INTELLIGENT CONNECTIVITY AND THE NEED FOR A NEW DATA DEAL

— Ensuring data privacy and 'good' digital identity are key to reaping the full benefits of intelligent connectivity. Getting there will require new technology and a new social contract.

By Jennifer L. Schenker

At Mobile World Congress, an annual industry conference taking place in Barcelona Feb. 25-28, a new handset will be unveiled that promises to give its users control over their personal data. Taiwan's HTC, a manufacturer of both Windows and Android-based' smart phones, will announce that it is teaming with several startups and Opera, a European browser company with 320 million users worldwide, to make an entirely different kind of handset, one that separates personal data from the phone's operating system, encrypts it, gives the phone's user total control over their own data, and eventually will allow them to use blockchain and cryptocurrency to slice and dice their data, choose who they want to release it to, and give them the ability to be compensated via micro cryptocurrency transactions. The phone, aptly named EXODUS, promises freedom from snooping and what some see as exploitation.

"We are giving away our data and digital identity for likes and cheap endorphins, surrendering all of our power to the big data monolithic tech giants that mine that data for artificial intelligence agents, advertising revenue and even more nefarious means," says veteran venture capitalist Phil Chen, HTC's Chief Decentralized Officer. "EXODUS is about the future of data and getting the right architecture for the Internet, one that includes security, privacy and transfer of ownership of data back to the person generating it," he says. "This is a great opportunity for enterprise, entrepreneurs and anyone who isn't one of the big seven Internet companies."

The launch of EXODUS is just one example of efforts underway as part of Internet 3.0, the next iteration of the Web, to wrest power over personal data away from Internet giants. Sir Tim Berners-Lee, the inventor of the World Wide Web, announced last September that he is building on current web standards by extending them to provide a distributed data service that would permit individuals and organizations to keep their data in Personal Online Data stores known as PODS.

Another initiative, led by MIT professor and serial entrepreneur Alexander "Sandy" Pentland, a co-founder of MIT's Media Lab and one of the world's most cited computer scientists, seeks to use an open source AI algorithm to give individuals collective bargaining power and control over their own data with the help of credit unions and trade unions, which together represent hundreds of millions of workers.

"We need a new deal on data," says Pentland, who has spent the last 12 years working on ways to ethically extract insights from data without endangering privacy or security through an initiative called The MIT Trust Consortium. The current business model of the Internet relies primarily on users – willingly or unwittingly - giving over their personal data in exchange for free services. Every digital move is tracked and traded. A simple app can - without a user's knowledge – download photos, record a user's voice and transfer personal data such as phone numbers, emails and texts to build a profile. That profile can, in turn be used as a tool to control populations by authoritarian states and/or for what Harvard emeritus professor Shoshanna Zuboff calls surveillance capitalism, a term defined as "a new economic order which claims human experience as free raw material for extraction, prediction and sales."

"Although some of these data are applied to service improvement, the rest are declared as a proprietary behavioral surplus, fed into advanced manufacturing processes known as 'machine intelligence,' and fabricated into prediction products that anticipate what you will do now, soon, and later," Zuboff writes in her new book The Age of Surveillance Capitalism: The Fight For a Human Future At The New Frontier of Power. "Finally, these prediction products are traded in a new kind of marketplace that I call behavioral futures markets. Surveillance capitalists have grown immensely wealthy from these trading operations, for many companies are willing to lay bets on our future behavior." Things have gotten so out of whack that due to a lack of coherent policies and government oversight Internet giants have – until recently - been allowed to hoover up data with few if any constraints while academics and health researchers have been refused access to data that could help society, such as curbing the outbreak of a disease like Ebola, out of fear the information could be misused.

A backlash - fueled by a series of scandals last year that raised questions about how Facebook collects and handles personal information – is starting to change this. In the United States, the Federal Trade Commission is investigating whether Facebook's data-sharing practices violated a 2011 consent agreement prohibiting it from deceiving users on privacy. Laws like Europe's new General Data Protection Regulation (GDPR) that sets stringent privacy standards for any company with business in the European Union are curbing what companies can do with data. And business leaders are starting to call for privacy to be considered a human right. But some industry experts say investigations, new rules – or attempts to break up

●●●

Internet companies – are not enough to shift the balance of power in a world in which Internet companies make moves without first asking for permission, can afford to pay huge fines, and put forward arguments that some regard as disingenuous. Facebook, for example, announced in February that it is going to combine data from its social network with WhatsApp and Instagram, a move opposed by the German competition authority on the grounds that combining these sources substantially contributes to the social networking giant's ability to build a unique database for each individual user and thus gain even more market power.

Facebook disagreed in a blog post, arguing that it needs to collect all of that user data in order, among other things, to ensure "public safety."

Pentland disputes that claim. The open source algorithm developed by MIT's Data Trust Consortium has developed a system that proves it is possible to ethically extract information for the public good from data without moving or owning the data, he says. And that same system could be used to upset the current balance of power.

Hardwiring Security And Privacy Into The Technology

When the global economy was first transformed by industrialization and then by consumer banking, powerful players emerged that concentrated power in the hands of a few. Citizens joined together to form trade unions and cooperative banking institutions, which were federally chartered to represent their members' interests. The same collective organizations could be used to shift the balance of power away from giant Internet players and place it in the hands of workers, says Pentland.

In the U.S. alone almost 100 million people are members of credit unions, not-for-profit institutions owned by their members and already chartered to securely manage their members' digital data and provide a wide variety of financial transactions, including insurance, investments and benefits.

"The question then is, could we apply the same push for citizen power to the area of data rights in the ever-growing digital economy," asks a white paper authored by MIT Connection Science professors and signed by a global trade union and the MIT Federal Credit Union.

Advanced computing technologies make it possible to automatically record and organize all the data that workers knowingly or unknowingly give to companies and the government and to store these data in credit union vaults. The MIT Trust Data Consortium has already built and demonstrated pilot versions of such systems. And, almost all credit unions already manage their accounts through regional associations that use common software, so widespread deployment of data cooperative capabilities could - at least theoretically - be both quick and easy, says Pentland. "By leveraging cooperative worker and citizen organizations that are already chartered in law virtually everywhere in the world, along with technology that has already been demonstrated, we can…change this situation and create a sustainable digital economy that serves the many and not just the few," says the white paper.

If credit unions and trade unions managed their members' data it would give individuals control over their own data and the power of collective bargaining, says Pentland. "It would also benefit traditional enterprises by giving them data that today are only available to large Internet giants."

That said, it would be counter-productive to realizing a more enlightened data-governance ecosystem to "encourage unions to simply surveil their members as Big Tech does, which will of course be a temptation," says Jonnie Penn, an affiliate of the Berman Klein Center at Harvard University who is collaborating with the MIT Trust Data Consortium on the project.

"In collaboration with trade unions and my colleagues Mary Gray and Nathan Freitas at the Berkman Klein Center at Harvard, I've recently co-developed an actionable 'lightweight' data-collection approach built around consent and data-minimization rather than the current 'collect-all' approach."

While it is early days for the program – coding is set to begin in about six weeks – Penn envisions ways trade unions could not only control data collection but use it to improve working conditions. "We want to create an alternative paradigm in terms of data governance," he says. "It has to be the workers themselves that lead." Relatively simple changes in how data are collected and processed, such as having credit unions also manage members' data, and moving from an economy of data sharing to one where questions are shared but data stays under user control, could go a long way toward fixing the current situation, says Pentland.

"Estonia did this switch two decades ago in order to survive a cyber attack by Russia, so why not us? If not now, when?"

During the World Economic Forum's annual meeting Forum executives met with Berners-Lee, the creator of the World Wide Web, to discuss his technology approach to data privacy - Personal Online Data stores known as PODS that are designed to be secure, and allow the owner, whether an individual or company, to provide access to portions of their data, as well as revoke access as needed. "People want apps that help them do what they want and need to do - without spying on them," Berners-Lee said in a blog post announcing the launch. "Apps that don't have an ulterior motive of distracting them with propositions to buy this or that. People will pay for this kind of quality and assurance."

HTC's Chen says he believes blockchain is the technology that is the best suited to underpin the transition to a more distributed Internet architecture that protects data and ensures privacy. Opera, which bills itself as the first the world's first crypto-ready browser, is the first to officially use HTC's key management application programing interface (API). This means that users of the first EXODUS handset can interact, transact and log-in with websites and Web 3.0 services on the browser using their private keys, which are held in HTC's Zion wallet, a kind of private vault on the blockchain, without fear of being tracked.

HTC's new EXODUS handset aims to challenge the big data business models of tech titans. It bills itself as the first Web 3.0 mobile phone.

So what happens if the owner of an EXODUS handset loses their phone? HTC does not maintain copies of keys. Each user's keys are dispersed among five friends of their choosing. Reassembling the keys requires information from at least three of them. The advantage of using cryptocurrency is that it will be easy to make and receive micropayments, enabling users not just to protect and secure their own data, but also monetize it if they wish to do so. HTC says EXODUS has received the support and validation of the crypto community and leaders within it, including Vitalik Buterin, the co-founder of Ethereum, a decentralized software platform that enables smart contracts and distributed applications.

The Need For A New Social Contract

But technology alone is not enough. Building trust in data privacy and security along with "good digital IDs" will require a new social contract, argue some. "Digitalization is transforming and disrupting every area of our lives so institutions and frameworks and ways of thinking are now being re-evaluated and questioned," says Derek O'Halloran, the Forum's Head, Future of Digital Economy and Society, and Member of The Executive Committee. "Policies coming out of one industry or one government department are not enough….we need to establish high level goals and frameworks, and learn from real life examples."

The Forum is trying to do just that, through a number of initiatives involving data privacy and digital identity. Both topics were on the agenda at the annual meeting in Davos in January. Government officials such as Japanese

Prime Minister Shinzo Abe called for a new system for the oversight of data use, as did business leaders. During the annual meeting in Davos the GSMA, the industry association that represents the world's mobile operators, launched a 'Digital Declaration' that is meant to serve as a guide to acting ethically in the digital era. It has so far been signed by CEOs representing 40 companies. The Digital Declaration principles call on businesses to respect the privacy of digital citizens; handle personal data securely and transparently; take meaningful steps to mitigate cyber threats; and ensure everyone can participate in the digital economy as it develops while combatting online harassment.

"Trust is the new collateral," says GSMA Director General Mats Granryd, a board member of the World Economic Forum's stewardship initiative on Digital Economy and Society (See the interview on page 14.) Without consumer trust and ethical guidelines a wealth of new services that take advantage of intellectual connectivity are likely to be delayed or never rolled out. For example, one service being envisioned - with participants' buy-in, could serve as an early warning system for health issues by running diagnostic tests on discarded tooth brushes, dirty diapers or used kitty litter (see the story on page 20) but the information could potentially be misused if it got in the wrong hands and will not be launched unless the right framework can be put in place.

"If credit unions and trade unions managed their members' data it would give individuals control over their own data and the power of collective bargaining. It would also benefit traditional enterprises by giving them data that today are only available to large Internet giants."

MIT professor and serial entrepreneur **Alexander "Sandy" Pentland**, a co-founder of MIT's Media Lab and one of the world's most cited computer scientists

"People want apps that help them do what they want and need to do — without spying on them. Apps that don't have an ulterior motive of distracting them with propositions to buy this or that. People will pay for this kind of quality and assurance."

Sir Tim Berners-Lee, inventor of the World Wide Web, a member of the Stewardship Board for the World Economic Forum's System Initiative on (the Future of) Digital Economy and Society and co-founder of Inrupt

"EXODUS is about the future of data and getting the right architecture for the Internet, one that includes security, privacy and transfer of ownership of data back to the person generating it. It is a great opportunity for enterprise, entrepreneurs and anyone who isn't one of the big seven Internet companies."

Veteran venture capitalist **Phil Chen**, HTC's Chief Decentralized Officer

Data For Good

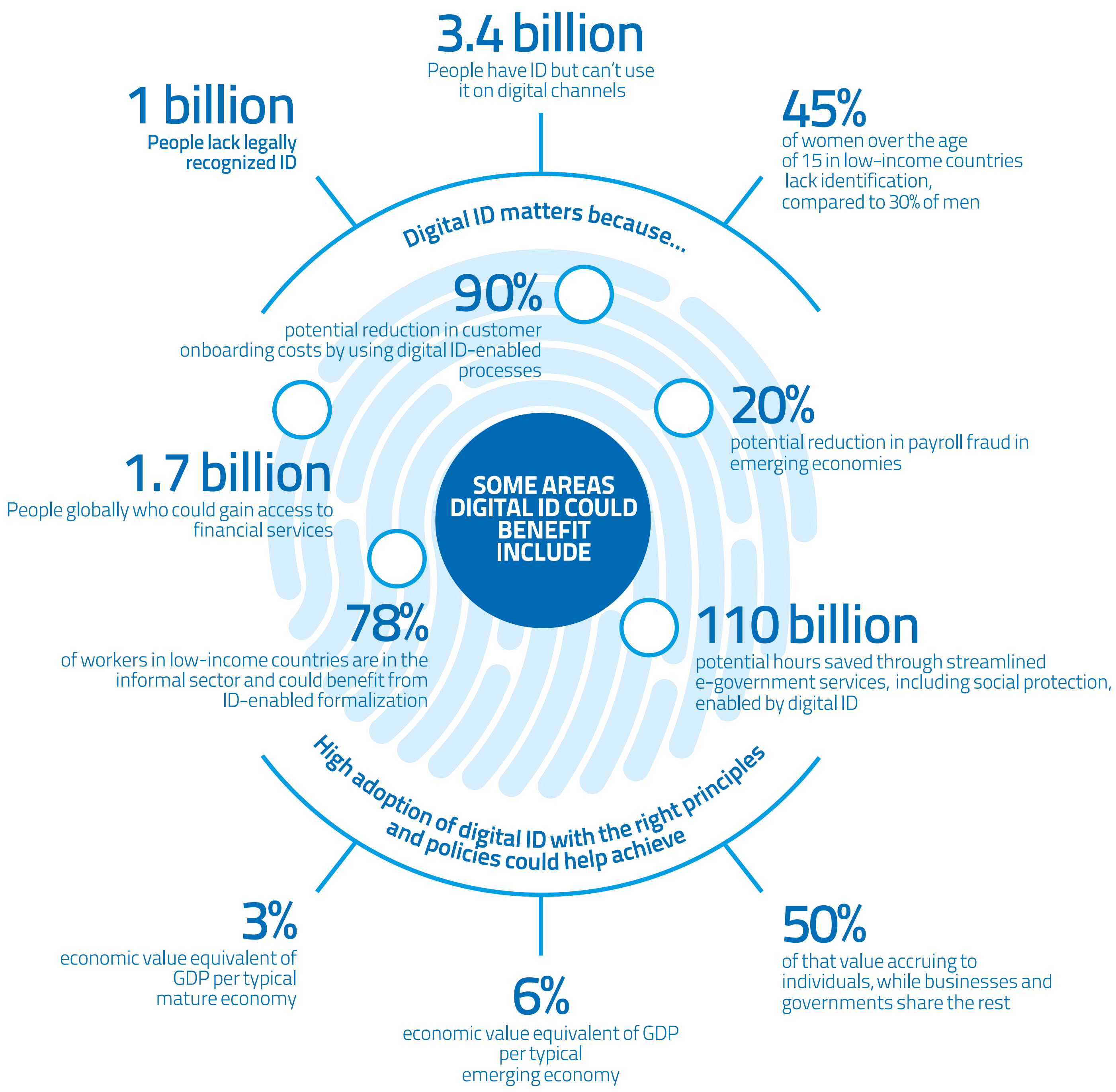
The new social contract also has to take into account the needs of researchers working for the public good. With mobile phone penetration rates reaching 90% - and under-resourced national statistical agencies - the data generated by our phones, including traditional Call Detail Records (CDR) but also high-frequency x-Detail Records, have the potential to become a primary data source to tackle crucial humanitarian questions in low- and middle-income countries, says a recent paper in Scientific Data co-authored by MIT's Pentland. For instance, such data has already been used to monitor population displacement after disasters, to provide real-time traffic information, and to improve understanding of the dynamics of infectious diseases. At the same time our digital breadcrumbs contain intimate details of our lives: rich information about our whereabouts, social life, preferences and potentially even finances.

Historically and legally, the balance between the societal value of statistical data in aggregate and the protection of privacy of individuals has been achieved through data anonymization. The trouble is that recent studies show that pseudo-anonymization and standard de-identification are not sufficient to prevent users from being re-identified in mobile phone data. Four data points — approximate places and times where an individual was present — are enough to uniquely re-identify people 95% of the time in a mobile phone dataset of 1.5 million people.

The limits of the historical de-identification framework to adequately balance risks and benefits in the use of mobile phone data are a major hindrance to their use by researchers, development practitioners, humanitarian workers and companies. "This became particularly clear at the height of the Ebola crisis, when qualified researchers (including some of us) were prevented from accessing relevant mobile phone data on time despite efforts by mobile phone operators, the GSMA, and UN agencies, with privacy being cited as one of the main concerns," says the white paper. Governing Mobile Phone Data. Another problem is the lack of an agreed upon policy framework for the privacy-conscientious use of mobile phone data by third parties. Such frameworks have been developed for the anonymous use of other sensitive information such as census, household survey and tax data, making it possible to use data in aggregate for the benefit of society. Such thinking and an agreed upon set of models has been missing so far for mobile phone data. "This has left data protection authorities, mobile phone operators, and data users with little guidance on technically sound yet reasonable models for the privacy-conscientious use of mobile phone data," says the white paper. In their paper, Pentland and the other authors propose four models for privacy-conscientious use of mobile phone data for the public good in areas such as disaster management. Cases in which individual-level identifiable information is needed, such as targeted advertising or loans based on behavioral data, are excluded. One of the recommended approaches is a system in which the data stays within the premises of the operator and third parties only access it through a question-and-answer system. The questions are validated in advance by a board of advisors. Such a system has been devised, using an open-source algorithm, by the MIT Data Trust Consortium and is already being piloted in Senegal

THE BENEFITS OF GOOD DIGITAL ID, A KEY COMPONENT TO INTELLIGENT CONNECTIVITY

The World Economic Forum defines good digital ID as unique, high-assurance, consent-based, digitally verifiable identification that can be based on a variety of possible credentials such as biometrics, passwords and smart devices



Digital ID matters because...

1 billion People lack legally recognized ID

3.4 billion People have ID but can't use it on digital channels

45% of women over the age of 15 in low-income countries lack identification, compared to 30% of men

SOME AREAS DIGITAL ID COULD BENEFIT INCLUDE

90% potential reduction in customer onboarding costs by using digital ID-enabled processes

20% potential reduction in payroll fraud in emerging economies

1.7 billion People globally who could gain access to financial services

78% of workers in low-income countries are in the informal sector and could benefit from ID-enabled formalization

110 billion potential hours saved through streamlined e-government services, including social protection, enabled by digital ID

High adoption of digital ID with the right principles and policies could help achieve

3% economic value equivalent of GDP per typical mature economy

6% economic value equivalent of GDP per typical emerging economy

50% of that value accruing to individuals, while businesses and governments share the rest

Sources : World Bank ID4D; World Bank ID4D-Findex; We are Social; International Labour Organization ; McKinsey Global Institute analysis

●●●

and Colombia as part of a program called OPAL (see the story on page 24) which seeks to use anonymized data to save lives during periods of crisis, and improve education and city services. It is also being applied in another project in Colombia that uses data to establish fairer distribution of government cash transfer payments to the poor (See the story on page 31.)

Digital Identity: A Key Building Block

Digital identity services – which promise to unlock enormous economic and social value – are a key building block for intelligent connectivity because they are increasingly pivotal in a wide range of interactions among individuals, enterprises and governments. What the Forum calls good digital ID – unique, high-assurance, consent-based digitally verifiable identification – could help the approximately 1 billion people who have no legally recognized ID, preventing them from being able to vote, go to school or receive government services. And it could unlock economic value equivalent to up to 6% in emerging economies and 3% in more mature economies, according to a new report compiled by the Forum and McKinsey. The benefits for businesses and government of adopting digital identification include: an up to 90% cost saving in onboarding customers; a reduction in fraud; an increase in sales of goods and services; streamlining employee verification; and making contracting with contract workers easier, according to the report.The United Nations has set a goal of ensuring that the entire global population has digital IDs by 2030. Examples of digital ID systems already in place can be found in Argentina, Canada, Estonia, India, Sweden and the U.K. The issue is that digital ID systems today vary in terms of their policies and practices – from technology choices to levels of security and privacy – and often do not communicate with each other, making it cumbersome for users and leaving them vulnerable to risks. Shared understanding and collaboration between governments, businesses and civil society can address some of these challenges and advance appropriate innovations and policies, says Manju George, the Forum's Head of Platform Services, Digital Economy and Society.

To that end the Forum has launched a shared Platform for Good Digital Identity to bring together existing and new digital identity solutions. The Omidyar Network committed a three-year grant to support the platform. "Good digital identity is the foundation for innovation and value creation across digital services," says George. "Our shared challenge is to build frameworks that encourage adoption and realize the value while ensuring trust is not eroded."

Time For An EXODUS

HTC's Chen, who previously worked as a venture capitalist for Horizon Ventures, says the monopoly that the world's seven biggest Internet companies have on data is not just undermining trust, it is curbing innovation. HTC's new handset will, for example, enable its users to direct micropayments to content websites, which has the potential to "reshape the face of journalism and create a new, content-centered revenue stream away from the hands of controlling tech giants and click-chasing advertising models," says the company. There is an opportunity for startups, academics, developers and big traditional companies to re-architect the Internet and create a variety of new services that could benefit consumers and society as whole, says Chen. It is why, he says, it is high time – in more ways than one – for an EXODUS. ●

J.L.S.

STARTUPS WORKING WITH EXODUS

BITMARK
CAYMAN ISLANDS

WHAT IT DOES: Its technology establishes ownership and property rights over digital assets of value such as health data, art, digital collectibles, song rights, and medical records and makes them divisible. Backers include Alibaba.
https:/bitmark.com

NUMBERS PROTOCOL
HONG KONG

WHAT IT DOES: With user consent identifies all the sensors on your phone tracking things like walking, sleeping and driving to package the data for third parties. Allows data owners to sell or trade data, repackage it and sell or trade it again. In stealth mode.
http://numbersprotocol.io