this process would happen instantly and seemlessly.

Facebook is a strong advocate for the convergence of all services into personal assistant platforms. According to David Marcus, Facebook M, their smart assistant, would make it " so much easier to do everything in one place that has the context of your last interactions, as well as your identity - no need to ever login - rather than downloading apps that you'll never use again and jumping around from one app to another."[47] It is interesting to note that Google has very recently launched their own AI-powered assistant designed for enterprise customers[53].

A very important move towards this convergence was deployed by Apple in their recent iOS10 release. In June 2016, Apple unveiled their iOS10 release that now includes a third-party API for the proprietary 'phone' app. This means that any third-party app's calling service like WhatsApp, Facebook, or Skype, will work through the central 'phone' application on Apple devices [54].

5.8 Virtual & Disposable Numbers - Contextual Identity for the PSTN

DID & SIP Trunk provisioning services like Twilio or Voxbone that provide virtual numbers have powered many new services that offer "loading" of multiple phone numbers on a SIM card or

smartphone applications. Fueled by the growth in the need for individuals to have independent identities while being interoperable with the PSTN, fully-fledged IP carriers like Truphone or OTT applications like OnOff[14] allow individuals to enable phone numbers for a particular uses like selling a car or contacting someone in online dating communities. The emergence of Disposable numbers allow for users to have contextual identities even on the PSTN, without having to switch SIM cards constantly, while keeping a central identity to the service they are using.

This trend is interesting as it ties the phone number back to its voice use and the PSTN while disregarding its capabilites for a centralized identity. It is undeniable that Virtual and Disposable numbers have caught on in the past couple of years with the emergence of many services like Google Voice, OnOff[14], Tossable Digits[10], Ring Me Maybe[11], Burner[12], or Hushed[13], and address a need of the population resulting in the extension of the more "traditional" use (voice/PSTN communication) of the phone number.

5.9 Concerns About Data Protection, Security, Privacy, and Anonymity & Emerging Solutions

The shift to the economy of people or "Sharing Economy" and customer-to-customer transactions, fueled by affordable, powerful mobile devices, intuitive apps and hyper-connectedness via social media platforms, has one very distinct consequence: people produce and share an exponentially increasing amount of private data [1]. With the growing number of government surveillance programs, cyber attacks and data breaches, there has been a growing push back against gathering data about individuals online and growing concerns about data protection, online privacy, anonymity, and security. Individuals today have an increasing need to regain and retain control over their own data. They want to decide which data to share, how much and when and they want the choice to revoke their data from any provider [1]. This trend has resulted in the development of solutions in two distinct areas:

5.9.1 Security & Data Protection

Growing concerns for security against identity theft have fueled the development of 2-factor authentication mechanisms, initially powered by a combination of online credentials and SMS messages. Initially developed to provide users with added security, 2-factor authentication has become the go-to solution for next-generation identity systems based on the phone numbers like Facebook's Account Kit [2]or GSMA's Mobile Connect [15].

5.9.2 Privacy & Anonymity

The concerns for sustained privacy and anonymity on the web, along with the rise of persistent IP addresses provided by the introduction of IPv6, have led to the development and introduction of new technologies like the TOR project (See Glossary), the Blockchain, and private browsing which, all combined, power the subjacent DarkNet.

These concerns have led to ever more fragmented identity systems. Most users maintain multiple digital identities, private and work-related, and value the independence of those different online personas. These identities can sometimes be public, partial or even anonymous, however people want an integrated way to manage these independent digital identities [1]. The digital identity system of tomorrow will have to provide the flexibility and integration required for the different types of transactions.

5.10 The Rise of e-Government

Telefonica's Mike Short believes that it is important to consider how identity management is going to change irrespective of telephony and addressing because it will work with numbering in some cases and with addressing in some cases. The most important point to consider in terms of the future of identity management is where the leadership is coming from. Mike Short states that this leadership will be coming from governments that say "we need verification of identity for certain services from the government" (in the UK) and "we need secure access online consistently handled for a range of services in the USA". (See Appendix Q [V])

Mike Short stresses that it is important to note that it is the government drivers that led to the design of telephony systems, numbering systems, or addressing systems. Therefore, the government drivers will lead to the design of the digital identity of the future.

In response to the growing concerns about data security and fraud, governments are globally addressing the shortcomings tied with the current identification and authentication frameworks for people and devices to allow both the public and private sectors to offer more services on the Web.

Whether to prevent fraud or terrorism, the need for governments to offer convergent and reliable identification and authentication systems for the private and public sectors will grow as more transactions are performed on the web. Hence, authenticating citizens securely while identifying accurately will be a demand driver for the public sector.

Such initiatives have launched in the United States like Connect.gov, but also in Europe like Gov.UK Verify or Europe's eIDAS which allow citizens to use government services on the web while being securily identified.

5.11 Bringing Emergency Services to the Digital Age

Enabling emergency services for the current widespread usage of data services includes the upgrade of Emergency Services and call centers along with the proper regulation of OTT services to allow access for emergency services.

We are now 'Digital by Default' and data usage dominates voice, just like smart mobile handsets have overtaken land lines [19]. Ofcom figures show younger generations are more likely to use data services including text and social media than voice. Most calls are made from mobiles - and with features like call trace, messaging , video and mapping, the modern smart mobile is much more capable than the PSTN-connected landlines to greatly improve triage and response at emergency call centers[19]. Even though control centre systems are also being upgraded to access smarter handsets in initiatives like Next Generation 911 (NGN911) in the US, they do not fully utilize these capabilities. Additionally, the initiatives that will

allow emergency services to keep up with communication technology used by the public are still fragmented.

The deployment of IP-based telecommunication networks has enabled the decoupling of application layers and the emergence of OTT providers that provide similar voice and messaging services than the PSTN without being regulated like network operators. The main regulatory issue has been whether OTT providers should be considered as telecom services (voice or data) or telecom infrastructure, and therefore whether they should be subject to regulatory obligations like legal intercept and emergency call access or not.

As adoption rates of these Media (Voice & Messaging) OTTs increase and become the main means of communication for some, it seems to be crucial that they allow access to emergency calling. However, the very nature of IP communications means that the VoIP sessions are often location independent and their reliance on electricity-supplied devices makes them unreliable in disaster scenarios.

In May 2015, the European Commission stated in its Digital Single Market communication that "Telecoms operators compete with services which are increasingly used by end-users as substitutes for traditional electronic communications services such as voice telephony, but which are not subject to the same regulatory regime."[21]

After Commission re-examining a wide array of policies that affect the internet sector, it seems certain types of OTTs will have to comply to allowing emergency call access. As stated, "a large number of stakeholders consider that all the voice services perceived by the users as substitutive to the current PSTN voice service and which also give access to E.164 numbers should be subject to the same obligations regarding the access to emergency services" [20]. In the recent European Commission communique, regulators support this mandate for all communication services (including OTTs) that give access to numbers in the numbering plan [20].

Being enabled for emergency services, the PSTN was always thought of as the network of 'last resort' (See Appendix T [V]). However, if OTTs were to offer 911 services access, it could be the last draw for the PSTN as a voice or messaging communication network.

5.12 Internet Giants Become MVNOs: Google Fi, Apple SIM & Facebook's Internet.org

Apple, Google, and Facebook have recently launched initiatives that bring them closer to becoming MVNOs. For example, Apple has released Apple SIM for iPad which provides the ability for the consumers to choose a carrier partners' cellular data plan right on their iPad.

The most interesting is Facebook, which have explicitly voiced out their objective to implement telco infrastructure within 10 years (See Appendix H [V]). Apart from their voice/messaging OTT applications, Facebook has already launched various telco-based solutions like their acquisition of Endaga or the launch of Internet.org which aims to provide free internet connectivity to the developing world.

These companies identify their users by means of single sign-on proprietary identifiers (eg. Google Email, Facebook ID) which are usually composed of email addresses and are compatible with OpenID and OAuth integrated.

A McKinsey report defines Google's Project Fi as one of the "potentially highest-impact and most disruptive new ventures" in the E-SIM industry. The report states that "Social-media voice services mean that mobile-phone numbers are no longer the only unique client identifiers. A user's online communication account (for example, Hangouts) is enough to set up a phone call" [18]. While this is true, these platforms still value the universal attributes of the phone number as a unique identifier but could be using them as an underlying technology - one that matches usernames with phone numbers so that users can communicate by means of social IDs. Alan Quayle argues that this dualship has to exist if these MVNO subscribers want to talk with other mobile subscribers, for example on AT&T or Verizon (See Appendix T [V]).

James Body argues that with Apple SIM "you cannot have a telephone number because you immediately lose it [when using it internationally], you cannot have an identity". Body states that Apple would argue that this SIM ID (or phone number) is only used connect subscribers to the internet, and then once they are connected it is their Apple ID that is used. It is interesting to note that Apple IDs can actually store telephone numbers along with the email addresses

(See Appendix R [V]).

In terms of ID verification, this is an important trend. Until now, MNOs could build profiles around a subscriber's phone number because it collected name, address, and billing information. All of which were sufficient to build trusted identities and verification systems (eg. the use of this in Gov.UK Verify, etc..). If Social platforms become MVNOs, they could well become the next trusted identity verification systems and replace the phone number with their own unique identifiers.

6 Extinction or Evolution?

These factors have led to the increasing fragmented use of the phone number: a communication endpoint and a binder to a rich profile (or unique identifier). Factors like the rise of VoIP and teenager communication trends are leading to the eclipsing of the PSTN while factors including social profile verification and eGovernment initatives are demonstrating the future use of the phone number. As the PSTN is eclipsed, the phone number would not die - it would evolve. This is because phone numbers hold tremendous baggage of information and have been anchored in society for a long time. Using them as unique identifiers for digital identity solutions in the future would allow the making of an instant ubiquitous identity system for the digital age. We can now consider the E164 as a digital identifier and the following section will attempt to undermine what the requirements for the digital identity systems of the future are and whether solutions involving the phone number at their core fit these requirements.

7 Requirements for Next-Generation Digital Identity Systems & How the Phone Numbers Fits

7.1 Ubiquity & Universality

7.1.1 Description

Identifiers should be universal in the sense that they should be readily available or distributable to a high majority of the population and allow for a convergence in identifying individuals that could be using various platforms.

Regulators view ubiquitous identity systems as enablers for new digital public and private services to improve all citizens' daily life[25] and reductors of the digital divide for those services. Massive adoption will be the result of convenience and ease of use for the consumer and efficiency for the private and public sector. In fact, GSMA's Marta Ienco views easy-to-use digital identities to be a "key enabler to building a more connected society and enhance digital inclusion"[26]. In other words, it would be an enabler for ubiquity. Europe's strategy for the Digital Single Market of online services focuses on enabling universal digital identity through their Future ID initative.

In their ID4D initative, the World Bank group reviews the widespread lack of ID in developing countries to be a critical stumbling block to national growth. Their view is that "Digital IDs combined with the already extensive use of mobile devices in the developing world would offer a transformative solution to the problem." [26]

Even though universality allows for interoperability for contextual identity for individuals it may reduce privacy as identity is managed in a more centralized manner like in the case of most NSTIC programs (See Appendix K [Appendix K - Topologies of Intermediaries]).

Many industry experts, including U.S. National Strategy for Trusted Identities in Cyberspace (NSTIC) (See Glossary), the FutureID Consortium, Mike Short and James Body believe that the thriving digital identity mechanism will be the one that is massively adopted. All see the critical mass of users as an important success factor for the digital identity systems.

7.1.2 Relevance of the Phone Number

It is undeniable that the phone number's biggest atray is its ubiquity. With more than 4 Billion unique subscribers around the world, the phone number is the most pervasive identifier for humans. Being around for so long and being so anchored in society, it has a large advantage over any other identitifier that could be released upon the public. A research by the Radicati Group estimates the number of unique email users to be 2.6 billion[28] and the number of social media users to be 1.4 billion[29].

In fact, as part of their ID4D initative (See Glossary), the World Bank believes that an estimated 1.5 billion people do not have an official documents of their legal identity[30]. This widespread lack of identity in developing countries is a critical barrier to national growth. They believe that Digital ID combined with the already extensive use of mobile devices in the developing world will offer a transformative solution to this problem[26].

Public services like the World Bank see great interest in the GSMA Mobile Connect (See Glossary) initiative as it offers a digital identity solution by leveraging the use of the phone number and has the potential to gain massive adoption because of its inherent ubiquity. In fact, with 34 mobile operators have been in enabled in over 20 countries in the past year making the Mobile Connect solution currently enabled for over 2 billion individuals around the globe [31]. This rapid expansion (See Appendix I [V]) foretells the possibility for massive ubiquity of the service.

GSMA believes that to achieve massive adoption, convergence with mobility is a must[22] and their Mobile Connect initiative is thought to provide a simple user experience on a device that citizens already carry with them and providing a frictionless login that encourages citizens to access government services more often[26]. The view that Mobile Connect could be the most convenient digital identity mechanism that promotes digital inclusion, and ubiquity is one that Mike Short from Telefonica shares.

Though Facebook, with over 1 billion users, displays great potential and intention for ubiquity, the phone number holds a considerable advantage over any other type of identifier in terms

of universality and ubiquity. Facebook's launch of Account Kit (See Glossary), which allows developers to integrate single sign-on features to their applications by allowing users to log in with their phone number, shows that Facebook views the phone number as a powerful identifier. Additionally, their unique ID is based on the phone number while their social IDs are infinitely editable (See Appendix A [Appendix A - Facebook Messenger's Use of the Phone Number]) . Even though the phone number is a powerful identifier in terms of universality and ubiquity, if we assume any increase in rate of technological advances, the adoption of new digital identifiers in the future could reach billions of people (and machines) instantly.

7.2 Federation & Interoperability

7.2.1 Description

Christian Marc of Gemalto believes that to achieve digital identity convergence for the future, Federation is key [22]. A proper federation scheme is key to achieving this convergence which will lead to interoperability, drive scale and ensure national and international inter-operability [23]. This interoperability should be manifested at all levels: international, inter-device, inter-sectors (public and private), inter-services, between the different types of identities (public, self-asserted, partial, or anonymous), and even between identity providers.

The Chair of Digital Economy states that "Digital Identity 3.0" "will not confined to one organisation, ecosystem or purpose"[1]. The Chair belives that instead, it will be "open to be used for any purpose the owner wishes to use it for ".

This means that federation needs to be decentralized to some extent for interoperability to be achieved. OAuth (See Glossary) solutions like Facebook single sign-on is slightly more open than traditional siloed authentication systems, because it usable for purposes outside of Facebook's immediate control. However, a service using OAuth or OpenID will lose control over their userbase as the identity of the users and their ability to login is controlled by the OAuth provider.

Open and decentralized digital identity schemes will allow for critical mass services, which is

the single most important success factor according the to European Commission's FutureID(See Glossary) initiative[25], as individuals will be free to choose from their identity providers regardless of the service they use. The choice of service and identity provider is a point that the US White House's NSTIC believe is primordial to building identity systems [41]. However, interoperability will be more difficult to achieve and proper federation has to be put in place in order for interoperability to be achieved. The FIDO Alliance (See Glossary) believes that the key is to develop the technical specifications that define an open, scalable, interoperable set of mechanisms that reduce the reliance on passwords to authenticate users [24].

Interoperability can drive the future of identity schemed: The Chair of Digital Economy support the fact that "a digital identity platform would learn about preferences and attributes effortlessly, and use continuously updated data to allow providers to personalise services and products even further" [1]. Interoperability and integration are key to achieving this and would mean that various data streams and attributes would be part of the same data record. Data is currently framented at the hands of a different organisation, creating "walled gardens". That Chair states that in a consumer empowered digital identity, information would be updated once and would be pushed out to all parties that the owner has chosen to share that information with". The report further explored the possibility for predictive, automated and integrated learning to arise: "your digital identity would know so much about you and your habits that it could predict events, changes in attributes and even changes in habits."[1] The OECD believes that a "common, consistent IDM layer will afford users a single, centralised dashboard (or control panel) for their distributed identity information". Such a consistent IDM layer would allow the linking of users' information "across distributed external systems and then update and synchronise those aspects of their information over which they are authoritative, at the push of a button on the centralised service". In this way, a individuals could change their address, for example, and propagate this change to hundreds of external systems at once.**[56]**

7.2.2 Relevance of the Phone Number

The phone number has long been the perfect way to federate voice communication and achieve international interoperability whether between communication technologies (landline vs. mobile), between countries, or even between operators through number portability. Even in today's case of LinkedIn's acquisition by Microsoft[33], the phone number is the only unique identifier common to both platforms that can provide interoperability for the convergence of an individual's profiles on both platforms. Social networks like Facebook or LinkedIn could become ubiquitous but because of their inherent private attribute, they currently remain "walled gardens" and therefore cannot provide interoperability or open federation by themselves[1]. With today's fragmentation of communication platform, profiles, devices, or even protocols, and the need for convergence, interoperability and open federation becomes ever more important.

Though the use of the phone number on the PSTN is not interoperable with today's IP services without the use of SIP trunking services, the phone number as a digital identifier has grounds for global federation and interoperability, epecially in the public sector.

Being common to most public service platforms, like National Insurers, Mobile Operators, Banks, or Government services, the phone number provides a consistent binding to a an individual across all of these platforms and can easily be used for identity verification and federation - making it inherently interoperable as an identifier (See Appendix W [V]).

GSMA's Mobile Connect initative leverages OpenID's MODRNA (See Glossary) project, a mobile operator-focused flavour of OpenID Connect (See Glossary), which allows the federation and interoperability of online identity based on the phone number across the web.

An example of Mobile Connect's potential for interoperability includes a cross-border public sector pilot conducted in November 2015 which made it the first private sector cross-border public service authentication solution compatible with European Union eIdentification and Trust Services (eIDAS) Regulation. The pilot demonstrated how Mobile Connect allows the identification of an EU-citizen of one Member State to gain access to a public service of another. GSMA believes that Mobile Connect offers a simple way of achieving pan-European federation

of cross-border services for the EU governments compatible with the eIDAS regulation, whilst enabling growth in digital public services nationally[34].

It is evident that OpenID and its use in the Mobile Connect offering provides great interoperability and federation at large. However, the digital identifier of the future should have an open approach to federation[1]. OAuth and OpenID Connect (OIDC) do not support distributed session logout, which provides security and administrative control across all devices, and can support the theory of continuous authentication, a set of identity checks that follow a user across networks[35]. Technologies like the Blockchain (See Glossary), Hashgraph (See Glossary) and the Ethereum (See Glossary) platform, or Matrix.org (See Glossary) can provide open federation and interoperability across service providers in a distributed and decentralized manner by leveraging Consensus systems rather than an authoritative entity affirming one's identity[35]. This approach could disrupt the digital identity landscape and someday replace the digital identifiers we have today, whether it is the email, the phone number, or a social ID.

7.3 Security

7.3.1 Description

Security is an obvious attribute for the digital identity of tomorrow and is growing as a driving demand while currently being a tradeoff of convenience (like changing passwords regularly or keeping multiple credentials for multiple services). Security mechanisms for online identities should make it more difficult for the compromise of online transactions and personal data while providing a simple and convenient access for individuals. Marta Ienco, Regulatory and Policy Director of GSMA, states that this is achievable by leveraging the inherent security of network assets via the individual's mobile phone for authentication [26].

According to the GSMA Consumer Report, nine out of ten of the respondents in the consumer survey in the UK would welcome a single log-in solution - a username and password that they are confident are secure - for all or most websites [23]. Solutions like the combination of OAuth and 2-factor authentication do reduce the dissemination of username and password

while making it more convenient for individudals to use online, however it centralizes all that information to the identity broker platform and becomes a better, also centralized, target for hackers. Back in 2014, the OAuth Covert Redirect (See Glossary) hack gathered personal data ranging from email addresses, birth dates, contact lists, and even control of the account, based on a known exploit parameter[27].

7.3.2 Relevance of the Phone Number

The inherent flaw of the phone number is that it is only composed of a string of a handful of digits. Unlike a hexadecimal key with millions of possibilities, a phone number is easily "discoverable" even by accident. For example, it would be easy to discover a real individual's profile by looking up random phone numbers ona social platform that accepts searching by phone number. However, recent development in authentication technologies have led to a new wave of security for authentication linked to the phone number - 2-factor authentication being a prime example. The Mobile Connect initative leverages mobile network authentication with OAuth and OpenID to increase security tied to mobile authentication. Istvan Lajtos from GSMA stated that "mobile network authentication is a secure and closed environment which is difficult to compromise and hack." (See Appendix S [V]) However, recent cyber attacks including OAuth's covert redirect[27] and SS7 vulnerabilities used in OTT applications[36] shine light on the concern of whether Mobile Operators would be the most adequate identity brokers. Marta Ienco, Regulatory and Policy Director of GSMA, seems to think that Mobile operators who work with digital service providers are the ideal partners to create a trustworthy ecosystem[26].

Additionally the use of SMS two-factor authentication, which is the foundation of the Mobile Connect offering, has shown to be vulnerable to cyberattacks. Wired Magazine reports that the "last few months have demonstrated that SMS text messages are often the weakest link in two-step logins: Attacks on political activists in Iran, Russia, and even here in the US have shown that determined hackers can sometimes hijack the SMS messages meant to keep you safe."[55] In fact, the National Institute of Standards and Technology has recently announced

it was actively discouraging the use of SMS as an "out of band authenticator" [62], a method for delivering a one-time use code for 2FA. For now, only 2FA-based solutions that depend on services that virtualize phone numbers are deprecated. But before long, all use of SMS will no longer be allowed, as the public preview states.

7.4 Privacy, Trust & Control

7.4.1 Description

GSMA reports a growth in concern over personal data management: consumers' expectations to exercise choice and control over their data when accessing digital services are raising continuously worldwide[26]. The Chair of Digitial Economy states that "people want to control how their digital identity grows and is maintained"[1]. Services, devices, and things, may be given rights to add, update or authorize data, however users want to have full control over the user management of their digital identity. This includes control to who has access to which information and for how long. This means users should be able to disclose attributes (or part of themselves) without disclosing their full identities and keeping a layer of privacy - privacy will become user-enforced[1]. Self-asserted identity mechanisms like OAuth do permit the sharing of specific attributes (eg. contact list, basic info, photos, etc.) to an extent, however these solutions are still based on third-party social platforms and identity brokers that have all the control the user's data.

The digital identity schemes of the future should allow citizens to be in control of their credentials & personas and have an outspoken privacy focus that preserves citizens' trust while being aligned with government priorities[26]. In fact, European Commission's FutureID initiative believes the solution should allow an informed choice of intermediaries and full awareness and transparency[25]. In fact, GSMA reports that 82% of consumers worldwide would like to know when personal information, and what type of information, is being collected. In today's digital climate, it seems reasonable that 74% of EU consumers want to give their specific approval before any kind of personal data is collected and processed. However only 18% feel in

control of the information shared [26].

The OECD's report on digital "Personhood" and Digital Identity describes the technical qualities that users implicitly demand for the privacy aspects of user control to include decentralisation of identity information into separate data contexts, data minimisation on authentication and transactions, localised identification, verifiability, and selective disclosure. These will be a challenge to tackle with a single identification system as they tend to be constraints to one another[56].

7.4.2 Relevance of the Phone Number

Unlike an email address or a username, the phone number provides inherent privacy as it does not give up textual information like a name, date of birth, or server the identity is associated to. The digital identifier of the future will have to allow users gain control of how much attribute of their identity is communicated to the service they authenticate to. Laurie Austenaa, VP and Head of Personal Data & Mobile Identity at GSMA, believes that mobile operators' have a status of trusted guardians of personal data [32]. Istvan Lajtos from GSMA states that service provider have no visibility to the MSISDN of the subscriber, they can only see Mobile Connect Identifier (PPID) as it is defined in OpenID Connect specification (See Appendix S [V]). Additionally, Lajtos states that platform developers that integrate Mobile Connect cannot retrieve any kind of personal data of the user, without explicit consent from the user. This approach allows users to trust that the Mobile Connect digital identity system provides them with sufficient privacy and control over their personal data.

However, the blockchain has gained a lot of traction in the anonymous web as it provides even greater privacy and anonymity than the phone number and the Mobile Connect initative because of its distributed approach. As the population's focus on privacy and anonymity increases, the blockchain could become a favoured alternative.

Trust is not only how the users perceives the way identity providers handle their personal information but also the way that these identity brokers verify other users. This verification system vary from one model to another. In the Mobile Connect model used in Gov.UK Verify

(See Glossary) or Connect.gov (See Glossary), trusted identity brokers are used to verify the identity of online users in a "verified attribute exchange approach. In the traditional OAuth and OpenID approach used in social media, identity is "self-asserted" by the user and information could easily be edited within the social profiles without any authoritative supervision (See Appendix J [V]). Distributed identity frameworks, often leveraging the Blockchain, are usually based on consensus systems deployed on machines worldwide to establish a user's identity. These various models provide completely different approaches to identity trust and it will be up to the users to decide which is more appropriate based on the service they are using and the level of trust they want to be guaranteed compared to the level of information they are willing to give up.

7.5 Contextual Identity

7.5.1 Description

More than just demanding means for disclosing more private identities, individuals will require the ability to have contextual identities. Most users already maintain multiple digital identities, depending on the context they are used in, and value the independence of those different online personas [1]. The Chair of Digital Economy states that people have a desire for an integrated way to manage independent digital identities [1]: interoperability will be key to managing independent identities in an integrated way.

However, contextual identity is not only about the type of personal data linked to particular profile that an individual chooses to share, it is also the type of identity mechanism used. These mechanisms - which can include hard, soft, anonymous but also self-asserted, multi-identity federation, or verified attribute exchange[26] - dictate the amount of information is shared and in which manner (in terms of verification or assertion). While this concept will create added complexity in management and interoperability [26], it will become a priority for online consumers[1]. In fact, the OECD underlines the growing need for multiple digital personas to become the social norm: "The concept of multiple digital personas (the common parts of

each which are linked together for quick update) enables the introduction of more nuanced relationships into online social networks. It is clear that the requirement for allowing a person to express himself differently in different contexts is fundamental to society in many ways. And it will be a requirement of all future IDM solutions as well. Creation and maintenance of multiple simultaneous, digital personas will become a new social norm."[56]

7.5.2 Relevance of the Phone Number

Contextual identity through the use of the phone number alone is difficult to achieve because of its centralized tie to mobile operators keeping rigid profiles. An early example of this attempts includes Verizon Universal ID which actually allows the addition of multiple phone numbers to a person's profile[37]. However, contextual identity is a one-to-many relatonship rather than a many-to-one. OpenID and OAuth protocols have enabled the use of mulitple personas of individuals over the web by giving them a choice over which social identity service they choose to use - most common ones include Facebook, LinkedIn, Twitter, and Google. By leveraging the ubiquity of the phone number and the flexibility of OAuth and OpenID, Mobile Connect allows users to have an additional choice when connecting on the web. Additionally, the longer-term opportunity of Mobile Connect lies in building out a wider set of identity services across public and private sector use cases to allow for multiple levels and types of attributes to be shared with various services[26].

7.6 Spamming, Spoofing & Reputation Management

7.6.1 Description

Reputation management, anti-spam, and anti-spoofing mechanisms have always been a crucial aspect to identity management in communication as it provides trust and security for the users and victims. With the rise of online intelligent assistant that could one day manage the way users are reached, management of reputation and anti-spam or spoofing mechanisms will become a crucial feature. When discussing the possibility of development of interoperable

signalling systems and universal decentralized database that would lead to the convergence of communication, Matthew Hodgson of Matrix.org states that “Without a reputation and an anti-abuse mechanism, all we’ve done is to create the single biggest spam vector known to man.” (See Appendix U [V]). In fact, whichever the identity system of the future is, centralized or decentralized, reputation management and anti-spoofing will be a “make or break” point for that technology to gain widespread adoption. Hodgson further describes the problem with spam and reputation to be to be politically challenging because “it is not an absolute spectrum”. For example, “one person’s direct marketing material is another guy’s spam just like one person’s terrorist is another guy’s freedom fighter.” (See Appendix U [V])

7.6.2 Relevance of the Phone Number

James Body from Truphone describes that “the problem we have with telephone numbers at the moment is that there is no real perfect way of making sure that the call is coming from who you think it’s coming from because it’s very easy to spoof.” (See Appendix R [V])

Additionally, companies including Neustar, Facebook, and Google have been working on smart caller ID applications that allow users to trust the identity of the caller. Body further describes that “one of the things that Matrix[.org] solves is exactly that problem. Because when you offer a call, there is high-grade ephemeral crypto "à la" Blockchain so there is always an audit trail. So you can always locate where the calls come from with a high level of confidence that the person who is calling or accessing that service is a who they say they are”. However, in a proper decentralized manner, the issue of spamming and reputation management becomes a political issue and a much more challenging one (See Appendix U [V]). Other initatives to secure communication through reputation and anti-spoofing include IETF’s MODERN (See Glossary) draft which would provide credential tied to an issues phone number.

Tom McGarry from Neustar explains that these certificates can be used as anti-spoofing for example “ the originating end, [has] a certificate associated with the phone number that the terminating end can look at and say: “was this phone number associated with the network that originated it? If so, let it complete, if not - don’t.” The regulators could then trace the spoofers

or robo-calling." (See Appendix P [V])

7.7 Legislation, Regulation & Governmental Impact

Digital identity schemes of tomorrow will have to be compliant with regulatory requirements and be aligned with the International Standards [26]. It is important for such frameworks to understand and comply with the regulators' demands like reducing digital divide or enhancing digital inclusion, allowing access to emergency services and USO, privacy and security, data protection for the consumer.

The legislative and regulatory future of topics like Net Neutrality, mass surveillance, encryption, and government's interference upon the internet will shape the future of digital identity and will deeply impact whether digital identity will follow a trend of distribution and decentralization or will take a turn for massive centralization and strict federation. Being a vast topic, this research assumes that the current rate of expansion and freedom of the internet will perpetuate and therefore identity distribution, anonymity, privacy, and decentralization will become a pervasive topic.

eGovernment will become an increasingly important talking point in the public sector and digital identity will be at its center. GSMA believes that the political momentum behind digital identity "is greater than ever with governments around the world realising that it can enable the delivery of convenient and secure public sector services at a greatly reduced cost", the World Bank estimated that $50 billion could be saved by governments globally due to digital identity enabled services[26].

7.7.1 Relevance of the Phone Number

Initatives around the use of the phone number make compliance much easier than new identification technologies. Marta Ienco from GSMA describes the Mobile Connect initiative to be an easy-to-use digital identity system that will be a key enabler to building a more connected society and enhance digital inclusion. Additionally, Mobile Connect is described to be a compliant solution with regulatory requirements on authentication, aligned with the International

security standards [26].

7.8 Constraints & Challenges

The OECD believes that identity problems are "complex and subtle", and regardless of the implementation or requirements there will be limits to the effectiveness of any technical or social identity system. These limits and constraints in requirements will have to be factored in when making the decisions of implementing a particular solution. These challenges include the fact many parties (governments, media, private businesses, individuals, and society generally) are involved and have conflicting rights and demands (See Appendix L [Appendix L - Digital Identity Value Chain Players and Stakeholders]).

Additionally, the process of identification and verification is inherently uncertain as it involves technical, social, and legal systems uncertainties. In fact, uncertainties extend beyond the identification, natural disasters, poverty, war, and other misfortunes will ensure that there will always be new demands but more importanty: undocumented individuals.

The challenges of building an ecosystem mixed with asserted identity, anonymity, and pseudonymity must be tackled since certain activities, like voting, see anonymity or pseudonymity as crucial to the integrity of the process, while financial transactions need better verification systems.

Furthermore, individuals maintain multiple identities which is "normal, appropriate, and even necessary in some cases". This new norm must be taken into account and accommodated by social and technical identity systems. Though questions of identity "will always create conflict, because identity is consequential and valuable". The challenge lies in building social and technical identity systems that provide fair processes for resolving disputes about identity claims.

Finally, the OECD states that in designing and implementing IDM policies, "any organisation that maintains an extensive collection of identity information about individuals has considerable power, which it will be reticent to give up". The OECD believes that such power

must be balanced with appropriate accountability[56].

8 Scenario Planning

The following scenario planning attempts to predict the future of trends that will impact the future of communication and digital identity specifically with regards to the future of the phone number. These trends are not mutually exclusive and therefore provides more of a risk matrix for probable trends than a handful of scenarios. The following trends have shown tremendous tremendous evolution in a handful of years. Therefore, it is likely that the factors discussed in this research will evolve even faster and deeply affect the future of communication and digital identity. The rate at which these factors evolve will determine the speed at which society will observe the concluding predictions discussed. The following factors have been investigated for their impact and likelihood based on a maximum score of 5 (very likely or very high impact) for each. These values are arbitrary estimations and to be used for guidance only. They are mapped to the Risk Matrix in Appendix N [V] which illustrates the imminence of evolution and the trends to watch for various stakeholders.

8.1 Use of Disposable Numbers Delay the Eclipsing of the PSTN

8.1.1 Impact - 2

Thanks to the development of SIP trunks and virtual numbers, it is likely that more applications offering disposable numbers will see the light. As the demand for disposable numbers grows, the traditional use of phone numbers, being endpoints on the PSTN, will be extended in the short term. Because of its inherent integration with the PSTN and allowing it to become “smarter”, these applications could penetrate the global market and fill an important need. Therefore, the rise of applications that offer disposable numbers could delay the eclipsing of the PSTN.

8.1.2 Likelihood - 4

These applications fill an important need in society to have contextual identity over the current circuit-switched network. Therefore, they could easily be adopted globally. A simple snapshot of the Google Playstore shows the popularity of Disposable Number applications often exceeding 1 million downloads for the more popular ones (See Appendix M [Appendix M - Google Playstore Disposable Number Applications]). However, a significant penetration rate may also foretell the eclipsing of the PSTN because the penetration of these applications mainly means an increase in adoption rate of smartphones and VoIP applications. Therefore, as mobile internet and smartphone penetration rate grows these disposable numbers applications will eventually become obsolete. This obsolescence could even occur before these applications become widespread.

8.2 Voice & Messaging OTTs Become Primary Means of Communication for Most

8.2.1 Impact - 5

As adoption of VoIP and messagin OTTs grows along with the penetration of mobile internet and smartphones in all parts of the world, they could become the primary means of communication for a lare part of the population. This would seriously threaten the future of the PSTN and the traditional use of the phone number. However, most OTTs still use the phone number as identifiers which would lead to the definitive dissociation of the use of phone numbers from the PSTN and instead as digital identifiers.

8.2.2 Likelihood - 5

Voice and messaging on the PSTN is becoming largely replaced by VoIP OTTs: WhatsApp sees 100 million calls a day[49]; SMS usage in 2-factor authentication is being replaced by applications like Authy; Facebook is integrating SMS into their app to provide a seemless experience to the user[51]. These factors reinforce the vision that VoIP and messaging OTTs

may soon become the world's primary means of communication. However, they lack in crucial features that the PSTN can already offer like access to emergency calling.

Emergency calling remains one of the last unique features of the PSTN that is not universally offered by OTTs. It is unlikely that OTTs become primary means of communication before they they are mandated by regulators to enable emergency calling. However, when OTTs become permanently obligated to integrate with emergency services, it is highly likely that OTTs will replace the current PSTN as primary means of communication. The European Commission has already passed a legislation that would oblige some VoIP OTTs that connect to the PSTN to allow emergency calling[20]. As Emergency Services evolve to integrate with IP infrastructure and IP data, OTT integration will become an obvious procedure, especially with the increasing rate of penetration of mobile internet and smarphones in developing regions.

8.3 WebRTC Becomes Widespread Across Browsers and Platforms

8.3.1 Impact - 4

The adoption of WebRTC across all major browsers would allow any service provider to add communication features to their platform and hence render WebRTC an ubiquitous communication technology. Traditional PSTN or even VoIP communication could gradually become irrelevant and the dissociation of the use of the phone number from the network even more plausible. This ubiquity would lead to an even greater fragmentation of endpoints across platforms and the increasing need for consolidation and convergence through adequate digital identification systems. Though it is fairly likely that WebRTC could replace current PSTN communications and hence provide more grounds for the end of the phone number as an end point on the network, it does not affect negatively whether the phone number will be used as the universal means of digitial authentication. The fragmentation of services WebRTC may lead to a call for the need for convergence and solutions based on OpenID, which Mobile Connect can provide. With the current advances of Mobile Connect, the phone number may in fact become even more relevant as WebRTC gains terrain and becomes integrated in all sorts of public or

private online services (for example online bank tellers, tax advices, passport pictures through facial recognition, etc..)

8.3.2 Likelihood - 5

WebRTC is currently fitted into 4 of the 5 major browsers and only excluding Apple Safari (See Appendix O [Appendix O - WebRTC Completion Rate for Major Web Browsers]), who have started working on WebRTC integration[57]. It is highly likely that WebRTC becomes integrated in all browsers and in many online services very soon. In 2015 it was already reaching critical mass with expectation that 2 billion people would be using WebRTC apps and websites by 2019[39].

8.4 Mobile Internet Ubiquity Led by "Social" MVNOs

8.4.1 Impact - 5

The penetration of mobile internet in the developing world will have a massive impact not only on the future of the PSTN and the traditional use of the phone number but also on the future of digital identity. If social MVNOs like Google or Facebook were to deploy ubiquitous mobile internet through their Project Loon (See Glossary) or Internet.org (See Glossary) initiatives, respectively, they would gain an important control over the way their users authenticate and identify over the Internet. These "Social" MVNOs would become the go-to verification systems and social IDs.

For example, Facebook's Free Basics (See Glossary) would allow them to deploy their Messenger application, along with many others, as an ubiquitous communication system. This would allow Facebook to become a global identity broker and become a trusted one for public sector use because of the large amounts of information tied to a Facebook ID.

Google and Apple, on the other hand, would push their own email-based ID as a universal identifiers to replace the phone number as a digital identifier.

8.4.2 Likelihood - 3

Though having over a billion users and a strong desire to connect the rest of the world, Facebook's Free Basics has been rejected by India[38] showing that regulators are pushing back to guide these social network initiatives in a way that truly benefits society and does not hand out too much power to private companies. Private internet companies offering communication services are, however, still not properly regulated even though they have expressed the desire to build telco infrastructures [17]. This leads one to believe that these Internet giants could have their way to dictate the way the world authenticates to online services regardless of public and regulatory concerns.

Additionally, because of the competitive nature of the worldwide markets, it is unlikely that there will be a unique private company ruling the world of communication on its own. Therefore fragmentation is bound to happen and the use of a common universal ID still relevant.

8.5 The Smartphone Becomes Central to the Internet of Things

8.5.1 Impact - 3

The rise of the internet of things along with wearables and smart homes will create an increase in fragmentation in endpoints where a person is reachable. Phone numbers have long provided an adequate way to provide a consistent endpoint to a person. However, as population increases and estimates of 20 billion of objects connected to the internet by 2020[44] the 15-digit unique string may not be sufficient to provide an endpoint to everyone and everything.

It is likely that many of those objects will have SIM cards or at least be connected to a device that has one, therefore it is likely that many of these object will be reachable via traditional 3G/4G or even 5G networks.

It is obvious that different types of connected devices will have different levels of authentications. For example, a mere sensor may not need to be enabled for 2-factor authentication whereas the larger object that combines many of these sensors (eg. a fridge) with which a human will regularly interact will need to become a reachable endpoint. The place of the phone

number as an identifier of "things" will increasingly become a crucial talking point.

The future may be that IP and MAC addresses are allocated to all IoT devices while the smartphone remains the human's ultimate wallet which interacts with these services on the go. This way, humans are always reachable the same way even on the move or when interacting with other devices. This means that phone numbers and IP addresses can both serve for different purposes.

As the world of IoT becomes more and more fragmented, it is becoming difficult to grasp whether the smartphone will stay at the center of the connected ecosystem. If it does, the phone number will remain a powerful identifier as the ultimate endpoint for a human being, whichever the interface it is interacting with.

However, if this fragmentation increases and smart objects become "autonomous" from the smartphone's control, it may become harder to identify people on these platforms.

8.5.2 Likelihood - 4

Nigel Brown, Lead ICT Resilience of the UK Cabinet, believes that the smartphone is and will increasingly become the human's castle (See Appendix W [V]). As the importance of the smartphone in the technologic ecosystem increases, it will play a much bigger part in humans' interaction with connected interfaces like fridges, cars or houses in general. Hence, it is highly likely that the smartphone or "personal device" will continue to act as a gateway for humans interacting with various connected objects .

8.6 Decentralization, Convergence & Mapping Lead to the Obsolescence of a Universal ID

8.6.1 Impact - 5

Matthew Hodgson from Matrix.org believes the emergence of digital identity "mapping" will replace the use of the phone number as the single identifier that it has historically been (See Appendix U [V]). Futhermore, Hodgson believes that no one system will prevail as the land-

scape is already fragmented. What is needed is a decentralized secure service that sits on top of different identity systems so that they can be mapped to one another. As devices, apps, and platforms continue to fragment a person's identity and reachable endpoint, the need for convergence may arise in the future and digital identity mapping will be the solution to convergence. Furthermore, artificial intelligence would operate in a "mapped environment" and hence no one single identifier will be needed. In fact, universal identifiers might not be needed at all. While the phone number may seem like the appropriate solution for now, decentralized identity mapping may become the technology that will allow for the convergence and rise of smart assistants that can understand which service, device, interface, or app humans are reachable from and hence redirect messages and calls according to a set of rules.

Distributed identity systems could replace OpenID, which provides a choice of identity providers rather than a possibility for decentralization of the individual's personal information. With the adoption of decentralized systems, Digital identity mapping will be a bigger threat to unversal identifiers liek the phone number. As governments become increasingly concerned with national security and fraud while individuals are concerned with privacy, anonymity, and control over their personal information, the future of the Internet along with digital identity will be affected by the legislations and regulations battling against market demands. Net Neutrality, end of privacy and anonymity along with the centralization of data and identity will affect the way individuals connect to the web in the near future. As markets increasingly demand for decentralized identity intermediaries while government-oriented pilots tend to deploy centralized alternatives, the future of decentralized and distributed technologies, like the Blockchain or Matrix.org's concept of decentralized identity servers, will largely depend on the government's compliance to market demands.

8.6.2 Likelihood - 4

Chat bots and smart assistants have already vastly penetrated the consumer market and interoperability between platforms is being implemented in many bot assistants (eg. SMS-to-Slack, Telegram-to-WeChat, etc..). It is only a matter of demand that will drive the actual commercial

implementation of such assistants. Matrix.org actively work on developing decentralized identity server systems to allow for the convergence of communication. Even though the technology of decentralized and secure ID mapping does not exist today, Hodgson believes the time frame for the emergence of these decentralized secure systems is "probably in the next 2 to 3 years." (See Appendix U [V])

In terms of decentralization technology, the public sector understands the market demands for decentralized identity systems and the security benefits they involve. The OECD, the European Commission[25], and the NSTIC[41] mention the need for distributed systems in their reports for the development of future identity systems. However, the European Commission's Future ID Consortium seems to believe that most NSTIC pilots are centralized whereas FutureID framework is based on market-oriented distributed intermediaries (See Appendix K [V]).

Furthermore, blockchain is increasingly being considered in the public sector. In fact, Christine Lagarde from the IMF stated that the technology would make it incredibly convenient to generate trust and identify players and invited the financial industry to embrace the disruption it will bring[40]. Following Largarde's comments, the Bank of England reported that it had partnered with researchers at University College in London in 2016 to produce RSCoin, a digital currency designed for central bankers[42]. It is therefore highly likely that the future of online identity in both the public and private sectors will involve some form of decentralization at various levels of services.

Part IV

Conclusion & Recommendations

Alain Wahba raises the idea that to understand what the future of identification and communication will look like, it is important to first understand whether we are currently experiencing a intermediary or definitive technology (See Appendix V [V]): whether the identification and communication technologies we observe at the moment are the most advanced or whether they

will continue to evolve.

The various factors put forth in this research show that trends, whether in human behavior or technology are definitely set to continue to evolve much further. Hence, the current technological environment is definitely intermediary when it comes to the future of communication and identity.

Nigel Brown from the UK Cabinet believes that access to content will drive the way communication, identity, and technology as a whole will evolve (See Appendix W [V]). In fact, the need for society to share or consume media will affect the development of technology whether for connection speeds to online identification systems.

The following section features a prediction timeline for the future of the phone number as an online identifier along with the evolution and impact of many of the factors discussed previously in this research.

9 Prediction Timeline

9.1 Short Term (2-3 years)

- PSTN is still well and alive and used by billions.
- Penetration of smartphones and mobile internet is growing fast, especially in developing countries.
- Social Networks and OTTs leverage the use of the phone number as an identifier and binding to a profile through 2-factor authentication.
- Social Networks launch MVNO solutions that would allow them to gain control over the distribution of their communication apps and their own identification systems (eg. Internet.org, Free Basics, Project Loon, Apple SIM).
- Governments are considering various identification technologies to enable eGovernment services online, often based on verification through phone number (eg. Mobile Connect).

- Younger generations are using OTTs as main means of communication (text and messaging) while PSTN voice usage drops in teenager age group
- Decentralized Identity Mapping is developed. (See Appendix U [V])

9.2 Medium Term (3-7 years)

- OTTs have largely penetrated the developing markets.
- OTTs are fully integrated with emergency services and vice versa.
- The PSTN is still around but defunct as a means of voice or messaging communications.
- The phone number is largely used as the binding identifier in OpenID-enabled services.
- eGovernment have fully implemented online identity mechanisms that rely on OpenID or the Blockchain depending on the service used. Having integrated with OpenID through the Mobile Connect initiatives, these services can expand to other OpenID identity providers - just like Facebook for example.
- In fact, Internet giants that launched MVNO initiatives, like Facebook, have leveraged the phone number "under the hood" to connect large quantities of information of individuals together along with facial recognition software and other AI initiatives. Their social ID becomes highly valuable and verifiable and they become trusted identity brokers for eGovernment services.
- The Internet of Things will still need to leverage central hubs like smartphones to authenticate and interact with humans. Smartphones truly become the humans' castles.
- Essentially, the PSTN + SIM Card + SMS + Phone Number become the way to authenticate an internet-device (smartphone) rather than to communicate over it.
- eGovernment fully implemented and online identity mechanisms rely on OpenID or the Blockchain depending on the application.

- Things will authenticate via central hubs connected via 4G/3G.

9.3 Long Term (7-20 years)

- Internet access ubiquity achieved through Internet Company/MVNO initatives, the last 4Billion people are connected mainly via mobile.

- Connected objects, like smart homes or cars become autonomous interfaces, meaning they do not rely on a central hub anymore and the fragmentation of reachable endpoints for a single human is much larger. The need for "smart assistant" services to act as a communication firewall through the most appropriate endpoint and set of rules exists. Thankfully for many Internet companies (eg. Facebook), their AI assistant offerings are very powerful.

- Coupled with the rise in world population, these autonomous objects lead to a need to extend the phone number as there aren't enough phone numbers for everyone and every "thing".

- Through the ubiquity of OTT services and convergence of online profiles due to large scale acquisitions, the phone number has evolved to become a universal Identifier and becomes completely dissociated from the network. To accommodate the need for more identities, the phone number (or universal identifier) evolves into alphanumerical strings.

- This convergence allows artificial intelligence assistant to assist humans into contacting other people in a more semantic way rather than knowing their "universal identifier": eg. "Call my dad", "Call Andy", etc...

- Phone number's ubiquity was initially leveraged to connect and converge the world - once it was done, the world of identity was free to evolve as it pleases (eg. adding an additional number, a letter, a symbol, an encryption key) in a decentralized manner, thanks to identity mapping.

- Even though the phone number (or universal) held a considerable advantage over any other type of identifier, if we assume any increase in rate of technological advances, adoption of new digital identifiers in the future could reach billions of people (and machines) instantly.
- Decentralized identity management and technologies like Blockchain have allowed for ubiquitous and flexible usage over online services.
- Decentralized Identity Mapping is widely implemented and replaces the need for a universal identifier.

9.4 Very Long Term (20+ years)

- The future of identity is set to change as humans and machines interact in indiscernible ways.
- The convergence of large amount of information about an individual and the development of AI has made it possible for infinite means of identification beyond fingerprints, DNA, or facial recognition. Examples include driving pattern recognition, skull sounds.

10 Will the Phone Number Disappear? What Will Replace it and How Long Until Then?

10.1 Will the Phone Number Disappear?

Yes, over time the phone number will disappear in terms of its traditional use to become a digital identifier at large scale. However, its evolution will go beyond and it will turn into a universal identifier. The fact that public switches become irrelevant means that the phone number can evolve into any alphanumerical string as population increases and handheld devices too.

10.2 What Will Replace it?

As the phone number becomes dissociated from the network, the communication endpoints usage it used to serve will evolve into any OTT endpoint that user use. However, the phone number itself will evolve into an identifying technology for digital use. In a sense, the phone number is replacing itself.

In the very long term, the global population will be connected to the internet and social platforms like Facebook will provide ubiquitous identification. At this point, Facebook or other social media platforms can make the universal identifier be anything.

Additionally, decentralized identification systems like the blockchain will gain terrain and along with technologies like facial recognition, EEG, or Artificial intelligence the very definition of identity may evolve to beyond anything we can expect. The development of decentralized identity mapping means that the concept of a universal identifier may eventually become obsolete.

10.3 How Long Until Then & The Problem with Predicting the Future

Even though it is clear that the phone number still has a future as a digital identifier for the next decade, predicting the future of technology and humanity as a whole is an extremely challenging task especially in 2016. Science Fiction author and University professor Vernor Vinge believes that "We are on the edge of change comparable to the rise of human life on Earth.[58]" This is a belief backed by Futurist and Google's Director of Engineering, Ray Kurzweil, who suggests that the progress of the entire 20th century would have been achieved in only 20 years at the rate of advancement in the year 2000 - meaning that by 2000 the rate of progress was five times faster than the average rate of progress during the previous century. Furthermore, Kurzweil believes that this rate of advancements will increase exponentially as time goes by, meaning that the technological advancements made by 2030 would blow away a teenager living in 2016[58]. This is mainly due to the tremendous advances in Artificial Intelligence and its potential to

disrupt society to an unrecognizable extent.

To think about the future accurately, research would have to acknowledge the fact that technology is moving at a much faster rate than it is moving now and the rate of change in the next few year will still continue to increase. Therefore, predicting the future becomes a task highly difficult for human beings.

11 Recommendations

11.1 Commercial

11.1.1 Online Directories

Online directories like Infobel or White pages have extensive databases containing businesses along with information of all sorts about them. These companies could become identity brokers or at least play a part in the verification schemes for B2B services. In fact, Infobel has already seen early signs of this with VeriSign. By developing sets of Discovery & Identity APIs, these online directories could even integrate with OAuth and OpenID to develop Business Single Sign-ons.

11.1.2 Virtual Number (DID) Providers

DID providers still have some time to profit from sales of SIP trunks: call centers still need local phone numbers wherever they provide service to, VoIP service companies still need to provide access to emergency services that haven't upgraded to IP technologies, disposable number applications become popular, and much more. However, in the long run, phone numbers will not be used the way they used to be. These companies have large IP backbones that they could leverage for other purposes, for example providing IP messaging solutions like Twilio or WebRTC services like Voxbone. Additionally, they have the possibility to provide geographic and non-geographic numbers to users that will want an identity in the future. Because of their Regulations APIs in place and their large stock of numbers, they may well become identity

providers for businesses too.

11.1.3 Mobile Operators

As the PSTN looses its edge for voice and messaging, operators will have to battle against the increasing cannibalization of data over voice and the looming demand for bundles rather than "per byte" fees. The future of communication holds an array of services that mobile operators could offer. One example includes the development of smart assistants for their subscribers' communications. This assistant would be aware of the users' whereabouts (physically and virtually) and preferences and direct calls and messages accordingly.

Additionally, Mobile Operators still have a competitive edge for providing verification services in the digital world. Mobile Connect provides a perfect solution for MNOs and MVNOs to move into the new future of the phone number as a digital identity.

In terms of deploying ubiquitous broadband, Facebook and Google are lurking threats to beating MNOs to the deployment of internet services to the unconnected population. MNOs should actively try to provide ubiquitous and free voice services (similar to Facebook Free Basics) to retain some control over the identity of their users in the future. If companies like Facebook and Google beat them to it, they may someday have the control over the population's' digital identity in an unregulated manner.

11.1.4 Internet Companies with Telco Infrastructure

Google, Facebook, and Apple have the opportunity to become large MVNOs and take a large control of the population's access to the Internet. In terms of digital identity, providing ubiquitous access to Internet through their own platform will provide these companies with the opportunity to force authentication and identification through their platforms. This could allow these companies to link much more data to unique identifiers and become trusted verification systems for online transactions.

In the future, network operators, MVNOs like Facebook, Apple, and Google, or smartphone manufacturers applications may leverage their development of AI software to converge com-

munication by creating sets of rules and priorities for forwarding calls or messages to different endpoints and devices based on these rules. Projects like Siri or Facebook M could well be the solutions of the future that will allow humans to communicate.

11.2 Regulatory

Regulatory bodies will have to address the current lowly regulated colonization of the world's communication by companies like Facebook and Google. Regulatory frameworks will have to be set to address the Net Neutrality and user privacy issues that arise with internet giants becoming MVNOs.

As many initiatives to centralize identity management arise, regulators will have the responsability to protect citizens from handing over to much power over to private companies or even the public sector. One example includes The Identity Cards Act 2006 of the United Kingdom that created national identity cards linked to a database known as the National Identity Register (NIR). This scheme was debated as many of the concerns focused on the fact that the Act specified fifty categories of information that the National Identity Register could hold on each citizen which included up to 10 fingerprints, digitised facial scan and iris scan, current and past UK and overseas places of residence of all residents of the UK throughout their lives and indexes to other Government databases – which would allow them to be connected[59]. Since then, the Act has been repealed but initiatives to consolidate identity around central databases are still relevant today for large Internet companies like Facebook.

Additionally, regulators will have to address the effect of decentralization of identity and the challenges tied to it as decentralized identity management gains terrain worldwide.

11.3 Governmental

The public sector should embrace eGovernment solutions based on Mobile Connect for now but understand the future of digital identity is about choice - both based on centralized and decentralized solutions. Decentralized identity management will become the norm and governmental

agencies should embrace its use across digital services.

Policy makers are in fact calling for decentralized architectures. For example, EU H2020's work group believes that "Current centralized platforms for big and social data management consolidate the dominance of existing incumbent actors, stifling innovation and allowing less and less control over the data by citizens. Distributed architectures and decentralized platforms have a huge potential to enable the creation of viable alternatives to current dominant models".

11.4 Working Groups

11.4.1 OpenID

Though being decentralized in the sense that OpenID is not controlled by any one website or service provider, it must still rely on a centralized system to hold the credentials including Facebook, Google, or other provider.

Matrix-like services that allow the development of decentralized identity servers could be the key to render OpenID truly decentralized. By integrating with Matrix.org, OpenID could serve authentication mechanisms for any identity scheme rather than a select amount of identity providers.

11.4.2 IETF

Blockchain and decentralized federation has long been on the IETF's agenda. However, this agenda should incorporate the acceleration of the development of digital identity mapping that would allow true decentralization and choice of identifiers for users.

11.4.3 GSMA

Mobile Connect is a solution that is likely to be persistent in today's current model of "life revolving around the smartphone". However, Mobile Connect is dependent on SMS-based 2-factor authentication and SIM card verification.

The following 3 scenarios could affect the relevance of Mobile Connect in the future:

- PSTN is eclipsed and SMS is replaced by smartphone applications like Authy.
- Smartphones are not the epicenter of the digital environment as autonomous interfaces like smart homes or cars emerge.
- Ubiquitous WiFi is achieved and SIM cards become no longer relevant.
- Decentralized authentication systems become the norm and the phone number is abandoned as a universal identifier.

GSMA should investigate these scenarios and improve Mobile Connect to stay relevant.

11.4.4 ITU

As communications become largely IP, ITU should be considering the NGN portability plan put forth by IETF's Modern draft and covered by Tom McGarry. Additionally, the ITU's numbering plan will be instrumental to the evolution of the phone number as a universal identifier. As population and number of devices grow each year, the current length and assignation plan of phone numbers will not support this expansion. The ITU should investigate the release of new country/usage codes along with the addition of numbers, letters or characters to support this expansion.

11.5 Winners & Losers

With the strict current regulations in place for telcos and the lack of it for private internet companies and OTTs, it is clear that companies like Facebook and Google have gained a massive competitive advantage over MNOs in both the quest for offering ubiquitous Internet services and the development of AI software. Even with the integration of identity systems like Mobile Connect, unless MNOs follow the same path as internet companies rapidly they may well be left behind in the race for centralization of identity and control of communication.

Verizon's recent acquisition of Yahoo [61]is a strategical move for the company and one that will allow them to deliver better bundling services by leveraging the "Internet know-how"

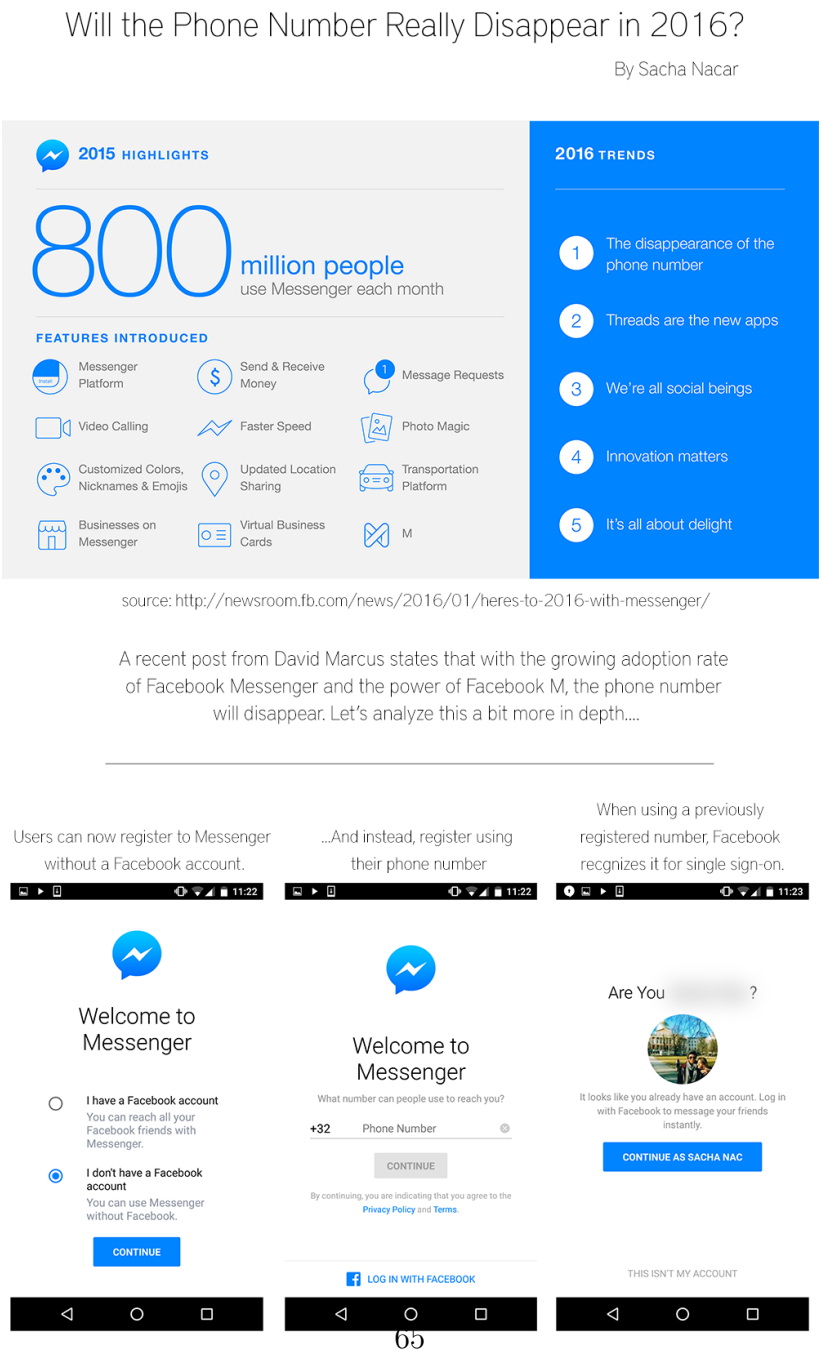
of Yahoo. These kinds of strategic acquisitions of Internet companies by MNOs will become mainstream for industry winners.

It is unlikely that there will be a single central identity system governed by a single entity globally. Moreover, efforts to decentralize online identity are multiplying and being support at a high political level. This means that private companies should look into integration with decentralized systems like Matrix.org or OpenID to become interoperable with the rapid changes in the OTT scene. Companies that miss out on decentralization of identity may well become disregarded as providers as concerns for privacy, control, and choice are growing in the general public.

Part V

Appendices

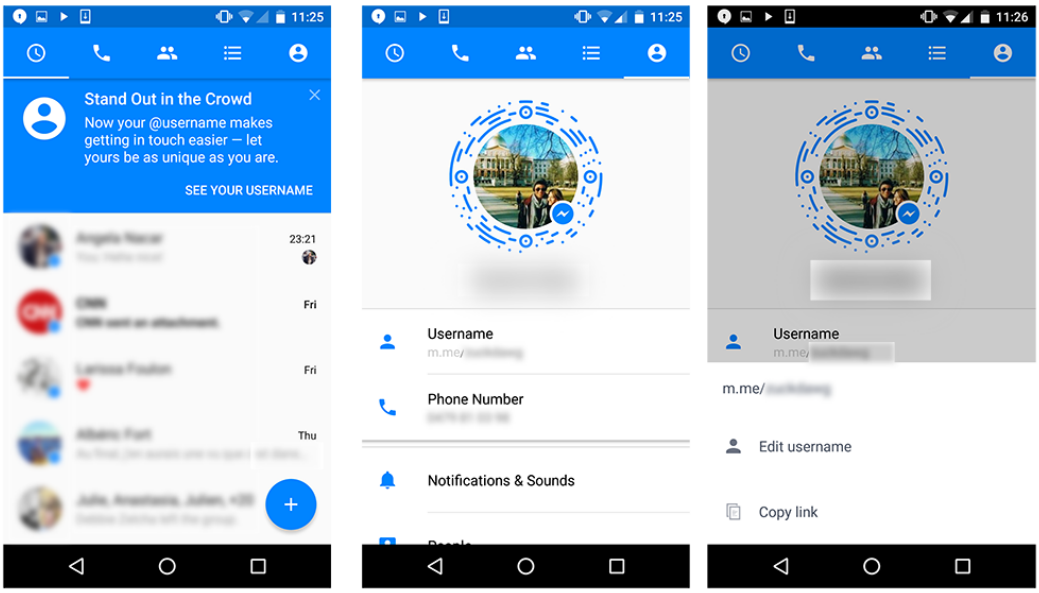
Appendix A - Facebook Messenger's Use of the Phone Number



Once your phone number is linked to your profile, Facebook asks you to set a username...

...Which will be linked to the phone number you registered with.

This username can be changed as much as you like while the phone number associated with the account is permanent.



With over a billion users (and Messenger downloads), it is undeniable that Facebook is becoming an identity broker. In fact, having a whole social profile linked to a phone number is much more powerful than just a name, an address, and some billing information. It is clear that Facebook is trying to become the universal communication platform and will be pushing for their universal ID. However, it seems that the phone number will remain the underlying identifying technology, the users' unique ID under the hood.

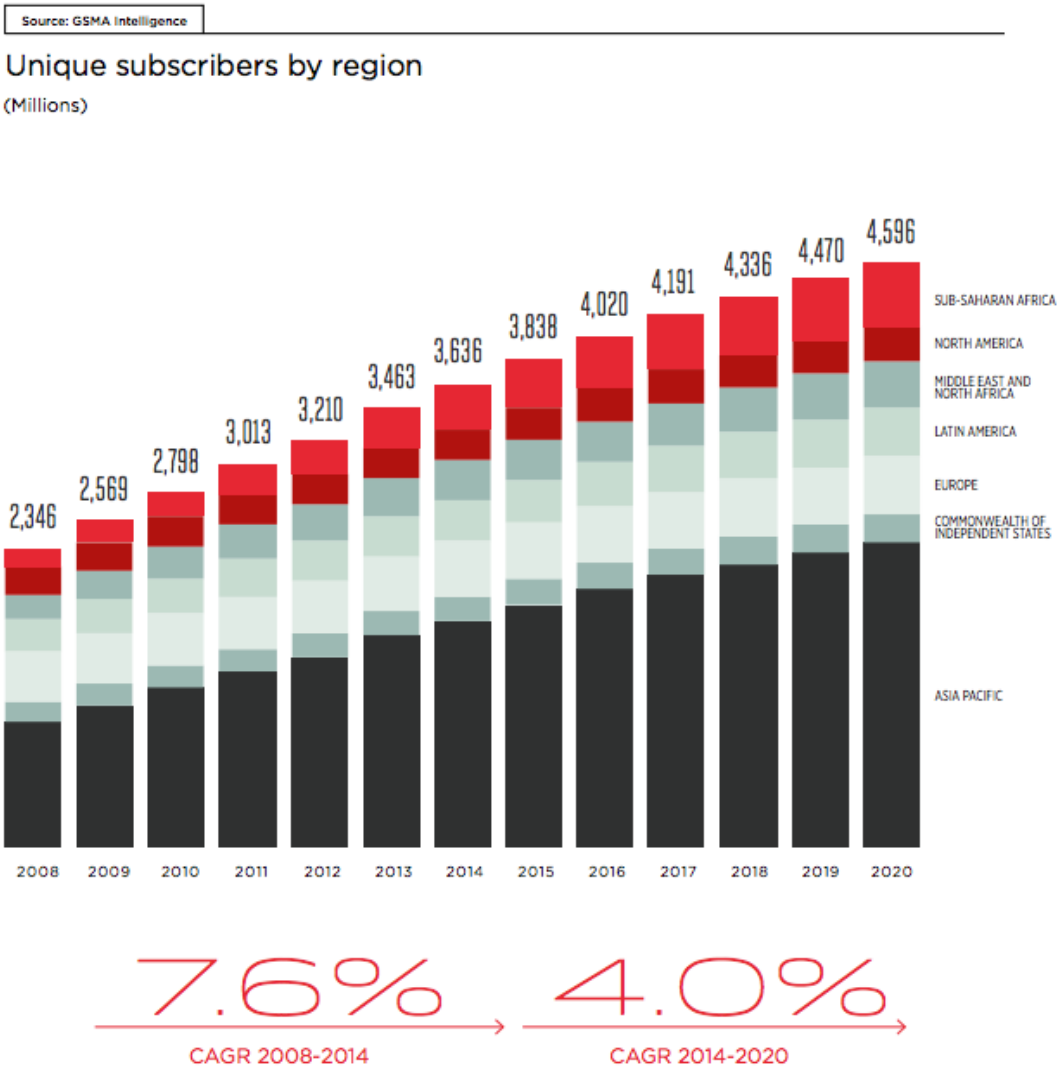
While it may be that in the future, Facebook M will be able to retrieve anyone you want to communicate with based on their name, the underlying identifier will remain the phone number.

So yes, the phone number may disappear... but only from the users' eyes.

By Sacha Nacar

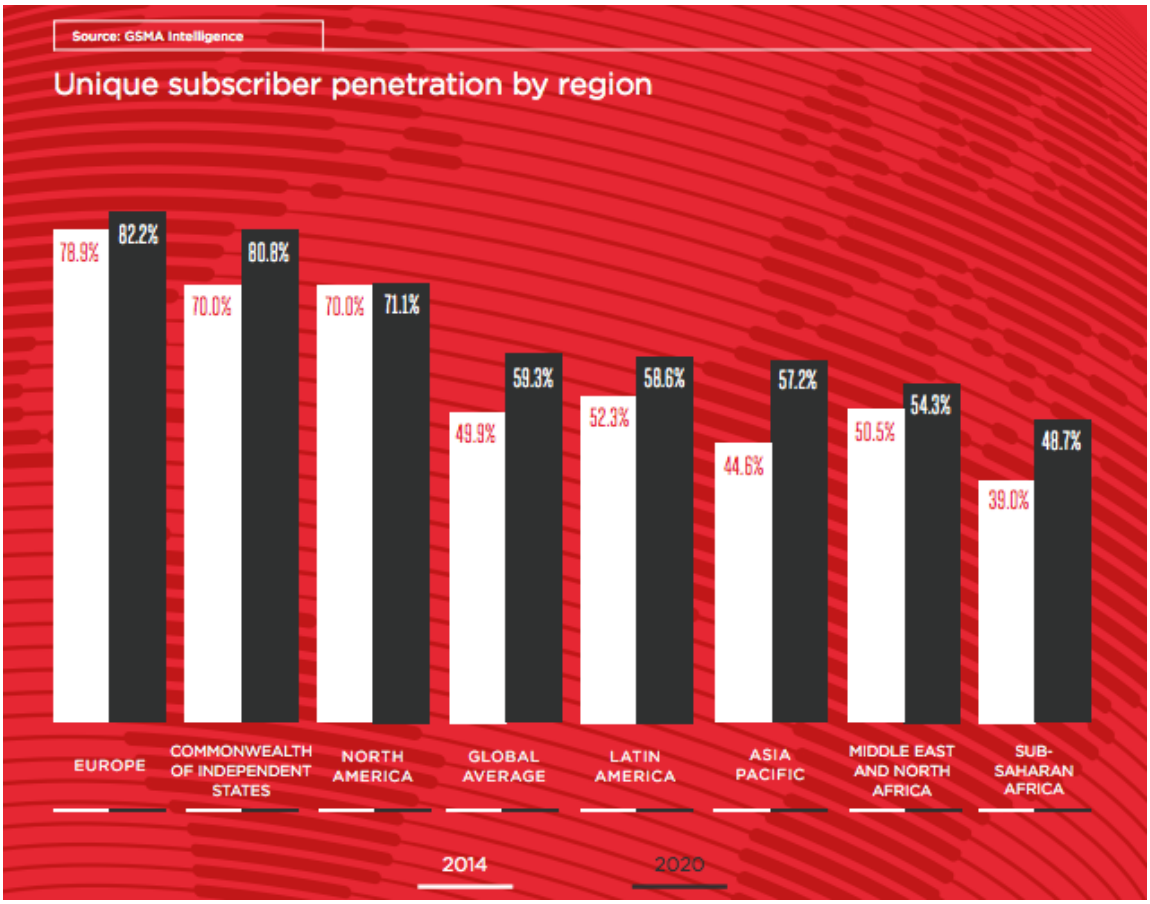
Source: Sacha Nacar [48]

Appendix B - Unique Subscribers By Region



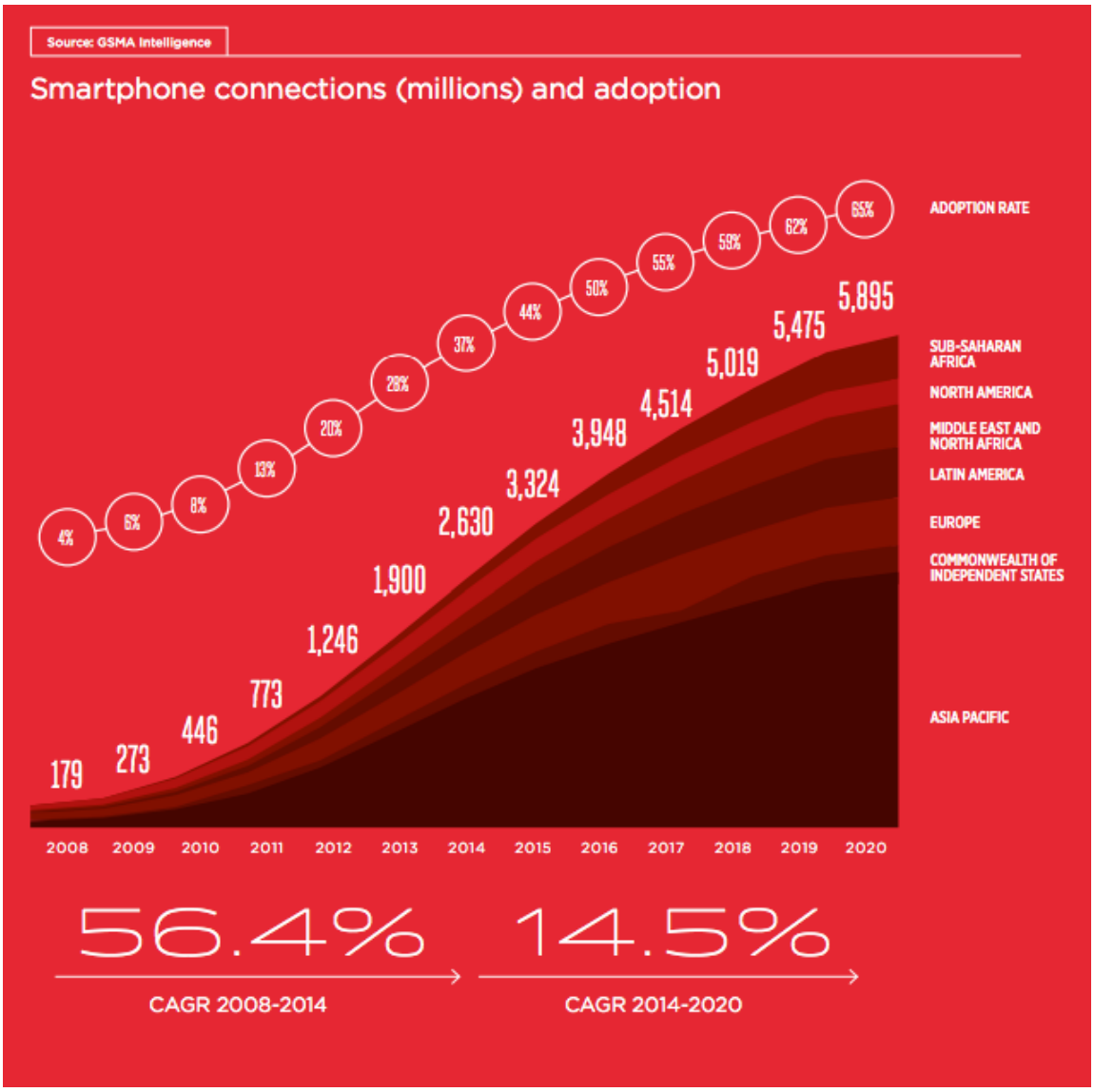
Source: GSMA Intelligence [5]

Appendix C - Unique Subscribers Penetration By Region



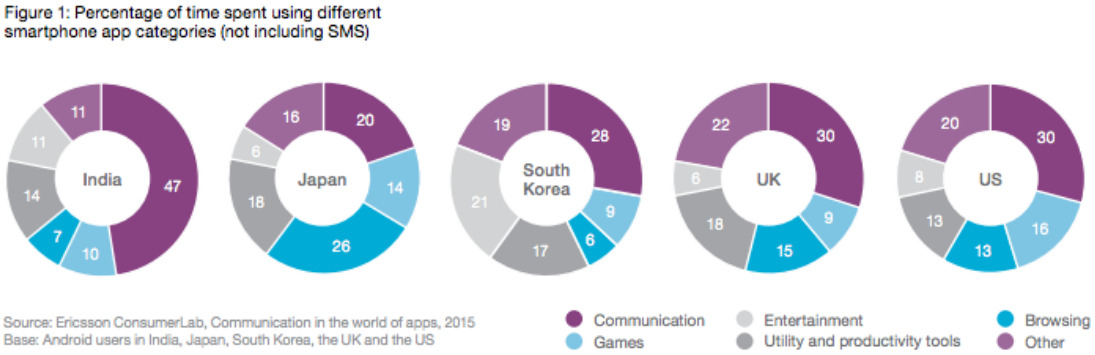
Source: GSMA Intelligence [5]

Appendix D - Smartphone Adoption Rate



Source: GSMA Intelligence [5]

Appendix E - Communication App Consumption



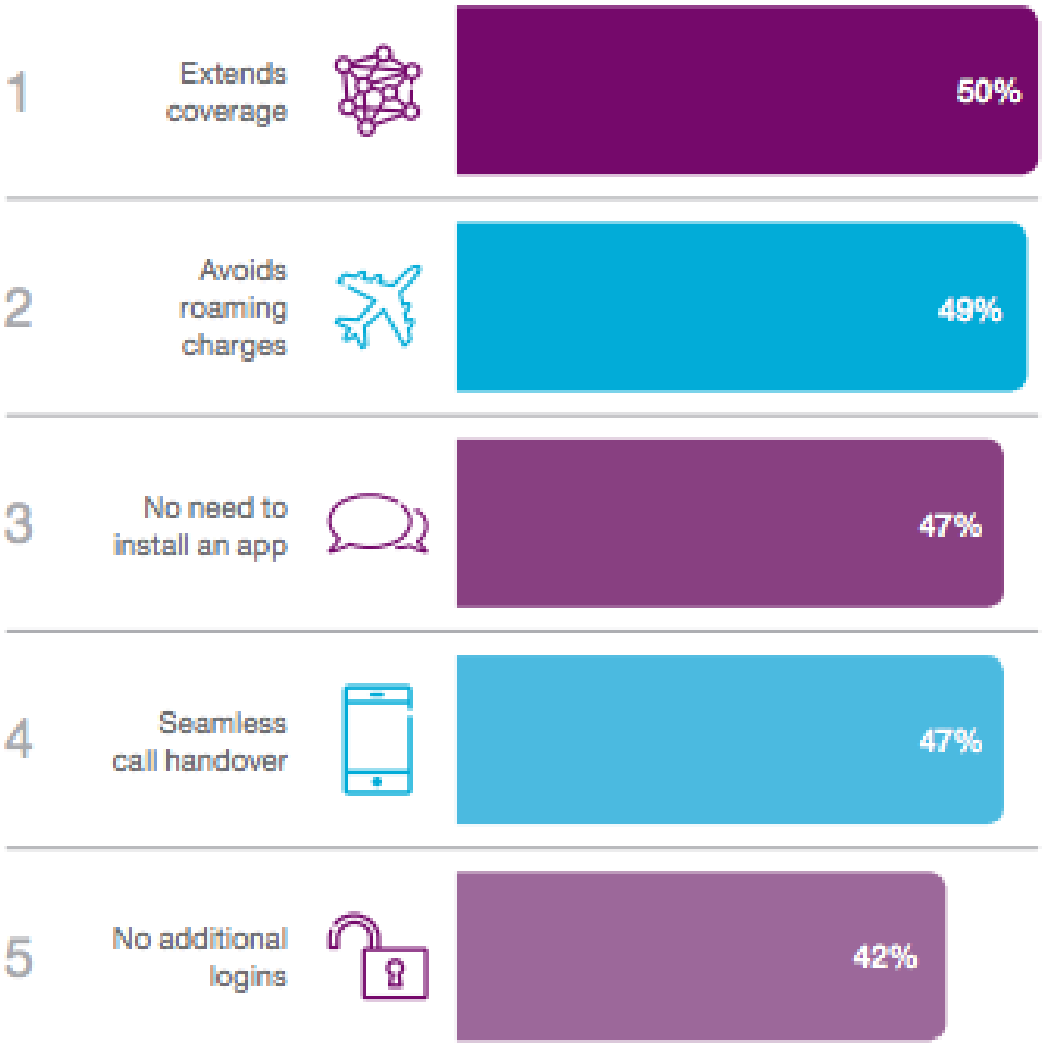
Source: Ericsson Consumer Lab [6]

Appendix F - Digital Quotient By Age Group

Source: OfCom Communications Market Report [7]

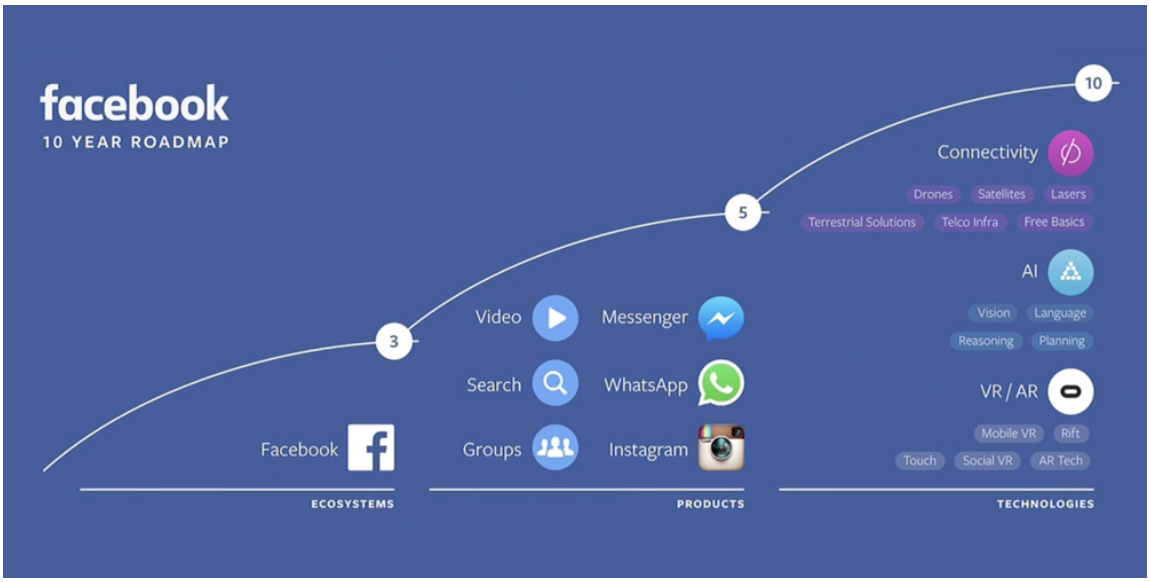
Appendix G - Why Users Find WiFi Calling Appealing

Figure 2: Why users find Wi-Fi calling appealing



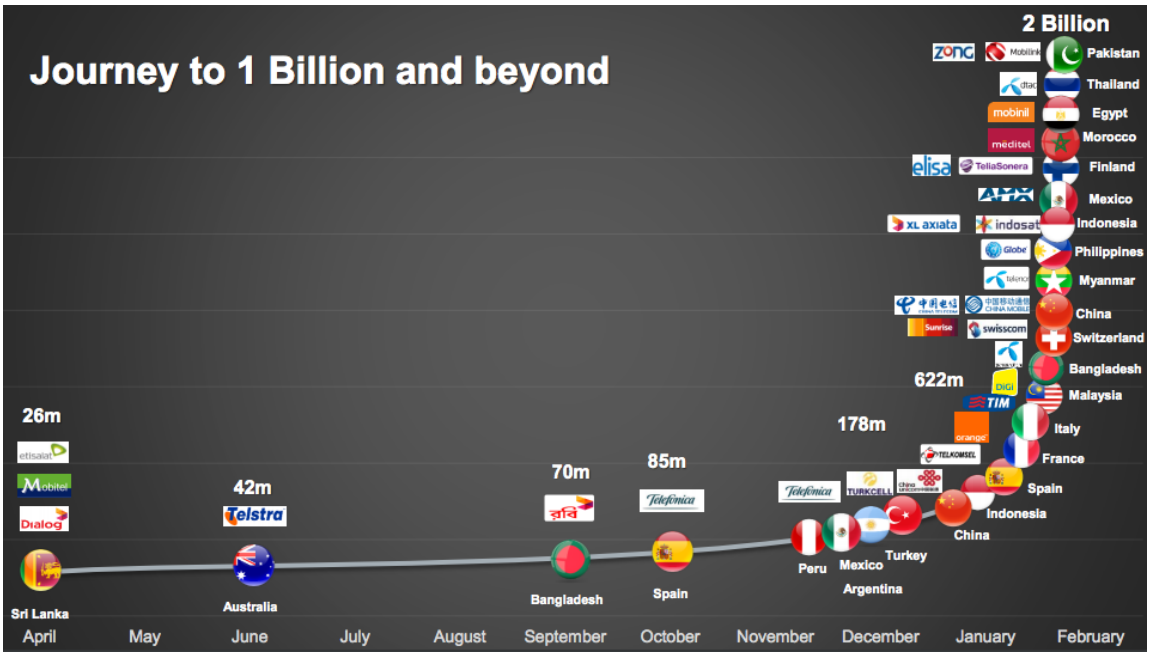
Source: Ericsson Consumer Lab [8]

Appendix H - Facebook 10 Year Plan



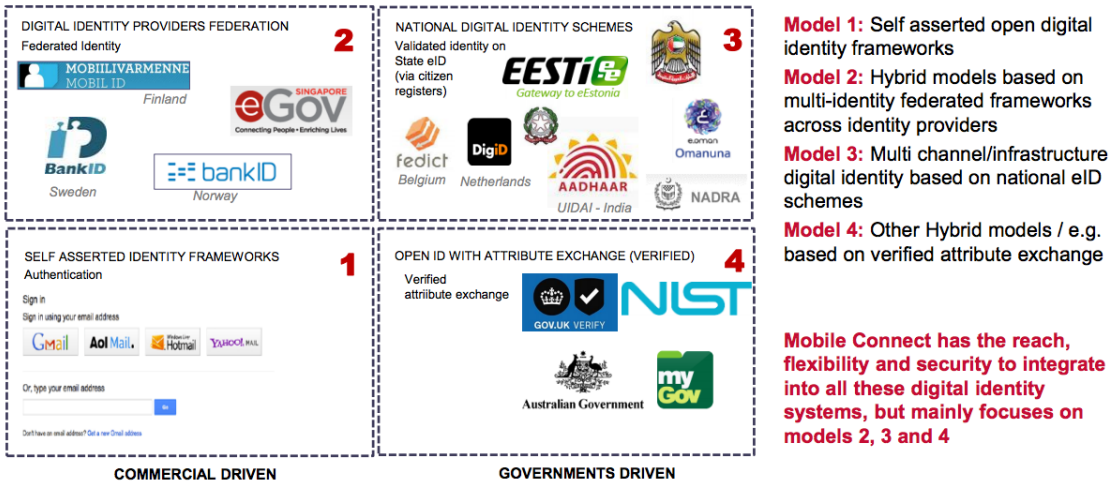
Source: Mashable [17]

Appendix I - Adoption of Mobile Connect Around the World



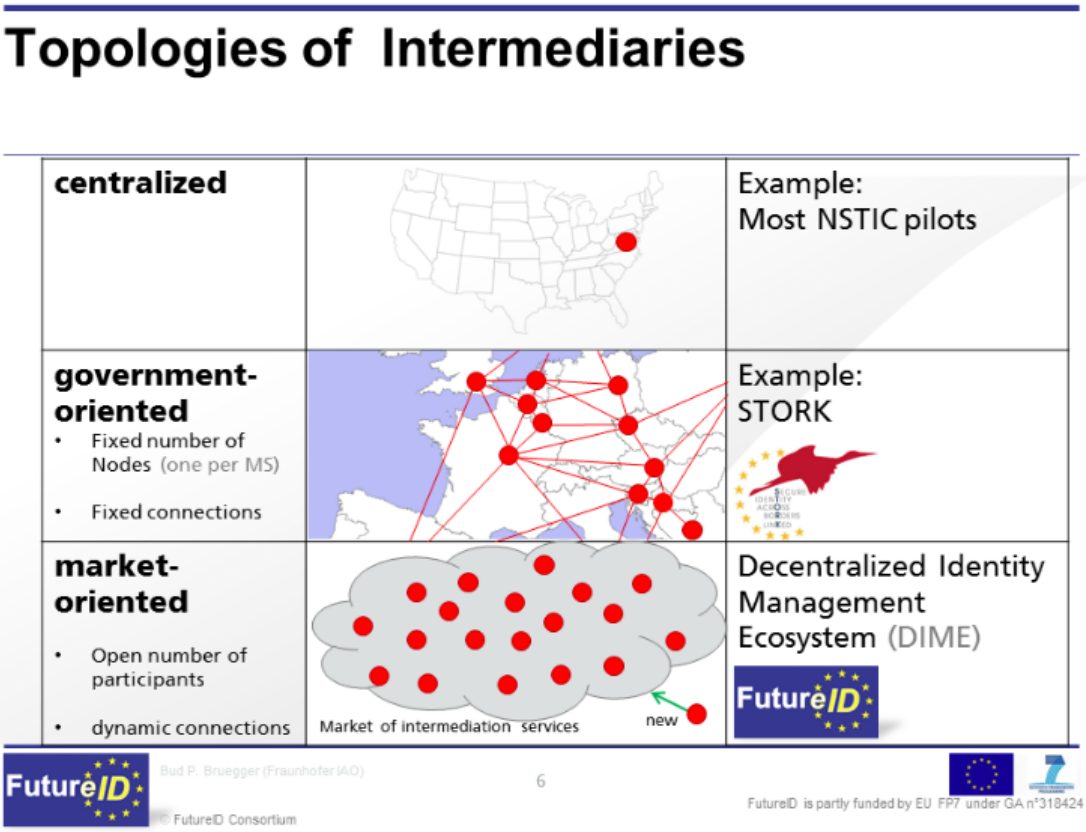
Source: GSMA [32]

Appendix J - Existing International Models to Digital Identity



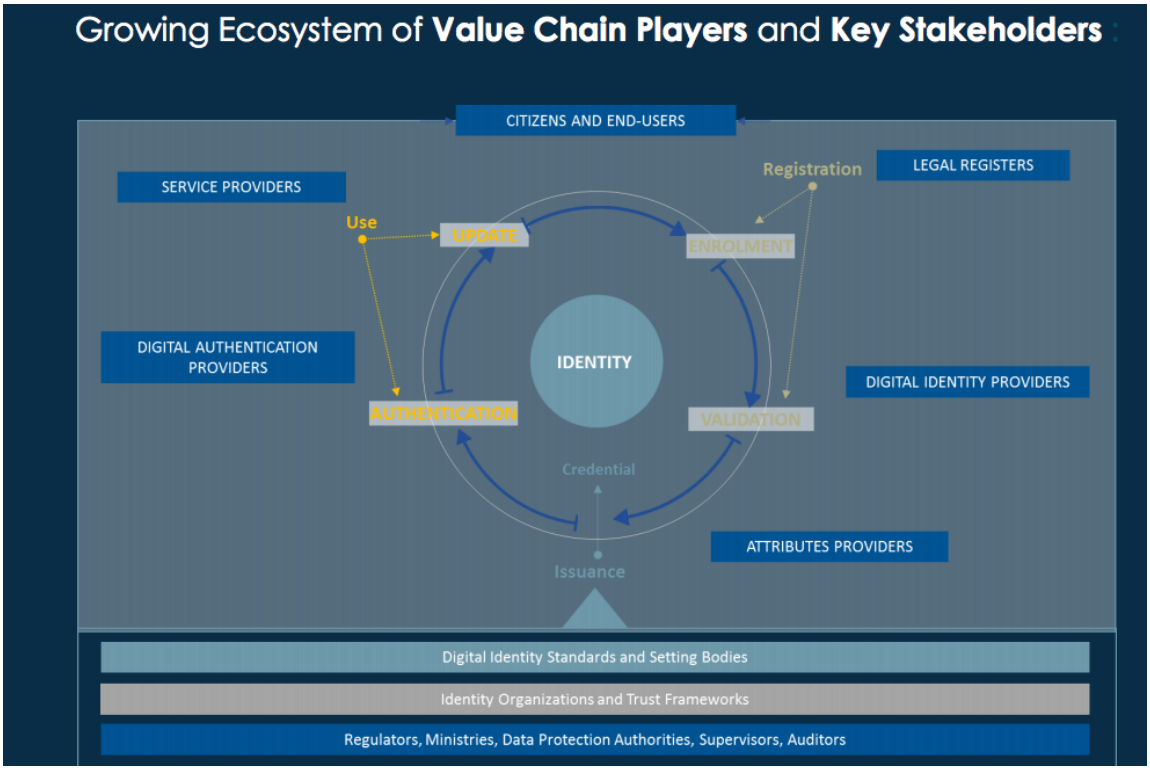
Source: GSMA [26]

Appendix K - Topologies of Intermediaries



Source: FutureID Consortium [25]

Appendix L - Digital Identity Value Chain Players and Stakeholders

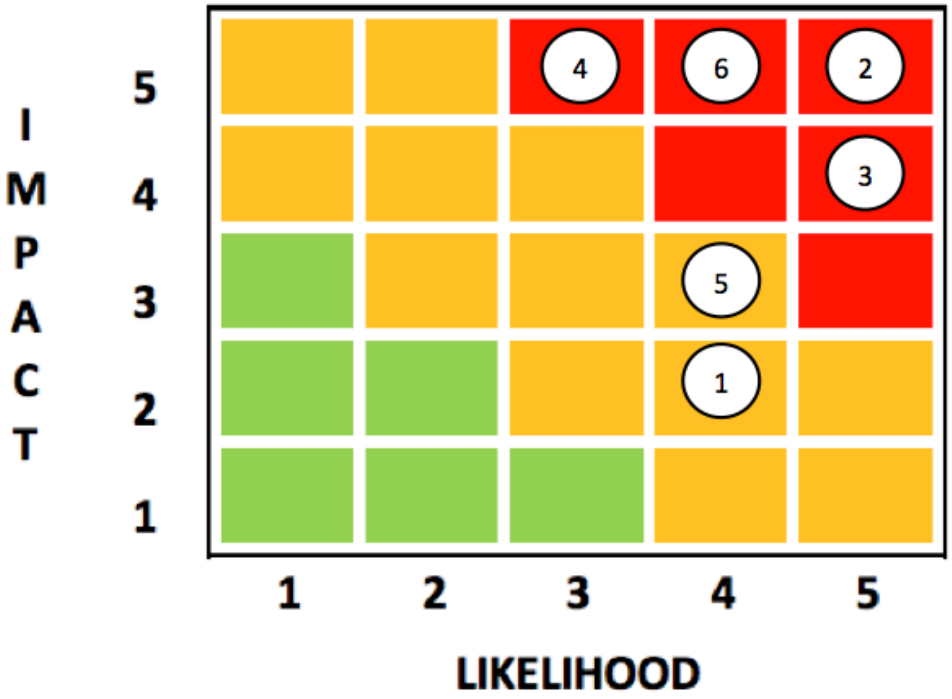


Source: World Bank [[60]]

Appendix M - Google Playstore Disposable Number Applications

Source: Google Playstore

Appendix N - Risk Matrix for Scenario Planning



Appendix O - WebRTC Completion Rate for Major Web Browsers

Source: iswebrtcreadyyet.com

Appendix P - Interview with Tom McGarry (VP R&D Neustar & IETF Chair)

Sacha: Will the phone number disappear? Do you have any opening comments?

Tom McGarry: Everybody asks this question of what is going to be the next telephone number, what would people use instead of the telephone number because the telephone number

seems kind of old. My answer typically is that there will never be something that is a replacement for the telephone number. Telephone numbers are globally managed, globally unique, have the buy in from all the countries. They are regulated both internationally and nationally and I just don't think there will ever be anything like that.

You're probably familiar with ICANN, it is hard enough to manage domain names globally. Something else coming around that has all of the characteristics that telephone numbers have and that [is] globally usable [doesn't seem realistic]. Now there could be something like Skype or Facebook ID, anything that people refer to as being replacements for email addresses. Those are walled gardens, they don't [work] between systems, between Skype and Facebook for example. so they are not like phone numbers and therefore I don't see them as a replacement at this point. One of my colleagues likes to say that something like Facebook's [Open Graph] will replace telephone numbers. You know which Tom McGarry you're looking for because you know he grew up on Long Island, lives in Washington DC, he works for Neustar, and that's how people tell the difference between the different people [they search]. So he seems to think that there's going to be something around the social graph that's like Facebook, maybe not exactly Facebook, that would probably be some kind of identifier in the future. I'm not sure I agree with that but that is certainly one thought. So I think that phone numbers can seem to be killed they've been around for a long time they are convenient they work wonderfully on these little tiny devices you put the number in the phone once and you never look at it again but definitely use food to put it in the first time. What you see as part of the future is that telephone numbers we're really designed as an address on the PSTN network. They were real addresses they identified a switch, they identified a place on a switch, they identified four wires that went to a house. On IP networks that doesn't exist anymore, telephone numbers aren't addresses and in fact they have to be turned into something else to complete. So a lot of people think that this is the time the phone numbers are going to be going away but it just hasn't happened. Telecom companies are still designing their networks around phone numbers so I don't see any way in the near future.

Sacha: As you said, phone numbers are becoming transparent - they are put once in your device and then you don't look at it again. So essentially, these identifying strings could look completely different and we would not even care. How important is it for Telcos to have these identifiers to be numerical strings?

Tom McGarry: So let me touch on the way they do IP routing in the US today. A couple years ago, the way carriers have been deploying their networks is that in their own core they replaced everything with IP. So when there was a Verizon call that originated on the West Coast and was going to the East Coast, they would go over their own backbone and they would have ways to figure out how to route on there. They actually had some form of what is called carrier ENUM. Most carriers here in the US have some version of ENUM which means they query a database with the telephone number and then get back something that tells them the service provider. Then they started connecting between each other. Because of regulations it's easier to do between a CLEC and a CLEC (Competitive Local Exchange Carriers). For example, when an ILEC does an interconnection they have to do it for everybody the same way and offer the same prices. With CLECs and mobile carriers, they don't have this type of Regulation. So when it came to connect to network, the CLECs where connecting with the CLECs and the mobile was connecting with mobile, and the mobiles were connection with other CLECs. But the ILACs, the wireling companies (AT&T, Verizon, CenturyLink) we're not doing much interconnection. That started rolling out somewhat slowly but there is a lot in place now. A year or two ago, I learned how they route calls between them and I was incredibly surprised. today carriers and TDM networks have trunk route between them. In the US, the phone number is 3 digits, 3 digits, and 6 digits. First three digits is on the area code. The first six digits actually identify the carrier and a specific switch and the last 6 digits are the consumer numbers. So what companies do in the TDM side is they have these trunk routes between them and they look at the first 6 digits and they say: "okay which trunk route do these six digits go to?" So they send it out their trunk route and it goes to the other carrier. Basically it is their link to that carrier. IP, as you know, is a lot different. You should really

have large bandwidth between each other and, using DNS to resolve to a sip server, figure out which internet connection you go through. But what they've done is they have actually rebuilt the PSTN. They have these things called SIP trunk routes that look just like TDM trunk roots and they connect their SBC with the other carriers SBC. Then when a call is egressing their network, they do a query and they look at the first 6 digits of the number and they see which SIP trunk route this goes to and they send it over. The original concept of ENUM is that you query a DNS you got a server on the terminating network and it told you the IP address to complete to and you complete to it. Well [US operators] don't do any of that! They basically rebuilt the PSTN and I call that kind of ENUM vision "Ingress routing" because you're asking the ingress network "how do I get to you?". That is kind of how the Internet works. Whereas the PSTN was always egress routing. It's: "on my network, where do I send it out to get to a carrier?". Well, they just rebuilt it and in the US the routing looks exactly like it was in TDM. It still relies on the first 6 digits and still relies on trunk groups. The SBC vendors listened to the carriers and said: "Oh, you want to rebuild the PSTN? Here, I can rebuild the PSTN for you." And that's what they did. So they still rely on numbers today.

Sacha: So ENUM's initial concept was abandoned?

Tom McGarry: Yes, ENUM's vision never came around probably mostly because of policy reasons. There are a couple of reasons. The carriers wanted to have that information on their network. Today you run a number portability database in the US and what we do here is: when a number ports from one carrier to another, they associate a new routing number with that carrier. That routing number is the first 6 digits that have been assigned to one of their switch. So when they port the number, they send that information to [Neustar] system and say: "this [telephone] number now has this routing number." And [Neustar] send that information to every network in the country and they immediately update their SS7 network. Basically when a number ports it happens almost in real time. The carriers like having that information on their network for some reason - probably a combination of emotional and security reasons or

how that was done in the past. The concept of ENUM is that you didn't have that information on [the carrier's] network, the terminating carrier had that information and you had to query [it] to get that information. So [operators] did not like that. One of the other big problem with ENUM was it had way too much policy involved in it. There was a route that had to be managed by somebody like ICANN or ITU or IETF themselves and no one wanted anybody else to do it. ITU didn't want ICANN or IETF to do it, IETF didn't want the ITU to do it, [etc.] So no one wanted to manage that route. So when it came down to the countries, internally, there was a lot of regulation as well. Because, for exampe in the US, the FCC would theoretically have to figure out who manages this domain for the US. It could never get passed the policies. It's used internally in networks, a DNS query is done and it responds back with the MAP directory which was created for ENUM that tells them: "here is information about the number" and typiclaly that is egress information, something like a service provider, identifier or trunk group number. ENUM never came around. The IETF is sort of looking at this issue again. I am the co-chair of a work group called MODERN. What is [MODERN] looking at is how you would administer and manage telephone numbers in an all IP environment. It basically says: "we acknowledge that the way telephone numbers were used in the past as addresses is no longer relevant. We know we are going to an all IP environment. What would you do in an all IP environment?" Today, number management is incredibly anachronistic. A lot of times there are faxes or you have to compelte web forms to keep information about who they are and what their switch is. You think that this should be more immediate. Another problem with numbering today is that we give out blocks of numbers, 1000, 10,000. In Argentina, they give out 100,000 numbers at a time to a given carrier. That creates a lot of waste. In the US, back in the late 90s there was a concern that [Neustar] were going to run out of numbers so we looked at changing how [Neustar] managed numbers. [Neustar] used to allocate in blocks of 10,000, we would give out the first 6 digits of the number to a carrier. The utilisation rate of how many of those numbers were ultimately assigned to a carrier was about 25%, very low. [Neustar] have implemented since then the ability to give out a 1000 numbers, the first 7 digits of a 10-digit telephone number. We've only increased that to 50% and it looks like we've hit

a ceiling - it's been at 50% for a long time. In an IP world, there is no reason why when a consumer is online looking for service of a company, that that company does not have an API with the administrator that assigns a number immediately. Or, lets the consumer look at the administrator's inventory and choose a number. There is no reason why carriers should have large inventories anymore. The technology certainly exists for all this to happen in real time. So [IETF] is looking at that. [IETF] has acknowledge that there is a better way to handle the real time requests about telephone numbers from the operators such as "how do I complete to this?", "what is the address for this?", "who is the service provider?". That is also part of the [MODERN] effort. MODERN is theoretically looking at what would be the next version of ENUM taking into account that the old version failed because of policy reasons. The way numbers are administered today is you have a single monolithic authoritative database, every company has to come to [Neustar] to ask for a number and [Neustar] looks at them, see if they qualify and look at their network utilisation rate. Then, [Neustar] assigns them the numbers and this process takes days to complete. [Neustar] is the only company that [operators] can come to. The same thing for our number portability database: when they update the routing number to the telephone numebr when it is ported [Neustar] is the only database that they can come to. Carriers do not like being beholden by one entity for everything. Back in the 90s there was concern about dotcom being managed by Verisign. The indistry was arguing about how they were managing it and they said "well too bad, we have a contract to manage it forever." That was the beginnign of the problems you see with monolithic authoritative database. So now, one of the things we are looking at with MODERN is distributed database and how you would have multiple entities managing the same data and basically updating eacher other. For example, when there is a number assigned all registries update each other about the status of the number assignation. Everybody typically talks about blockchain, the technology that can power something like that. Blockchain is a specific technology but there are lots of peer-to-peer technologies that can be used to do this. There seems to be a trend were number administration is going in the future. It is not going to be a single monolithic entity managing it. Carriers themselves could be the registry. Today we don't allow it because we think they would have

a competitive advantage because they may hold numbers back. But if everybody can be a registry, why not let carriers be registries. In fact, that is probably the way it would evolve - that only carriers would be registries.

...

Tom McGarry: Here in the US, and I am sure it is the same everywhere, there are these ILEC switches on the PSTN - also called Tandems. A Tandem is a switch that connects one switch to another switch, there are no lines on tandem switches. The carriers are required to run these switches by the regulators and when a phone number is assigned, the carrier that it is assigned to has to have a connection into this tandem and the tandem routes calls to that trunk connection. So, here in the US, we have over 200 Tandems spread throughout the country, all TDM interconnections. If you are a phone company and you have the phone number, you have a connection into at least on of those tandems. If you have a New York number, you have to connect to the New York Tandem. It is fairly inefficient when you think about the IP world. It is very geographically focused. It requires physical trunks into these switches. Large companies like AT&T and Verizon and their mobile companies connect to all of these [tandems]. Then you have some CLECs (eg. EXO, Level 3) that are big enough to connect to all of these tandems but most carriers don't. When we port a phone number in the US, it has to go within that tandem. So when you port a number, it has to port to a number that has a connection in that tandem. You can't port a number form New York to California tandem, you have to be in the same region. So we had a rural carrier in Alaska. Alska has lots of transient residents, people come up there for the military, fo rthe energy business, for maritime. They go up there and live there for 3 or 4 years and then they go to another part of the country. So this small company that has lots of customers that come to them with numbers from New York or California, "I want your service but I want to keep my phone number." However, that small carrier only connects to the tandem in Alaska. It cannot port a number from California to Alaska. So small carriers went to regulators and said "Hey, we need this resolved." The other problem is that large carriers like AT&T and Verizon do connect to all of them, they have a

competitive advantage. As you know, regulators listen to rural companies. They need a way to do Nationwide Number Portability. You can do this by having a New York number have a California routing number but that tends to create havoc with the networks. Networks actually route geographically, if a call is going out of the region to a number in California, they would it differently than if it was within New York. It causes a lot of problems, in fact there are a lot of older switches that would not service these calls, the call would fail.

The old SS7 TDM switches are not being upgraded with new software or services. So I came up with this concept that is a little different that says "let's take a new area code and make it non-geographic, let's make it nationwide." Area codes in the US are geographic and are assigned to specific geography. For example, 212 is assigned to New York City. That means that calls to and from 212 numbers go through a switch in New York City. There are non-geographic numbers like toll-free numbers, like 1-800 but they are routed completely different and they are for special services. So let's take a brand new area code that is not geographic, and covers the whole country, and let's use it for routing numbers. Now, telephone numbers have to have a presence on the PSTN. Today, they have these trunk group connections into the 200 tandems that I mentioned. Basically, you are not a phone number until you have that connection into the PSTN - that basically defines activating a phone number. So what do we do with this new area code? Do we try and find the 200 tandems that makes sense for it to connect to? That doesn't make sense and only propagates the same problem we have today. Instead, we could do something more IP-based. Why don't we have a set of IP tandems? I call them non-geographic gateways which allow numbers to terminate on. The connections to them would be IP. You now have an all IP network and it's all part of the PSTN. This infrastructure actually exists but is not formally designated as part of the PSTN, the FCC has not said: "these are PSTN switches and here are the policies that they have to obey to." So you would have to have some kind of policy around those switches. So I suspect you would have an industry body that creates " what are the requirements for these switches?", "do they meet the requirements when someone wants to offer one of these non-geographic gateway services?", and those these non-geographic routing numbers. But why do they pick a new area code? when we still going to have old

network around? What they would have to do and have the capability to do is route to the IP network based on the area code. So they could say "every time I see this area code, I route it to my transport provider who is an IP company who does connect to these gateways." Basically you create an IP PSTN that is in parallel with the TDM PSTN. This new IP PSTN is made up of volunteer switch providers that are serving their customers. AT&T and Verizon could run these, anybody can run one of these gateways as long as they agree with the policies and processes. There have been this concept of PSTN or IP transition. It's used to talk about how the SS7 TDM network is evolving to IP but people really know what it means. I believe that in this solution, one of the benefits is actually defined by the IP transition - you can actually port your geographic numbers to these non-geographic numbers and anybody who participates on that IP network can stay all-IP. Ultimately, the TDM network gets smaller and smaller and the networks that route from TDM to IP will get less and less and you will be able to converge to an IP network.

...

Tom McGarry: These numbers do not have to be administered the way numbers are administered today. You could do it in a more modern-like way. You could have individual numbers assigned as needed, you could have them be immediately active when they are assigned.

...

Sacha: With this the Nationwide Number Portability project that you mentioned, would it make it easier for subscribers to switch carriers?

Tom McGarry: I am glad you asked and in fact this is probably the most important thing based on the way you're thinking about this. At Neustar, we came up with a concept that would associate some kind of credential with the telephone number. This is part of the MODERN concept. When a consumer gets a number assigned to them, they get a credential and that credential is linked to the phone number and it proves that this consumer has that

phone number. What made [Neustar] originally think about that concept is that today, when a number ports, the consumer goes to the carrier they want to go to and say: "hey I want to port my number to you." That carrier then has some system that figures out which carrier the customer belongs to and then they have to exchange some information about the consumer to prove who they say they are. In the US, generally name and Zip code are used - not even the address. It's fast for wireless but is a 5-day process for wireline. If the consumer had a credential and came to the new provider with this credential and the number, all the carrier has to do is tell the administrator: "I have this number, here's the credential and please port over the customer."

Sacha: Is that similar to the PAC (Port Authorisation Code) number?

Tom McGarry: There maybe things like PINs, those may be given out by the carriers as opposed to the administrator. They work fine. But the thinking of having a credential associated with the phone number that the consumer has access to, like a username and password or X509, gives the possibility of associating others things to it, eg. Facebook address. Having some kind of internet-based security credentials associated with your phone number could be very useful for not only porting number and activating service for your number on WhatsApp but it could replace the 2 factor authentication system used by Facebook and others.They don't have to send you a text.

...

Tom McGarry: People in the numbering world don't want change. So when I talk to companies like AT&T and Verizon and say: "Wouldn't you want to move telephone numbers into the IP world? Make it more valuable, you are the companies that manage the phone numbers the best. You have a competitive advantage, why wouldn't you want to move it there?" They just can't get over their own mindset that there is something fishy about that or it would give somebody else the ability to do something that they can't do. So oddly the

phone companies are against things like this. Companies like Cisco certainly want to see things changing for number, certainly not something they spend a lot of cycles on but would certainly be happy if it happened. Companies like Google and Facebook, I think, view the phone number as having too much baggage associated with it, too much regulation. None of these companies actually get numbers assigned to them from the administrator (eg. Google), they go through CELACs (like Level 3 for example). They like that because they let EXO and Level 3 handle these regulations for them.

...

Tom McGarry: Another thing that they want to use these certificates for is to, on the originating end, have a certificate associated with the phone number that the terminating end can look at and say: "was this phone number associated with the network that originated it? If so, let it complete, if not - don't." The regulators could then trace the spoofers or robo-calling.

Appendix Q - Interview with Mike Short (VP Telefonica)

...

Mike Short: Mobile Connect will have an important role going forward but it's not the only solution. So the general point to your question, I think, is that telephone numbers have been around for much longer than the technology of today and therefore people's culture doesn't change away from telephone numbers as fast as the technology changes. So people are used to their telephone numbers: they're putting them in their address book and they remember telephone numbers still but they don't always remember some of the IP addresses or other alternatives.

Sacha: This research has a big part to do with Human Behavior. Do you feel that the new generations, adopting OTTs instead, will forget about the use of phone numbers?

Mike Short: I think that people are forgetting about the use of phone numbers because actually as soon as more phone numbers go into your address book, you're dialing a number on the list. You know, Mom, Dad, brother, sister, University, the people you need in your address book are the people you dial and that's usually a code before the telephone number. But, I think the issue about data numbers or IP numbers is that they're increasingly being used in the wholesale arena as opposed to the consumer or retailer arena. so I think we will see a bigger shift in the wholesale business to business arena to do with alternative technologies such as IP address whereas in the consumer area, I think culture change will work at the pace of most consumer. Obviously, if we have a telephone switchboard here, we have extensions where people can be found. However, in this office you don't see many telephones on the desks and most people use their mobiles to make calls and receive calls. So it's a change in the pattern, both in the business to business sense and also in the consumer sense.

Sacha: You mentioned IP addresses and, in an email from you earlier, you mentioned NOMINET and it's equivalent registry scheme for addressing the internet was that a reference to ENUM?

Mike Short: Partly but I think also one of the things that NOMINET do is that they look after certain suffixes. So dot Co dot UK is looked after mainly by NOMINET. So when I think about numbering I think about numbering and addressing together. So telephone numbers are in the numbering category whereas addressing is in the internet category and it's quite important therefore to think about the NOMINET and the RIPE type mechanism for addressing. Historically in the USA, some of the numbering has been mixed with the addressing. So you often do the 1-800-FLOWER, you know, so it gives you the letters rather than the numbers - addressing is a form of letters. So the numbering schemes have grown and evolved, or rather continue to grow and evolve, but the addressing scheme, I think, are changing much more rapidly. Therefore, I think that understanding the roadmap of NOMINET or their equivalents is quite important because if you can personalize an address better than a number,

you will personalize the address.

Sacha: I see two trends happening here. One of them is making the address more user-friendly and the other one making it invisible.

Mike Short: Well I think it's making numbering and addressing more user-friendly in each case. I think also to make it more personalized but maybe more relevant to the service in each case, or relevant to the geography in each case, or meaningful in terms of costs in each case. Numbering tends to be associated with the price per minute whereas addressing tends to be associated with price per bit or per byte.

Sacha: I read that Telefonica was heavily involved with Mobile Connect, what was the thinking behind that?

Mike Short: We are active throughout Latin America. We have 350 million customers. They are mainly in Western Europe but throughout Mexico and all of Latin America. For Mobile Connect we made the decision to say: "major countries in Latin America, let's try mobile connect early" because as an identifier, not just a number, it's an important security benefit to the nations we serve.

Sacha: Mobile Connect is supposedly enabled for 2 billion people, which doesn't mean that it's being used by two billion people. Since you've launched mobile connect in Latin America, have you seen a large adoption rate?

Mike Short: it's a bit early to say that but actually it's caused for a different dialogue with governments and all mobile operators, or fixed operators, are licensed by governments. So it's important to have a dialogue around security, it's important to have a dialogue around identity management, and it's important to have a dialogue with governments about what is the future of telephony in the number and addressing way where you can add security for the nation. You might, in some cases, be helping the police to find criminals or you might, in some cases, be

helping the government prevent terrorism. So it's quite important to have a discussion around identity management with all governments.

Sacha: so essentially large Network operators will become global scale identity managers for the nation.

Mike Short: Could become identity managers and I think are well placed to do that given that they are regulated whereas big american entities are not typically regulated. So governments have a view which says what levers can we pull? And they often pull levers through the licensed businesses whether its telecom, broadcasting, energy, or water. They often pull those levers nationally rather than internationally. Whereas the Internet view on life is often: "We are a global player, don't interfere with the service". We do not expect OTT services to be regulated the same way as licensed telephony services. Why should they be? in some cases, if it's OTT for emergency services like 999 or 112, maybe there needs to be some regulation about the speed of delivery and reliability but OTTs are not regulated the same way as telephony. So the levers typically governments pull are on the license controls like telephony or broadcasting.

Sacha: What happens when Google and Apple become MVNOs, through there Apple SIM or Google Fi offering? Do they become regulated like a normal Telco?

Mike Short: So typically the source of regulation in telcos is your rights to deliver telephony services and in some cases your license for spectrum use. so that's where the controls or levers are. MVNOs are not typically regulated the same way because they're not full network, they're a virtual network. So in other words, it's a name associated with a service rather than a network. If Apple or Google wish to do that, that is their choice but they haven't said they were going to do that everywhere. They said: "we may do this in some countries", and sometimes that's a negotiation, it's not a service. It's trying to get better terms locally rather than the service that they may wish to offer themselves. Obviously we have MVNOs in this country and the

biggest MVNOs are Virgin, Tesco, and Talktalk. They are not licensed in the UK but they have certain obligations under the UK law. So, again, staying within the law is important.

...

Sacha: Would the IETF Modern initiative (Blockchain and X509) be a competitor to Mobile Connect or an add-on to better security?

Mike Short: I think there is addressing and numbering and the Mobile Connect approach is more in the numbering space and there is demand for that today. I think if IETF come up with something else, we need to see what that is. Specifically about blockchain, I think blockchain has a lot of potential there is no doubt about that but I think you still need to build something new with critical mass, with something that is trusted by government. [Blockchain] is effectively a distributed ledger scheme and not many people understand what distributed ledger means. So I don't think blockchain is adequately defined today to have got widespread adoption but I think it has great promise.

...

Mike Short: I think the answer to your question is telephone numbers have a long life because they're continuing to evolve but I think the internet's addressing an alternative have evolved faster more recently and people will choose between the two based on a range of factors and may be important to pick out what are going to be the factors that will help people choose. Regulation is one factor. How do you meet the regulation or how do you avoid the regulation? Secondly, competition. If you can differentiate by using a different scheme why don't you differentiate by using a different scheme? Saving money, if you can save money, why not do that? User-friendliness for the market you are serving. Is it going to scale quickly? Is it going to help you deliver new services which can stand out differently and be easier for adoption? So to me it is: "what are the criteria's for numbering and addressing schemes which helps people

to decide between those two?" And I think that for the next 10 years, the balance would be in favor of numbering for consumers and addressing for business to business.

Sacha: Mobile Connect provides a universal identity system, is that dangerous in the sense that it focalizes potential cyber attacks?

Mike Short: There always will be many identity systems so I might recognize you by your name, or your photograph, or your date of birth, or your passport. There will be many identity systems. If there were too few identity systems, the risk of attack would be even greater so I think Mobile Connect will have to sit alongside the other identity systems. But actually most countries want to avoid chaos, so how do you do a uniform numbering scheme or uniform addressing scheme to avoid chaos? You know, it makes sense, not so much in the attack point of view, but to avoid chaos to have some consistency. That's why I grew up in the world of standards like mobile network standards. They have been pretty successful and I think it will continue to be successful for many years.

...

Mike Short: numbering and addressing are really 2 key enablers for growth, change, and choice. So we have to keep looking at what are the best options for growth and change and choice.

Sacha: You mentioned Gov.UK Verify, is Telefonica involved with this initiative?

Mike Short: So most of the government Verify schemes are national and Mobile Connect is doing trial within the US scheme. Verizon is part of the Mobile Connect program so looking, at for example, connected health identity management, how do you get consistent to mobile calls into a patient record? How do you get consistent mobile identity into banking account? So it's driven more from a security concern point of view in the US whereas in the UK, the Verify program is more driven from a government services point of view. So how do you get else

access to healthcare without an identity card? How do you get access to Emergency Services or welfare payments? So it has a different focus but it's got identity management in the heart of it in terms of how you do that. So within the Verify program within the UK, we put in a staff member of 02 who work there for six months that provided advice and support and say: "these are some of the options that the mobile market can offer" for them to consider. Verify is more about identity management for citizens to pick up government services while the Obama program is more about security and access through the internet world to other services beyond the government. Mobile Connect could do more in the UK than it has done but it is currently doing trials in the USA.

...

Mike Short: Give shape of how identity management is going to change irrespective of telephony and addressing.It will work with numbering in some cases and with addressing in some cases. But actually, the leadership is coming from somewhere else, the leadership is coming from governments to say "we need verification of identity for certain services from the government" and in the states "we need secure access online consistently handled for a range of services in the USA". Again, these are demand drivers, or government drivers, which are totally different to the original drivers that led to the design of telephony systems, numbering systems, or addressing systems.

Sacha: Looking at the Mobile Connect offering, network operators have to connect to the APIGee platform. Does that connect in any way to the previous numbering systems built in the past?

Mike Short: I think there is a range of APIS that do exist and that people can use. The schemes are not always International because they're National in nature but I think people from a business-to-business point of view want easy access to both numbering and addressing. If we take examples in the numbering space, if we take mobile short codes in the UK we've

had mobile short codes for 15 years. The range has widened but some of it did not exist at the beginning. For example, dedicated codes for charity text, the ability to give money with 5 digits against the seven XXXX shortcode series or the ability to identify adult lines, which were 69XXX series numbers. So numbering continues to adapt to give better access to either donating money or certain type of services. Equally, addressing has continued to adapt and I think both will continue to adapt to meet market needs. And I think therefore the proposition about telephony dying is wrong. It's more about how do you choose between the telephony numbering vs. addressing options.

...

Sacha: How will emergency services adapt, and do they need to, with new services like Mobile Connect or Tugo?

Mike Short: First, Universal Service Obligation is not defined consistently across the world. There are many countries that have no USO at all. There are some countries that have very light definition of USO, and there are some countries that implement it very thoroughly. Europe implements it very thoroughly but even in Europe the definition of USO is not consistent. If you talk USO in the USA, it's not about Universal Services for the whole of the USA, it's often a very localized service within the license footprints: the state or the Wireless geography. Equally I think some UO issues are just about coverage, some are about resilience, some are about making sure there is a minimum level of service. So the definition of USO also differ as well. Emergency services to me means "Police, fire, and Ambulance" but emergency services doesn't mean the same thing in every country either because they're not all government to run in every country. In the states for example, fire services are very local for each city or state whereas the police from an FBI point of view is National. But most police in the USA is local so the reason they have the FBI is to cope with bigger for threats compared to what the local police can do. similarly emergency services for ambulances are very much in private hands in the USA whereas they are part of the NHS in the UK. So definitions of Emergency Services

very a lot. Also the definition of 999 in the UK vs 112 is not always as consistent as you might imagine. Now if I put all that together, there are some issues about how does USO play into emergency services and their needs and how does it also play into the services we as citizens might want with 999 or 112. I think it's good to have clear identifiers as in 999 or 112 for emergency services but some of the OTT players disagree. They would say: "we don't provide that service." Well, okay, "you don't provide it but you may not be appreciated if you don't. It may be that we will regulate to tell you you must." So there is a dilemma there, do you add cost for the OTT service for everybody? Or do you just have emergency services through the numbering scheme? Do you have widespread coverage based on the emergency services we know in the UK or do you have a more patchwork quilt as they do in the USA? So there are quite a few issues in there. To me what is key is the identifier has got to be absolutely clear in terms of what it is delivering. And in the UK, 999 is quite clear: "Police, fire, and ambulance." From wherever you call, it goes straight through as a 999 call and the location information goes with the call from mobile or fixed line through to the call center. In the USA, they had to introduce something called the Location-based Services Activity, which is LBS, based on 911 and that was a huge industry. They had to put in some overlay equipment to map the towers so that when the cell phones made the call for Police or Fire, they could be recognized with their state police forces. They couldn't do that 10 years ago but they can do it now. So the simple answer is, the identifier for emergency services, whether it is a number or an address, needs to be absolutely clear about what it offers and it is not as clear as it could be in some countries today. And the OTT players might not want the added costs involved in localized services because they might want to do an OTT service for Europe or the World. There is an expense in linking OTT to cell ID or OTT to some other tighter definitions.

...

Mike Short: I have said to the UK Cabinet: "Why aren't we using more of Cell ID?" as an identifier in the emergency call centers? I have said: "Why don't we take the 999 or 112 call into the data world?" Why? Because you could then bring in more video, you could bring

in other data sources if you did that. However, you would have to change both the culture of how emergency services from a consumer to emergency is dealt with. You've also got to get the emergency call centers ready to receive the right data. Imagine you were on an accident in the M1 or M4 and a 100 people are all ringing about the same accident. Actually, a data call could help you filter out more easily the [unnecessary calls] from the real emergent location which you have to get to. I think this year or next year, there will be changes towards emergency services as in "dying" for emergency and I think that will be changed as well.

Appendix R - Interview with James Body (VP Research Truphone)

Sacha: With the advent of IP technologies and IP services, there is this idea of a dual use of the phone number which used to be for normal PSTN usage for connecting a voice call. Now the phone number is becoming more of an identification string.

James Body: Exactly, it's an address! It's a way of identifying an endpoint, which in the case of mobile devices, is normally associated with a person. And that's been a bit of a paradigm shift.and that's been a bit of a paradigm shift because going back 30 years ago telephone numbers were associated with places but now they are associated with people. Telephone numbers aren't going to go away because they got so much going for them. They are globally unique, they are easy for humans to handle, and the user experience of the telephone number is pretty good because people have got used to them, they can handle them. In fact, they can even remember them. It's really easy to enter them in a handheld device, you can dial them. So they aren't going to go away overnight but I think what we're going to see is that people will not have just one identity, you are going to have lots of identities and we see that already with services like Skype and iMessage.

Sacha: I have been researching the Apple SIM

James Body: the fundamental problem with Apple SIM is that supports only one profile at any one time and that model breaks as soon as you're going to use it internationally. Imagine you are a U.S. user, you have a T-Mobile subscription, and you come to the UK and want to switch to an EE profile to take advantage of better rates in the UK. What you would have to do then is totally destroy your T-Mobile profile to have the EE one instead. You can only have one profile active. What it means is you cannot have a telephone number because you immediately lose it [when using it internationally], you cannot have an identity with [Apple SIM]. Apple would argue the counts as only being there to connect you to the internet. And then once you're on the internet you use the Apple ID, which actually can store telephone numbers along with the email addresses. It is a really modern way to address an endpoint. Another important thing you're seeing is telephone numbers being tied to different tariffing bands. Even to this day you find that if you call people in the US with an non-US number, they will not call you back because they do not know how much that phone call is going to cost.

Sacha: I'm also doing some research about the EU Single Digital Market and their efforts to slash roaming costs.

James Body: Well, they are gradually going away, certainly in Europe. From the mobile network operator perspective the cost to terminate a mobile call is sub $0.01. It costs more to run the billing than it does to terminate the traffic. So ultimately I suspect that's where we're going to end up with the scenario where you just pay a monthly bundle fee for access to the network and a number of network applications like your bot service or extra numbers, some kind of intelligence network. That is what you will pay for and you will not be bothered about minutes. You are still worried about data and certainly still worried about quality of service as a priority. However, the basic data access for things like moving low priority emails - that would be totally free, guaranteed. certainly when you want to do some kind of low latency high definition video then you will have to pay for it because you will need that kind of quality of

service to make it work. If you are willing to take background noise level type quality, it's free. In fact, access to internet will be a right to citizens. Going back to numbers, you clearly need a means of addressing endpoints but I think we're going to move to a time when one individual does not have just one number. at the moment you probably have one mobile number because it's expensive to have 2 or run all your SIM cards at the same time. What we will move to will be a number of services or a service where you plug in multiple communication strings with multiple numbers. We already see it on our services because we offer multiple numbers, where you can have different numbers for different services. So for example you can use it for a specific purposes such as selling your car and at the end of that transaction then you get rid of the number, you certainly don't want to put your [personal] or real number on the [web]. Another scenario might be somebody that may want to contact you but you only want to allow him one chance of doing it. so you give them one special number that will work once and once only.

Sacha: On an identity management level, how would that work?

James Body: Well it's more than just identity, it's also purpose and also precedence (how important is this call). So what we're doing here is we're allowing the bot or the agent that is sitting between the network and you to make some kind of decision about what to do with that call. One way of doing it is by having different addresses for different purposes, it is something that you probably already do with emails - you have different email addresses for different purposes. [The great thing] is there is no shortage of telephone numbers.

Sacha: On the human behavior level it seems we don't really care that we have to manage these different identities and we do a pretty good job at it. Hence, is there a need for services like Matrix.org?

James Body: Yes there definitely is I think without a doubt. Matrix[.org] is very brave and clever. what it doesn't bring is the concept of tariffing, I don't think, but it could do later.

One example of how that would work is you publish a number which people can use to contact you but if they use it it will cost them 5 pounds. It creates a barrier where only people who really need to contact you do so.

Sacha: yes, Facebook already explored this idea with their "Other Inbox" which allows anyone to send you a message to your non-personal inbox but if they want to reach your actual inbox, then they will need to pay a fee (if they are not your friend).

James Body: Yes and again that is an interesting evolution of telephone numbers as an identity, it's not just the telephone number it's an address.

Sacha: It sounds a bit like Bill Gates' idea for electronic stamps [that would counter spam emails] back in the days.

James Body: Another interesting concept is the idea of DHCP for telephone numbers so if you wanted to apply to a server and it issues you [one] with a lease on it. After that, the number goes into quarantine. At the moment, the industry standard for quarantine is 6 month, after that the number can be reissued again.

Sacha: How would emergency services update to more modern ways to identify someone?

James Body: Emergency services aren't tied to the number but to the location. The important thing about the number is that they can identify the endpoint from which it came so that they can dispatch people to where that endpoint is. That's where the focus for emergency calls are. It is particularly important in the U.S. because they have lots of localized emergency call centers. Here in Europe we tend to do it a little bit differently: we tend to have bigger call centers and then use the network to work out where the end point is.

Sacha: Is that using HLR?

James Body: It uses a number of techniques.but the current generation of mobile technologies does a network query to find out where the end point is. There is an SS7 map query which goes to your smartphone and return your GPS coordinates with no permission at all so the Emergency Services can see where you are even with no permission.

Sacha: SS7 is an important [technology] for emergency services then.

James Body: Yes, but SS7 is beginning to die now, it's being replaced by IMS. IMS comprises of 2 protocols: SIP & Diameter. SIP does everything to do with media while Diameter deals with access, authentication, billing, location, data sessions, and QOS.

Sacha: Matrix[.org] is supposedly the missing signaling framework that would connect everyone and everything- could it become compatible with for emergency services and replace SIP/Diameter?

James Body: Matrix is very interesting, the problem we have with telephone numbers at the moment is that there is no real perfect way of making sure that the call is coming from who you think it's coming from because it's very easy to spoof. One of the things that Matrix[.org] solves is exactly that problem. Because when you offer a call, there is high-grade ephemeral crypto "à la" Blockchain so there is always an audit trail. So you can always locate where the calls come from with a high level of confidence that the person who is calling or accessing that service is a who they say they are.

...

Sacha: How is [Truphone] using Enum?

James Body: Well there are two uses. There is what is known as carrier ENUM, which is all about identifying whether the number that's been dialed is reachable by VoIP directly and if it is then you don't pass of the call through the PSTN. The original concept of ENUM was much wider than that and was to have it run on individual clients so you could route traffic peer-to-peer. However, the big operators or government agencies did not really like that [for obvious reasons].

...

Sacha: OTT's have also used the phone number as identifiers, however in a very much dissociated way from their PSTN use, only as an identifier. For example, I could have my WhatsApp identity be my Belgian number when I'm calling from the U.S.. So these identities could just as well be anything else.

James Body: Yes, Facetime, iMessage, exactly the same. But the fact that you probably had your own personal mobile phone number for over 10 years, lots of people know it and it means you will be retaining that number for some time.

Sacha: will there be a point when new generations stop registering for phone numbers or plans?

James Body: I think possibly we could be seeing greater use of phone numbers rather than reduced use because with modern technology it's easier to support multiple concurrent profiles. With the old technology you couldn't, you had one or two. In the GSM's specification you could have Line 1 line 2. However, these days there's no limits.

Sacha: I see younger generations reducing their use of the phone number or the phone app of their smartphone and instead using the data part of their smartphone - Facebook Messenger, WhatsApp, etc. to communicate.

James Body: And it's interesting how communications habits and etiquette has changed. I won't dial the number and ring directly, I would normally just check with an email first to make sure the person at the other end is there and is in a position to take that voice call because it's rude just to phone. and that has only happened over the last couple of years

...

James Body: say I want to send a message to you and I have one of your many aliases it can be a phone number an email address or some kind of instant message identifier and I only need one of those to contact you and my bot client will work out what is the best way of sending that message.

Sacha: I guess signaling and services like Matrix[.org] is especially important to know about my real-time presence.

James Body: Yes, and there [should] also be some kind of scoring mechanism over which is the best way in case there are multiple. For example, iMessage is free compared to SMS and always has delivery receipts, [or Slack has more rich media features than Skype]. SMS uses something called "Home Routing" which tells whether the endpoint is available.

Appendix S - Email Interview with Istvan Lajtos (Director of Web Working Group - GSMA)

Sacha Nacar: What is the actual identifier that platform providers see with the Mobile Connect logins?

Istvan Lajtos: MSISDN – Mobile Subscriber ISDN number, otherwise if you are referring to a "Service Provider", they have no visibility to the MSISDN, they can only see Mobile Connect Identifier (PPID) as it is defined in OpenID Connect specification.

Sacha Nacar: How has Mobile Connect integrated USSD and SIM Applets? What data does this integration provide to Mobile Operators?

Lajtos: Mobile Connect does not bind to any authenticators. So it could either be USSD or SIM Applets used. It has a pluggable authenticator mechanism, any authenticator can be used/integrated.

Sacha Nacar: When users log in with Mobile Connect on a platform, are platform developers able retrieve any type of personal information about the user sent back from the Mobile Operators?

Lajtos: No, platform developers cannot retrieve any kind of PERSONAL DATA of the user, without explicit consent from the user. The information is safe with MC.

Sacha Nacar: Does the Discovery API work by just recognizing the operator from the phone number in the auth input or does it use any information from the SIM card?

Lajtos: Only MSISDN is used for Discovery API to identify the operator, nothing from SIM.

Sacha Nacar: What is being done to strengthen the security weaknesses linked to SIM Encryption (eg. Gemalto Hack 2015) or OAuth (eg. Covert Redirect Security vulnerability). Are there any other privacy and security concerns linked to a universal single sign-on mechanism that Mobile Connect has/will have to deal with?

Lajtos: Mobile network authentication is a secure and closed environment which is difficult to compromise and hack.

Sacha Nacar: How does Mobile Connect/GSMA plan to federate if there is such a large fragmentation of communication platforms operating with diverse signalling frameworks? Is an open standard like Matrix.org being investigated?

Lajtos: Matrix.org is using signalling for UC type services specially focusing on VOIP / SIP signalling convergence in my opinion. Mobile Connect follows OpenID Connect standard. Nothing else.

Sacha Nacar: Is Gov.UK Verify powered by Mobile Connect technology through Verizon in any way?

Siva (Lajtos' colleague): cannot disclose this, but Mobile Connect can be used anywhere.

Sacha Nacar: Facebook recently launched "Account Kit" which allows developers to build authentication systems based on the end user's phone numbers. Is this a part of Mobile Connect or a competitor?

Siva (Lajtos' colleague): NO, it is different , Mobile Connect is provided by Mobile connect Operators.

Sacha Nacar: How do regulators view GSMA potentially federating a universal identity management system in the future? Would they be pushing to keep fragmentation in place?

Siva (Lajtos' colleague): It depends on the choice. But, we recommend if Mobile Connect is used, you will be more secured and personal data is protected.

Appendix T - Interview with Alan Quayle

Sacha: Are people using their phone numbers anymore?

AQ: Well we've not been using phone numbers for at least 10 / 20 years now because you have a contact list and even when we did actually have to physically dial them in we had an address book with phone numbers. So we never really, if you like, use them in terms of directing, we've always had some augmentation whether it's a contact book or your phone book that enable you to translate from Sacha to a telephone number or my case I'll just look through and say Sacha and then "Ah there's a cellphone number" and they know basically how to call it so it's used today for the PSTN, it's used in a number of ways for identity so it's very active. It has its limitations because you have pre-paid/post paid. I've had the same number now for 18 years and people are shocked when they call this number (because you know they've updated their address book and they're like: "I wanted to talk to you, I wasn't sure this number was going to work but it works!") so it's transitory identity also country by country it's different. Some like in Italy it's very closely linked to your national identity because that's the one thing that you get. I have 2: I have my social security number in the US and I a similar number in the UK. That can't change. You can change your name, you can change your address or you can change your emails, you can change your phone numbers but that's one identity that remains the same but that's only ever used in terms of government, identity checks. But from that, the phone number remains an important aspect of your identity because of some of the regulations that exists around them. But again, very variable.

Will it be still used for voice? Absolutely. For traditional PSTN based voice, that's in the decline, it's not going to disappear any time soon but it's there. If I need to call you and I don't see a present on Skype or you know one of the platforms we're already connected on, I'm going to call you. So it will remain part of the portfolio communications and we appear of the geeks by using the whole of other systems. [Groupama] was saying: "farmers use feature phones. (My parents basically don't use any IT but) My mom it took years to get her to use Skype, now she uses Skype all the time but she still uses the phone as well. Now it will age out but again this is signification portion of the population that just is not anti-tech - it's just they haven't need to be in there and the governments will always want a national communication infrastructure that's controlled and managed by the government full stop. So for the national security reasons

they will always be a national phone network or national communications network and the phone number, because it's regulatable, is always part of that.

Sacha: Also, it's not only about age but also about demographics. For example in many parts of Africa, the use of SMS is widely spread in Africa and so they use the phone number as well.

AQ: Yes. You know there's a whole range of different services that they have in Africa to enable people to... they use Voice. Now, it is transitioning quite rapidly look at Nigeria there over 50% smartphone penetration but the actually sort of mobile data brand are actually I think less than 20% because of the price. They have to pay almost like a chance, education to get more data plan but what you see is people using Wifi, Hotspot all range of other services so they are becoming more data aware. So again, we're seeing that transition but again because you want that lowest common denominator that can reach everybody - that phone number remains.

In the US, for example, when I was doing my citizenship I got an SMS at work to let me know that the paperwork has been received; the reason they use SMS is you can reach over 90% of the US population reliably. E-mail you can't because there's SPAM filters, you can check their e-mail, for phone number nobody answers their phones so again the phone number for either Voice or SMS has that you can just reach people.

...

AQ: They use a variety of services. I use multiple emails, multiple phone numbers for different platforms whether it be Facebook, whether it be with Whatsapp or whatever. You can have multiple identities on these platforms. Some people will use different platforms for different application so for example, maybe the same platform with multiple identities or they may just clearly segment so for example, Skype for them is work while Facebook Messenger for them is pleasure. The two don't mix so what we're seeing is sort of mixing and matching and the

reason why on my desktop I have Skype, I have Wire, I have Telegram, I have Spark is because I have multiple composition going on with different groups of people. Is that a pain? Well no because the operating system is acting as the aggregator and a lot comes in, is a message from so and so and i just answer on that particular platform is it a pain? Well no not really. You know it's one where multiple identities are going to exist, the need to integrate across those multiple identities is actually very low. Is it inconvenient? Yes it could be easier but you could say life could be easier as well. ...

If Facebook came around with more of a more integrated proposition, it was more a platform playing rather than just being social media. MySpace got bought and mismanaged and we're going to see this. Companies are going to get bought. Going to be more integrated in more platform play or could be that they are mismanaged and go off to another direction. We've got the big facebook development conference going on today. They're going to set out clearly their rationale for why they made the 22 billion dollar investment in Whatsapp. They're going to be showing Bots, they're going to show their platform in basically a foundation upon which businesses can run their bots because got a billion plus people on their platform. My recommendation always remains treat Facebook because it is evil as a channel and put your intelligence and data at a layer outside of Facebook because they're all about harvesting your data and they're using it for advertisements.

Sacha: You touch a lot on this fragmentation of identity and some of the things i'm trying to research is the tradeoff between more unified platform versus security concerns or more fragmentation versus practicality. You seem to think that, from what you just said, there may not be such a need for frameworks like Matrix?

AQ: I think there is a need for it, it's not a mass market. I think that for segment, for groups of people, groups of businesses, for particular ecosystems to be able to enable and to operate effectively given they're tracked within particular silos this is great because it enables that group to be empowered. My personal view is Matrix is essential for us as individuals because it

removes the power in the silos. Hence why I say Facebook is evil because it is created a massive silo and it just wants to melt that silo.

...

AQ: I think that Matrix is absolutely essential from just a humanity perspective but in terms of driving of significant business - something that solves a general case, no. I think it'll be used for a lot of for example ecosystem so it could be like a supplier, contractors that are on different messaging platforms within their channels of communication - it now enables those systems to work together so you don't have to do rip and replace: "we're going to use this parallel system". It will enable them working as they've always done and to operate. So that's where I think we'll see in the next 5 years most of the money being made with Matrix.

Sacha: I wanted to touch again on these different identities, the different silos you talk about. Do you think emerging MVNO companies like Google Fi will attempt to just get rid of the phone number as identifier and just use whatever they need?

AQ: No. The primary identifier will be your Gmail. So they will want you to be on Gmail. If in terms of Google Fi and that to find your whole experience or content or your apps so you basically... whatever phone you are using is just entering your Gmail address and then its the phone you've always known and loved with all the services but the phone number as the lingua franca that enable to work with AT&T to be able to talk to your friends to be able to text them will always be there simply because the government, the regulator will mandate it. So your Gmail and phone number will both exist. Now from Google's perspective Gmail defines everything. But as an individual the number you can contact or text me on if we're not already connected by other platforms it always remains this particular number.

Sacha: So we will always have this dualship ?

AQ: Yes because government will mandate it.

Sacha: Is that something you see across all regions of the world?

AQ: Yes absolutely. Most of the regulators that I talk to see this as it's not going away. It's too strategically important to the operations of the country to seed anything outside the country. China, no way. They have their own internal apps but for them, they will never seed anything to Apple or Google same is true when you talk to regulators in Africa, in Asia, in Europe so it will always remain there just for national security purposes as a result always remains the network of last result. The problem as a Telco is how do you make money on the network of a last resort. That's the challenge.

...

AQ: You were talking about the fixed lines of PSTN. What I find very interesting is again, they haven't gone because all call centers you have all basically these business lines people want to have a business phone because it's the lowest common denominator. If you look at the US and some of western Europe we're down to 25-26% households that have a phone line. Now that's slowly aging out, you generally find sort of baby boomers and above that sort of have a phone line but also you see with the triple play that in the US it's free, the phone line for your home is free so it just remains there. We got rid of our fixed phone line years ago but I still have an office fixed/VoIP line because I have to call the world and I need reasonable rates because not everybody is using Skype or some other IP communications platform so that's one of the reason why I still have a traditional PSTN number so again all this means that it remains as the network of last resort. It's good and regulated so it will always remain there. What gets more interesting is that across all these other identities what's going to come to the floor. Apple doesn't care: "just give us an email and use it". They don't care whether it's an Apple or whatever. Google wants you to have a Gmail and they will do their best to force you into getting a Gmail one way or the other so it's all under their control. Facebook, again, doesn't care: "give us your email, we'll just trap you in with all your data and all the apps and all the your friends that's using anytime".

Appendix U - Interview with Matthew Hodgson, Founder Matrix.org

Sacha Nacar: Do you have any opening comments about the future of the phone number?

Matthew Hodgson: Yes. Obviously, this is a very relevant problem for Matrix and it's also not one that we have solved yet. Matrix itself is obviously about interoperable communications at the signalling layer. There's one problem to get the signalling back and forth and another one to identify the person that you're talking to. Now, the strategy that we have taken is to start off with a kind of bootstrapping process where we have kind of a centralized, logically centralized, entity that manages identity. We call it the identity servers, it would be better to call it the "identity mapping servers" because all it does is to take existing ID systems likes E164 numbers from the PSTN or email addresses or anything really and map it through to Matrix IDs. So this is a temporary thing that we've done to get things up and running and right now it only covers email addresses. It would be obviously to extend it to E164 but we haven't done that yet. And there are two things that need to happen before we solve this problem. First of all, Matrix ID's themselves aren't intended to be publicly visible but they are right now and as you know, they look like an "@" and the username code on the back. So it's linked to DNS and has all of the same disadvantages as anything built on DNS that it's is basically again a centralized system. You have your DNS route servers run by different universities and governments and if those route servers are attack would compromise, even with DNS SEC or if DNS SEC infrstructure is compromised, that's still one place where you can kill and contol the entire identity system. So we've got that problem that Matrix's internal representation is currently up to DNS. On the other side, we've got the problem that the mapping servers need to be decentralized to like the rest of Matrix. Right now there are 3 servers run on Matrix.org and Vector.im and one of the developers runs his own server which form 3 clusters of the existing identity mapping servers. All this does is to take a third party ID like an email address and validate it and associate it

with a Matrix ID. So if I wanted to discover you on Matrix right now I got to the ID server and say "I want to take sacha@gmail.com" and hopefully you've gone and registered your identity on Matrix as a part of that email address. If you have, it will give me back your Matrix ID and I'll talk via Matrix to it. So, a horribly centralized setup and it's not cool because if we turn off the servers or deleted the databases or sold the mapping information, which is quite valuable because it's real email addresses, then that's a big problem for the Matrix community. But that's where we're at right now.

So we obviously want to fix this and it's a really hard problem so you've got a good thesis to talk about here. First of all, we don't want to lock it to any given ID system. We do not want to fixate on the E164 being the only system because in practice there are already many different ID systems out there. You've got Facebook IDs, you've got email addresses, you've got phone numbers, you've got...In the more interesting world, you've got public keys. So your Bitcoin ID is an identifier and is just the fingerprint of your public Bitcoin key. All of these different things and it would be stupid to think any one system is going to win because it's already fragmented. So what we need is something that can map between them. So in terms of whether the phone number is dying - yes, it's already dead as a universal identifier. It's still a very common one, but there are many other common ones out there. So the race is really to build a decentralized secure servers on top of the different ID systems out there such that you can map between them. Now the good news for us on Matrix is that this has nothing to do with Matrix. The problem of mapping your email address to your blockchain Bitcoin ID is the same problem as mapping your phone number to your Matrix ID - you would use the same solution for both. And that doesn't exist today and it has to exist and then that will clearly replace the phone number as the single identifier that historically the phone number has been. The time frame for that is probably the next 2 to 3 years or so. It's really interested because it is a current area of research and it is an unsolved problem.

...

Matthew Hodgson: So this is basically where we are at today. Knowing that it's a problem and not having a solution but talking quite a lot about it with other people in the industry and not in the VoIP industry specifically. But talking to the Bitcoin/Cryptocurrency community, talking to the email community because it's a very relevant problem and it gets really interesting because if you do have some kind of decentralized secure database that tracks people's identities and mappers and map between them, it's also a really useful place to store any metadat about people and in Matrix we have the problem of reputation. So, if you imagine that Matrix is widely successfully and I can fire up Slack and I can talk to you on Skype and I can send you an SMS and everything has this kind of glue connecting it together, without a reputation and an anti-abuse mechanism, all we've doen is to create the single biggest SPAM vector known to man. As you know, the Matrix API is just one HTTP hit to go and send a message anywhere and imagine how bad it would be if somebody could just take that API and literally spam anybody anywhere. We've reinvented email's spam problem but applied it to every instant message and VoIP tool and that would be a catastrophy. So we need to fix it on Matrix both to the identity mapping system and at the same time somehow keep track of these identites whether you are trusted or whether you are not trusted in terms of what your spam reputation is.

...

Matthew Hodgson: So there are lots of antispam techniques whether it's a micropayment tax or a reputation based system or just plain spam fitlering doing bayesian filtering and artificial intelligence to detect whether it's spamming or not. It is the same problem as email spam and it's a really hard one. It is also politically a really hard problem because Spam is not an absolute spectrum. One person's direct marketing material is another guy's spam just like one person's terrorist is another guy's freedom fighter. It's not a system where you can literally give everybody an absolute rating from +100 to -100 dependign on how reputable you think they are.

Appendix V - Interview with Alain Wahba, CEO Infobel

FR – Alain Wahba: J'avais une conférence à Paris en 2003. C'était sur le "Disruptive Competition justement et je parlais, je disais que les White Pages vont disparaître à un moment pour être remplacées par deux types de profils. Déjà en 2003, malgré le fait que Facebook c'est 2006, j'avais dis Facebook et LinkedIn. LinkedIn à commencé super tard mais il y'avait déjà des pendants, les equivalents. J'avais expliqué qu'en realité, déjà à l'époque, les gens vont demander à se delister des annuaires pour des raisons de "privacy". On voit en Europe, on diminue au niveau des quantités. Pour, entre guillemets, réapparaître de façon encore plus visible, donc c'est un paradox. Encore plus visible sur les réseaux sociaux avec encore plus d'information qu'ils "disclosent" en vie privée mais de façons totalement différente. Donc j'ai expliqué qu'un des challenges c'est de faire le lien entre les identifiants "online", donc par exemple sur Facebook ou LinkedIn et la donnée telephonique. Donc quelque part, tu peux créer a partir de la donnée telephonique une base de profil et la lier à l'autre. Quand elle est liée, elle devient très puissante. Pourquoi? Parceque tu peux donner n'importe quel numéro de téléphone mais à partir du moment ou tu donnes un téléphone qui est lié à une adresse que tu peux decider de cacher ou pas, mais qui est ensuite liée à des profils LinkedIn ou Facebook, la combinaison si elle est verifiée derrière par le téléphone qui était listé devient indéniable vu qu'elle à été connectée à la main par quelqu'un. Donc c'est une source de verification physique indéniable.

EN – Alain Wahba: I attended a conference in Paris in 2003. It was about "Disruptive Competition" and I was speaking. I was saying that the White Pages would disappear and be replaced by two types of profiles. Though Facebook was from 2006 , I had mentioned Facebook and LinkedIn. LinkedIn started much later but there were already the foundations for such a service, equivalents. I explained that in reality back then, people would ask to delist from directories for privacy reasons. We can see already in Europe diminishing quantities. Instead, they would quote-unquote reappear in a more visible way, hence it's a paradox. They would be more visible on the social networks with even more information that they disclose in private

in a totally different manner. So I explained that one of the challenges would be to link these online identifiers like on Facebook or LinkedIn with the phone number. So you can create a base profile from this telephone number and link it to the other. Once linked, it becomes very powerful. Why? Becayse you can give any number but once a telephone number is linked to an address, which you can choose to hide or not, that is in turn linked to a LinkedIn or Facebook profile, the combination - if verified using the phone number listed- becomes undeniable because it was connected by hand. Therefore it is a source of undeniable physical verification.

...

FR – Alain Wahba: Je disais déjà en 2003 que le challenge est de lier des profils professionels, profils sociaux à l'idientifiant en ligne téléphonique parce qu'après tout ce que tu peux en faire est beaucoup plus puissant. Quelque part c'est le seul moyen qui est possible pour palier au fait que les gens vont vouloir, pour des raisons de "privacy", se délister des annuaires. Je pense que les gens ont moins de problèmes d'être contacté par email ou messages que d'être contacté sur leur téléphone. Par exemple un message SMS est une aggression alors qu'un message Facebook n'est pas une aggression. C'est la perception. Et donc de ce fait la, il faut pouvoir reconnecter les deux. Nous avons developé des capacités de rapprochement, on l'avait fait sur des produits d'ID Verification ou les gens essayaient de retrouver les mauvais payeurs. Ça permettait de faire le lien sans que eux l'aient fait eux meme. Je pense que à terme il faudra donner la possibilité, de la même manière qu'on donne la possibilité à quelqu'un sur Facebook de "login" et de rajouter son information personelle, de faire l'inverse - pouvoir faire des "Login" de type Facebook mais telephonique à partir de ceux qui gèrent le téléphone.

EN – Alain Wahba: I was already saying in 2003 that the challenge would be to link professional profiles with social profiles to the telephone network's identifier because then, everything you can do with it becomes much more powerful. In a way, it is the only possible way to counter the fact that people wanted to delist for privacy reasons. I think people have less problems with being contacted by email or message rather than being contacted through

the telephone. For example, an SMS message is an aggression while a Facebook message is not. It is the perception. In that way, we need to be able to reconnect the two. We have developed ways to connect, we've done it on ID verification products where people tried to find bad debtors. That allowed to make the link without need them to do it themselves. I think that, in time, we need to give the possibility the same way there is on Facebook to login and add personal information, to do the opposite: create logins a la Facebook but leveraging the telephone number right from those that manage the issuing of numbers.

...

FR – Alain Wahba: Ça prouve et ça démontre que la certification est devenue liée au telephone, la certification est devenue importante. Je vais te donner un exemple: On a reçu un message sur Twitter le mois dernier qui disait: "Quand est-ce que Infobel publiera le profil que je viens de creer?" Normalement quand les clients payent un plan "basic" on fait une verification pour être sûr qu'il ne s'approprie pas le profil d'un tier. On lui a repondu "demain mais pourquoi?". Et [le client] repond "parce que VeriSign et Thawte don't want to create a profile until it is online on Infobel." Donc [Thawte et VeriSign] ne veulent pas certifier l'existence du business avant que ce soit sur Infobel. Il savent qu'on vérifie si les gens existe et si c'est pas [verifié] chez nous, ils n'acceptent pas.

EN – Alain Wahba: This proves and demonstrates that certification has become linked to the telephone, certification has become important. I will give you an example: we received a message on Twitter last month that said: "When will Infobel publish the profile I created?" Normally, when clients purchase a basic plan, we perform a verification to be sure they are not stealing someone else's profile. We responded: "Tomorrow, but why?". He responded "because VeriSign and Thawte don't want to create a profile until it is online on Infobel." So Thawte and VeriSign don't want to certify the existence of the business before it is on Infobel. They know that we verify if the people exist and if it isn't verified by us, then they don't exist.

...

FR – Alain Wahba: Le "Presence Management c'est une chaine de certification parceque tous ceux qui gèrent la presence de tiers sont en "procurement" et ont vérifie l'identité de chacun et la garantisse. Nous, derrière, on recoit des données garanties donc ce qui est chez nous est garantis. La donnée vient du registre du commerce, la donnée qui vient du telco est garantie. Donc finalement on a que des sources "legit". Ça c'est une des choses qui fait que quelque part on est incontournable parfois sur ce type de donnée. On est les seuls à combiner toutes ces sources ensemble.

EN – Alain Wahba: Presence Management is a chain of certification because everyone that manages someone's presence are in procurement and have verified everyone's identity and provided guarantee. We, behind the scenes, receive guaranteed data so hence we provided guaranteed data. Our data comes from the Trade Register and the telco, both are guaranteed. Hence, we only have legitimate sources. That is one of the things that make us unavoidable sometimes on this kind of data. We are the only ones to combine all these sources together.

...

FR – Alain Wahba: Si on reflechit aux ["Disruptive technologies"], finalement les LinkedIn et les Facebook ont déjà "disrupté" l'industrie et transformant l'usage de ton contact mais l'identité de ton contact se fait par des biais différents. C'est à dire que ce n'est pas en te téléphonant que je suis en contact avec toi et je suis obligé finalement de m'enregistrer à differents endroits pour être en contact là oû tu es.

EN – Alain Wahba:

If we think about Disruptive Technologies, the LinkedIns and Facebooks have already disrupted the industry and have transformed your contact's usage however your contact's identity is done via different parties. Meaning that I don't have to call you to be in contact with you, I have to be registered at all these different [applications] to stay in contact wherever you are. **...**

FR – Alain Wahba: Le numero de téléphone, derriere ton ["smartphone"] , tu as ton compte Whatsapp, Viber, etc. Derrière ce téléphone et cette verification unique tu peux avoir une dizaine d'application qui appellent les gens.

EN – Alain Wahba: The phone number, behind your smartphone, you have your Whatsapp account, Viber, etc. Behind this telephone and this unique verification you can have a dozen of applications that can call people.

...

FR – Alain Wahba: Quelque chose d'intéressant à analyser c'est "est ce qu'on est en technologie intermediaire ou technologie définitive? Ça c'est quelque chose que tu devras trancher. Pourquoi? Parceque, mets toi en perspective arrière: tu vois Skype arriver, il n'y a pas encore WhatsApp, etc. Tu vois que tout le monde se cherche par un nom dans un annuaire qui devient mondial alors que ce n'est qu'une des fonctionalités de [Skype]. Tu le vois comme disruptive competition et tu essayes de réagir à cette competition. Sauf que ce n'est peut etre pas la bonne reaction ni au bon moment parce que si tu regardes ensuite la démultiplications des "instant messengers" et le nombres d'identifiants differents que les gens créent, le besoin réel était justement de revenir à un identifiant unique. Le [numero de] téléphone n'était finalement pas en danger. Et eux ce sont quelque part focalisé par "le téléphone va mourrir parce qu'on devrait plus trouver les gens par le téléphone car il y'a un autre directory". Mais non, car il y'a d'autre directories, [chez Facebook par exemple].

EN – Alain Wahba: An interesting point to analyze is whether we are in intermediary or definitive technology. This is something you will have to decide. Why? Because I you put yourself in back perspective: you see Skype coming and WhatsApp doesn't exist. You see that everyone is looking each other up by name in a directory that is becoming worldwide while it is only one of Skype's functionalities. You see it as a disruptive competition and you try to react. However, it is perhaps not the right reaction or the right timing because if you then look at

the demultiplication of instant messengers and the amount of different identifiers that people are creating, the real need was actually to come back to a unique identifier. The phone number was not in danger. They focalized on "the phone number will die because we would not need to find people by phone because new directories are coming." In fact, they were other directories, like Facebook for example.

...

FR – Alain Wahba: Finalement, tout ces produits sont des technologies intermediaires mais on va arrivé a un "Unified Messaging System" qui est toujours une ambition des gens qui ont dix utilisations. À un moment il y'aura un Unified Messaging System qui gérera un seul ID. Je pense que le [numero de] téléphone sera l'unique ID de gestion.

EN – Alain Wahba: Finally, all these products are intermediary technologies but we will arrive to a Unified Messaging System that has always been an ambition for people that have a dozen utilizations. At one point, there will be a Unified Messaging System that will manage a single ID. I think that the phone number will become the unique ID for management.

...

FR – Alain Wahba: Aujourd'hui, la problématique c'est la démultiplication des moyens de communications sur un outil unique. Donc avant on avait un systeme de navigation "onboard", un PC, etc. Il y'a eu une convergence de ces technologies vers le smartphone. Le smartphone est un élément de convergence et est en train de produire l'inverse de la convergence. Donc on est dans un [environement] "one-to-many" et je pense que le challenge sera de faire du "one-to-one" sur des créneaux, par exemple les flux d'information.

EN – Alain Wahba: Today, the problem is the demultiplication of the communication means on a unique tool. Before, we had a navigation system, a PC, etc. There has been a convergence of these technologies onto the smartphone. The smartphone is an element of

convergence and is starting to create the inverse of this convergence. So we are in a “one-to-many” relationship and I think that the challenge will be to develop “one-to-one” on channels and flux of information.

...

FR – Alain Wahba: Cette démultiplication va, d’après moi, induire une convergence future par thème. Parceque les gens n’utilisent pas les applications autant qu’on le pense. Il y’a 95% d’usage le premier moi et plus que 5% d’utilisation d’usage après le 12eme mois quand tu installes une application. Par contre si tu arrives à créer ces pools, on s’en fout quel est l’usage de cette application. Tu te dis "mince, je ne recois qu’une message par an sur Kik". Si tout était consolidé, alors je m’en fout d’avoir [été enregistré] à 100 applications derrière, du moment que quand je recois l’info et que je répond, il le recoit. Idem pour les applications de communications téléphoniques.

EN – Alain Wahba: This demultiplication will, for me, lead to a convergence by theme in the future. This is because people are not using application the way we think. There is 95% utilization rate in the first month and only 5% in the 12th month when installing an application. Instead, if we’re able to create pools of information channels, we will not mind what the use of the application is. You’re thinking “I’m only receiving one message on Kik per year, [what’s the use?]”. If all this was consolidated, I would not mind having hundreds of applications downloaded and profiles registered, as long as when I receive the message and I reply, the other party receives it. This is the same for telephony applications.

...

Appendix W - Interview with Nigel Brown (Head of ICT Resilience, UK Cabinet)

Nigel Brown: The other big issue that needs to be really looked at is to do with authenticating individuals, credentials, and bindings. So what do I mean about that? And I may need to bring it up in the context of phone numbers. A phone number is a special form of binding. So, I have a security pass. The security pass some coded things on it. It has got my name, it's got a picture. So that security pass binds my name that is printed on this pass, that you can't change, to a picture which is me. So a passport has other bindings to it. The reason that European passports are so important these days is because they bind you biometrically whether you know it or not. The fact that there is a photograph on it that's being used certainly by the British to provide electronic authentication of you as an individual at the borders. So, bindings are complicated and have historically been used in the telephone number space for billing.

...

Nigel Brown: As you realize, we're moving into a world where the language around telephony is changing. We don't talk about subscribers, we talk about customers. So that's changing and along with that change, the telcos are currently agonizing big time about their completely [wrecked] business models. They are charging you for something you don't want and they are giving you something you want for nothing. That's a completely [wrecked] business model. So we are in a real state of flux at the moment and the state of flux is always complicated to look at and that is why I pull out those ideas to do with resilience and security and to do with the fundamentals of authentication.

Nigel Brown: The authentication space is particularly interesting because, you are probably young enough to be part of the "Wild West Internet" as it was in the 70's. Today's much less of a wild west space and if you want to explore the wild west you have got to explore the Dark Web. The Dark Web is difficult because the search tools are fairly cryptic to use and finding your way around the Dark Web is challenging. So the Wild West of the visible Internet is being

challenged quite dramatically as a consequence of basically preventing people from hiding.

...

Nigel Brown: So at the end of the day, those that are offering services want to know who they are offering service to. So it doesn't matter whether you're transacting a currency and the banks need to know that for money laundering and other purposes; whether you're ordering a barrow and a book on the internet, they need to know who to send that to so you need some binding to a physical address. Whereas if you're holding a conversation and you want me to get back to you, I need to know how to get back to you. So in the old days, I'd get back to you either by looking your physical address up. Then we moved on [...] electronically, I need to reach you, you have an email address perhaps or I get you on Facebook or other social media by your handle. So we're seeing a physical world becoming increasingly virtualized, namely: you can't put your paws on it. So the consequences of that are that you've got more challenges with binding people to a means of getting a hold of a person. Because ultimately, you want people to tweet you, you want to be part of a Facebook community, you want to perhaps do other things. So it's all to do with locating people and being able to have two-way conversations with them. [...] The key thing is it's all to do with tying people down.

...

Nigel Brown: It's all to do with being able to identify [someone] and the future is really exciting because smartphones are increasingly stuffed with sensors. One of them is a GPS sensor. So do I need to know your physical address? No because I'm not sending you a letter, I need to communicate with you. Do I actually need to know where you are now? [...] No. I think it's all to do with what is the purpose of the communication all about? If I want to communicate with you, your smartphone tells me exactly where you are on the planet within a few meters and that is what the emergency services are starting to do.

...

Nigel Brown: We are moving from a physical address to "do we really need an address?" [...] And Increasingly, [smartphones] are becoming part of you, unlike a computer where I can have multiple logins. You can share a computer, you can't share a [smartphone]. There's only one account you can have, you can have one password on it. Unless you share your password with me and then we share the phone.

Sacha Nacar: It represents you as an individual

Nigel Brown: Yes absolutely. So, the physical binding [...] that [security passes] provide, we're seeing them already with the smartphones. We're seeing it already with close proximity payment charging, done on mobile phones. Apple Pay is a classical example. So we're coming to a really exciting time where the phone providing, you've authenticated yourself to it, [...] at the moment it doesn't require a certificate of authenticity. It just requires your PIN number.

Sacha Nacar: Would it need a certificate?

Nigel Brown: Depends on how strong you want the binding to be?

...

Nigel Brown: The future, I suggest is very different. As we end up with this Internet of Things [scenario] that I've talked about and if we can't get over some means of perhaps a higher trust relationship with an authentication token you can see all sorts of exciting things happening. So rather than you going to the hospital and having an implant that can't be removed. For example, an implant put into your spine that you can't removed unless you die or become completely imobilized. That is sort of what I call a "passport" end of the market. Somewhere in the intermediary, you could use the forward-facing camera in the smartphone to authenticate yourself using visio-biometrics to provide you with a high degree of authentication.

...

Nigel Brown: Everything is moving in a very confusing space at the moment. Hence all the dynamics you are seeing in the ICT world, one of the key things in that space is clearly having a gorgeous, covetable, device is not going to be one we rely on. What are you going to use it for? Content. So content is king.

Sacha Nacar: Content is the driver.

Nigel Brown: A lot of the dynamics in the ICT space is driven by access to content, I would suggest.

References

[1] PWC Chair in Digital Economy. "Digital Identity 3.0 The Platform for People." (n.d.): n. pag. Chairdigitaleconomy.com. PWC, 31 Aug. 2015. Web. 4 June 2016. <http://www.chairdigitaleconomy.com.au/wp-content/uploads/2015/08/Digital_Identity_30_20150831_FINAL.pdf>.

[2] Kuznetsova, Olga. "Grow Your App with Account Kit: Give People New Ways to Log In." Facebook Developers. N.p., 12 Apr. 2016. Web. 05 June 2016. <https://developers.facebook.com/blog/post/2016/04/12/grow-your-app-with-account-kit/>.

[3] Digits. "The Future of Identity." Digits. N.p., n.d. Web. 05 June 2016. <https://get.digits.com/phone-based-sign-in>.

[4] Hart, Chad. "Does Telephony Matter If No One Talks to Each Other Anymore?" Medium. N.p., 18 Jan. 2016. Web. 5 June 2016. <https%3A%2F%2Fmedium.com%2F%40chadwallacehart%2Fdoes-telephony-matter-if-no-one-talks-to-each-other-anymore-5edf61f27e71%23.bu4467r71>.

[5] GSMA Association. "The Mobile Economy 2015." (2015): n. pag. GSMA Mobile Economy. GSMA Intelligence, 2015. Web. 5 June 2016. <http://www.gsmamobileeconomy.com/GSMA_Global_Mobile_Economy_Report_2015.pdf>.

[6] Ericsson Consumer Lab. COMMUNICATION IN THE WORLD OF APPS. Rep. Ericsson Consumer Insight, June 2015. Web. 5 June 2016. <http://www.ericsson.com/res/docs/2015/consumerlab/ericsson-consumerlab-communication-in-the-world-of-apps.pdf>.

[7] Ofcom. "Techie Teens Are Shaping How We Communicate." Ofcom. N.p., 07 Aug. 2014. Web. 05 June 2016. <http://media.ofcom.org.uk/news/2014/cmr-uk-2014/>.

[8] Ericsson Consumer Lab. Wi-Fi Calling Finds Its Voice. Rep. Ericsson Consumer Insight, July 2015. Web. 5 June 2016. <http://www.ericsson.com/res/docs/2015/consumerlab/ericsson-consumerlab-wifi-calling-finds-its-voice.pdf>.

[9] Ericsson Consumer Lab. The Networked Life. Rep. Ericsson Consumer Insight, Nov. 2015. Web. 5 June 2016. <http://www.ericsson.com/res/docs/2015/consumerlab/ericsson-consumerlab-the-networked-life.pdf>.

[10] "Disposable, Temporary Virtual Phone Numbers." Tossable Digits. N.p., n.d. Web. 05 June 2016. <http://www.tossabledigits.com/>.

[11] Ring Me Maybe. N.p., n.d. Web. 05 June 2016. <http://www.ringmemaybe.com/>.

[12] Burner App. N.p., n.d. Web. 05 June 2016. <http://www.burnerapp.com/>.

[13] Hushed. N.p., n.d. Web. 05 June 2016. <https://hushed.com/>.

[14] OnOff. N.p., n.d. Web. 05 June 2016. <http://www.onoffapp.com/>.

[15] GSMA. "Mobile Connect." GSMA. N.p., n.d. Web. 05 June 2016. <http://www.gsma.com/personaldata/mobile-connect>.

[16] W3C. "DRAFT Web Identity Working Group Charter." Web Identity Working Group Charter. N.p., n.d. Web. 05 June 2016. <https://www.w3.org/2011/08/webidentity-charter.html>.

[17] Strange, Adario. "Facebook F8: Everything You Need to Know." Mashable. N.p., 12 Apr. 2016. Web. 05 June 2016. <http://mashable.com/2016/04/12/facebook-10-year-plan/>.

[18] Meukel, Markus, Markus Schwartz, and Matthias Winter. "E-SIM for Consumers–a Game Changer in Mobile Telecommunications?" McKinsey & Company. N.p., Jan. 2016. Web. 05 June 2016. <http://www.mckinsey.com/industries/telecommunications/our-insights/e-sim-for-consumers-a-game-changer-in-mobile-telecommunications>.

[19] IET. "Contacting the Emergency Services in the Digital Age." IET. N.p., June 2015. Web. <http://www.theiet.org/policy/panels/comms/999/index.cfm?utm_source=redirect&utm_medium=a

[20] Europa. "Full Synopsis Report of the Public Consultation on the Evaluation and Review of the Regulatory Framework for Electronic Communications - Digital Single Market - European Commission." Digital Single Market. N.p., 20 Apr. 2016. Web. 05 June 2016. <https://ec.europa.eu/digital-single-market/en/news/full-synopsis-report-public-consultation-evaluation-and-review-regulatory-framework-electronic>.

[21] Eisenach, Jeffrey, and Bruno Soria. A New Regulatory Framework for the Digital Ecosystem. Rep. GSMA, 2016. Web. 5 June 2016. <http://www.gsma.com/publicpolicy/wp-content/uploads/2016/02/NERA_Full_Report.pdf>.

[22] Mark, Christian. "Mobile Identities - Digital Identity Services By MNOs". February 2016. Presentation. <http://www.gsma.com/personaldata/wp-content/uploads/2016/02/MWCB16-Mobile-Identities-Digital-Identity-Services-by-MNOs-Christian-Marc.pdf>.

[23] GSMA Association. MOBILE CONNECT CONSUMER RESEARCH REPORT: EUROPEAN UNION. Rep. GSMA Intelligence, Oct. 2015. Web. 7 June 2016.

<http://www.gsma.com/personaldata/wp-content/uploads/2015/10/Mobile-Connect-consumer-research-report_EU.pdf>.

[24] FIDO. "About The FIDO Alliance." FIDO Alliance About The FIDO Alliance Comments. N.p., n.d. Web. 07 June 2016. <https://fidoalliance.org/about/overview/>.

[25] FutureID Consortium,. "Futureid - Shaping The Future Of Electronic Identity". 2016. Presentation. <http://futureid.eu/data/reveal/vision.html#/2>

[26] Ienco, Marta. "Digital Identity As A Key Enabler For E-Government Services". 2015. GSMA. Presentation. <http://www.gsma.com/personaldata/wp-content/uploads/2016/02/MWCB16-Digital-Identity-as-a-Key-Enabler-for-eGovernment-Services-Marta-Ienco.pdf>.

[27] Low, Aloysius, and Seth Rosenblatt. "Serious Security Flaw in OAuth, OpenID Discovered." CNET. N.p., 2 May 2014. Web. 07 June 2016. <http://www.cnet.com/uk/news/serious-security-flaw-in-oauth-and-openid-discovered/>.

[28] Radicati, Sara, and Thomas Buckley. "Email Statistics Report, 2015-2019." EDiscovery Market, (2019): n. pag. Radicati Group. The Radicati Group, Inc., March. 2015. Web. 15 June 2016. <http://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf>.

[29] Radicati, Sara, and Thomas Buckley. "Email Statistics Report, 2013-2017." EDiscovery Market, (2013): n. pag. Radicati Group. The Radicati Group, Inc., April. 2013. Web. 15 June 2016. <http://www.radicati.com/wp/wp-content/uploads/2013/04/Email-Statistics-Report-2013-2017-Executive-Summary.pdf>.

[30] World Bank. "Identification for Development." World Bank. World Bank, n.d. Web. 15 June 2016. <http://www.worldbank.org/en/programs/id4d>.

[31] GSMA. "GSMA's Mobile Connect Available to 2 Billion Consumers Globally - Personal Data." GSMA. GSMA Intelligence, 22 Feb. 2016. Web. 15 June 2016. <http://www.gsma.com/personaldata/gsmas-mobile-connect-available-to-2-billion-consumers-globally>.

[32] Austenaa, Marie. "The Mobile Connect Opportunity". 2016. Presentation. <http://www.gsma.com/personaldata/wp-content/uploads/2016/02/MWCB16-The-Mobile-Connect-Opportunity-Marie-Austenaa-1.pdf>.

[33] "LinkedUp." The Economist. The Economist Newspaper, 18 June 2016. Web. 16 June 2016. <http://www.economist.com/news/business-and-finance/21700605-it-one-most-expensive-tech-deals-history-it-may-not-be-smartest-making-sense>.

[34] GSMA. "Mobile Connect Is Enabling Digital Identity for Public Sector Services - Personal Data." Personal Data. GSMA Intelligence, 25 Feb. 2016. Web. 16 June 2016. <http://www.gsma.com/personaldata/mobile-connect-is-enabling-digital-identity-for-public-sector-services>.

[35] Fontana, John. "Pair Aims to Heal Blockchain Ills with New Model, Identity Breakthroughs | ZDNet." ZDNet. N.p., 6 June 2016. Web. 16 June 2016. <http://www.zdnet.com/article/pair-aims-to-heal-ills-of-blockchain-with-new-model-that-supports-id-breakthroughs/>.

[36] Clark, Bryan. "Watch Hackers Hijack WhatsApp and Telegram Accounts Using Known Telecom Flaw." The Next Web. N.p., 01 June 2016. Web. 17 June 2016. <http://thenextweb.com/insider/2016/06/01/watch-hackers-hijack-whatsapp-telegram-accounts-using-known-telecom-flaw/>.

[37] "Access Management & Identity Management." Verizon Enterprise Solutions. N.p., n.d. Web. 17 June 2016. <http://www.verizonenterprise.com/products/security/identity-access/>.

[38] Agrawal, Rajat. "Why India Rejected Facebook's Free Basics." Mashable. N.p., 09 Feb. 2016. Web. 18 June 2016. <http://mashable.com/2016/02/09/why-facebook-free-basics-failed-india/#2OjkJeGHquq3>.

[39] Gulley, Kevin. "WebRTC Market 2015 - Statistics and Data. #Infographic." The UC Buyer. N.p., 4 Aug. 2015. Web. 18 June 2016. <http://www.theucbuyer.com/blog/webrtc-market-2015-statistics-and-data.-infographic>.

[40] FT. "Fast FT." Fast FT. N.p., 5 Nov. 2015. Web. 20 June 2016. <http://www.ft.com/fastft/2015/11/05/post-420521/>.

[41] The White House. "NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE." (n.d.): n. pag. Whitehouse.gov. Apr. 2011. Web. 20 June 2016. <https://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf>.

[42] "The Bank of England's RSCoin: An Experiment for Central Banks or a Bitcoin Alternative?" Bitcoin Magazine. N.p., 28 Mar. 2016. Web. 20 June 2016. <https://bitcoinmagazine.com/articles/the-bank-of-england-s-rscoin-an-experiment-for-central-banks-or-a-bitcoin-alternative-1459183955>.

[43] "Digital Single Market - European Commission." Digital Single Market. N.p., n.d. Web. 20 June 2016. <https://ec.europa.eu/digital-single-market/en>.

[44] "Gartner Says 6.4 Billion Connected." "Things" Will Be in Use in 2016, Up 30 Percent From 2015. N.p., n.d. Web. 20 June 2016. <http://www.gartner.com/newsroom/id/3165317>.

[45] Ullens, Rod. "The Future of Phone Numbers." Interview by InterComms. InterComms. N.p., n.d. Web. 27 June 2016. <http://www.intercomms.net/issue-16/pdfs/articles/voxbone.pdf>.

[46] Tom McGarry, "The Future of the Phone Number, Number Portability, and IETF MODERN." Telephone interview. 19 Apr. 2016.

[47] Marcus, David. "Here's to 2016 with Messenger | Facebook Newsroom." Facebook Newsroom. N.p., 7 Jan. 2016. Web. 27 June 2016. <http://newsroom.fb.com/news/2016/01/heres-to-2016-with-messenger/>.

[48] Sacha Nacar. LinkedIn Post. <www.linkedin.com/hp/update/6145548188058210304>.

[49] WhatsApp. "WhatsApp Calling: 100 Million Conversations Every Day." WhatsApp Blog. N.p., 23 June 2016. Web. 27 June 2016. <https://blog.whatsapp.com/10000625/WhatsApp-Calling-100-million-conversations-every-day>.

[50] Nacar, Sacha. "OTT Messaging Apps Chew Away at SMS." NoJitter. N.p., 26 Feb. 2016. Web. 27 June 2016. <http://www.nojitter.com/post/240171416/ott-messaging-apps-chew-away-at-sms>.

[51] Fingas, Jon. "Facebook Messenger's SMS Push Might Break Android App Rules (updated)." Engadget. N.p., 20 June 2016. Web. 27 June 2016. <https://www.engadget.com/2016/06/20/facebook-messenger-sms-push-might-break-android-rules/>.

[52] O'Donnell, Bob. "Be Prepared: We're Entering A Post-Device Era." Fast Company. N.p., 21 June 2016. Web. 27 June 2016. <http://www.fastcompany.com/3061084/were-way-past-steve-jobs-post-pc-era-and-headed-for-a-post-device-future>.

[53] Russell, Jon. "Google Launches Springboard, an AI-powered Assistant for Its Enterprise Customers." TechCrunch. N.p., 14 June 2016. Web. 27 June 2016. <https://techcrunch.com/2016/06/14/google-launches-springboard-an-ai-powered-assistant-for-its-enterprise-customers/?ncid=rss&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A%2BT

[54] Swider, Matt. "IOS 10 Release Date, News and Features." TechRadar. N.p., 20 June 2016. Web. 27 June 2016. <http://www.techradar.com/news/software/operating-systems/ios-10-release-date-news-beta-and-rumors-1311275>.

[55] Greenberg, Andy. "So Hey You Should Stop Using Texts for Two-Factor Authentication." Wired.com. Conde Nast Digital, 26 June 2016. Web. 28 June 2016. <https://www.wired.com/2016/06/hey-stop-using-texts-two-factor-authentication/>.

[56] OECD. At a Crossroads: Personhood and Digital Identity in the Information Society. Rep. no. DSTI/DOC(2007)7. DOC2007 ed. Vol. DSTI. Paris: OECD, 2007. Ser. 7. OECD, 29 Feb. 2008. Web. 28 June 2016. <https://www.google.be/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&cad=rja&uact=8&ved=0

[57] Barr, Lantre. "Apple Jumps On the WebRTC Bandwagon." NoJitter. N.p., 13 Apr. 2016. Web. 29 June 2016. <http://www.nojitter.com/post/240171589/apple-jumps-on-the-webrtc-bandwagon>.

[58] Urban, Tim. "The Artificial Intelligence Revolution: Part 1 - Wait But Why." Wait But Why. N.p., 22 Jan. 2015. Web. 30 June 2016. <http://waitbutwhy.com/2015/01/artificial-intelligence-revolution-1.html>.

[59] "UK Public General Acts." Legislation.gov.uk. N.p., n.d. Web. 01 July 2016. <http://www.legislation.gov.uk/ukpga#sch1>.

[60] Dahan, Mariana. "ID4D Program Coordinator The World Bank". 2016. Presentation. <http://www.gsma.com/personaldata/wp-content/uploads/2016/02/MWCB16-The-World-Bank-Mariana-Dahan.pdf>

[61] BBC. "Yahoo Sold to US Telecoms Giant Verizon." BBC News. N.p., 25 July 2016. Web. 27 July 2016. <http://www.bbc.com/news/business-36879831>

[62] Coldewey, Devin. "NIST Declares the Age of SMS-based 2-factor Authentication Is over." TechCrunch. N.p., 25 July 2016. Web. 27 July 2016.

<https://techcrunch.com/2016/07/25/nist-declares-the-age-of-sms-based-2-factor-authentication-over/>.