DIGITAL IDENTITY:
RISKS, CONTROL AND MONITORING IN THE ONLINE WORLD

"The use, misuse and abuse of data and technology is undermining the fundamental democratic process."

This report is based on a GTF panel discussion hosted in the House of Lords on July 2, 2018.

Digital Identity

A digital identity is the online version of an individual. It consists of all their personal data that is available online; from emails, physical address, pictures, banking information, shopping preferences, travel and so on. A digital identity can be very valuable. It enables governments, financial services, health services and many more to provide streamlined processes through digitized services, for example. But there are two sides to every coin. As we share different information on different platforms with different organisations, pinpointing a management system to safeguard digital identities is very challenging – but not impossible. This is still an embryonic field; potential for improvement abounds.

> *"Technology represents the 'plumbing' of how we interact. It is up to us – governments, businesses, media and the public – to create a safe and ethical digital ecosystem that leverages that plumbing. Equally, over-regulation could trigger knee-jerk reactions that strangle momentum for digital innovations. Fear of digital identity fraud cannot force the world into the digital dark ages. It is a very fine balance – one we each play a role in mastering."*

Sharing Safely in the 21st Century?

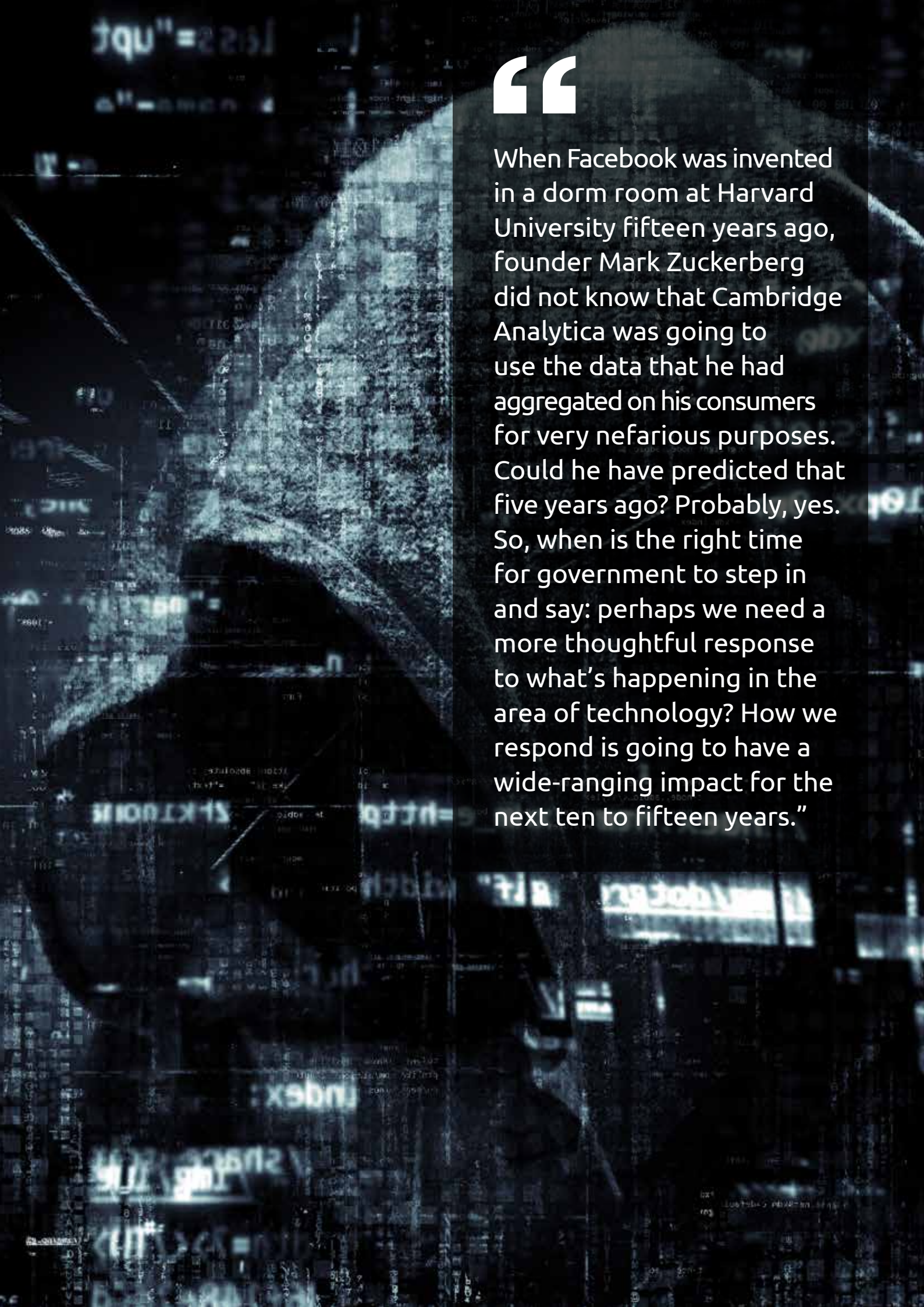
Just like the man who inked his handprint 37,000 years ago on a cave wall in France, our need to have a tangible identity, to communicate and to leave a mark is threaded into our humanity today. "In the social jungle of human existence, there is no feeling of being alive without a sense of identity," said Erik Erikson, an influential psychoanalyst. Now, the advent of the 4th Industrial Revolution means the way we publicly share our identify is heading into unchartered territory.
How best to spur digital innovation while protecting human rights?

On July the 2nd 2018, Global Thinkers Forum convened a panel of international experts in the House of Lords in London, to discuss the issue of digital identity and share concerns as well as recommendations to policy makers.
The conversation was under the Chatham House rules. The equivalent of that handprint is now a digital identity, which can be shared instantaneously with billions of people and will never 'rub off'; it is almost impossible to erase. Our natural instinct to share information about ourselves has a new set of ramifications; many beneficial, some less so *(see 'Real Risk' – p2).*

Our ambitions, opinions, hopes, fears and socioeconomic status are just the tip of a list of deeply personal information that is directly or indirectly communicated in the digital sphere. We share this information via the taps or clicks we make on our mobiles, iPad, computers or by giving details to organisations with digital access, such as banks, hospitals, airports and many more. Our digital identify is edited and added to every day, so our personal details have an increasingly public face.

How much is 'too much'?

Ethical lines cannot be crossed in this new era of sociotechnical divulgence. The basic human right to privacy must be protected. Data is a personal asset and users should have a say in how it is collected, used and shared. The persuasiveness of digital tools encourage us to reveal. Attractive marketing and excessively long terms and conditions in minute type are just two of the tactics that play on the public's desire to quickly be connected on a 24/7 basis. But how much is too much?



“When Facebook was invented in a dorm room at Harvard University fifteen years ago, founder Mark Zuckerberg did not know that Cambridge Analytica was going to use the data that he had aggregated on his consumers for very nefarious purposes. Could he have predicted that five years ago? Probably, yes. So, when is the right time for government to step in and say: perhaps we need a more thoughtful response to what’s happening in the area of technology? How we respond is going to have a wide-ranging impact for the next ten to fifteen years.”

How would you choose to balance your information between strict privacy and casual sharing i.e. a 50/50 split? How do you determine that split? And how can you be sure that your information is safeguarded and not corrupted? In short: is your digital identity always safe? The answer is no. This black hole of mistrust needs fixing.

Stagnant mistrust was the main reveal in the global Edelman Trust Barometer 2018. Trust in business, government, non-governmental organisations (NGOs) and media remained largely unchanged from 2017, as 20 of 28 markets and more than 33,000 respondents surveyed fell in distruster territory. Why? Because the risks associated with digital openness have rapidly spread. Stolen passwords, fraudulent transactions, unsanctioned online and geographic tracking, cyberbullying, the creation of false social media accounts and a lack of control over personal information and many more are no longer rare occurrences.

> *"How do we deal with trust in the digital space? We don't have the answer yet."*

In Numbers: Real Risk

£500,000 Half a million-pound fine was issued to Facebook by the UK-based Information Commissioner's Office (ICO) in July for serious breaches of data protection law. Among other failures, Facebook failed to keep personal information secure due to sub-standard checks on apps and developers using its platform.

87m These failings meant the Facebook data of up to 87 million people worldwide was harvested – 30% more people than the UK's entire population – without their knowledge.

16.7m Identity fraud affected 16.7 million victims in the US alone last year, according to the 2018 Identity Fraud Study by Javelin Strategy & Research. This is the highest level recorded since the company started tracking identity fraud in 2003.

x3 Account takeover grew significantly in the US, tripling over the past year to a four-year high. Total losses from account takeovers reached $5.1 billion last year - a 120% increase from 2016.

1bn The number of people today – 13% of the global population – who are still unable to prove their identity. This puts them at risk of digital identity manipulation. Accordingly, the World Bank launched the Mission Billion ID4D (Identification for Development), which supports the bank's other goals of ending extreme poverty by 2030 and promoting shared prosperity.

#1 ID4D is focusing on 'Privacy by design', so digital identities are engineered to both reduce the data protection risks and give those in developing countries greater control over their data. Improving privacy by design elsewhere should also be a top priority, especially in regions where digital fluency has created more detailed digital identities.


“
Human rights have no monetary value attached to them. So, how do we reconcile human rights with business?”

Level playing field

The rapid speed of digital progress cannot gloss over the fundamental building blocks of society; law and ethics. Creating a standardised understanding and safeguard of digital identities worldwide is vital. A fool proof security system that all can understand and abide to should not be an aim, but an imminent certainty. Today, there are very limited ways to raise a red flag of mistrust in a system or service. The primary options are oft-lengthy complaints procedures, 'naming and shaming' via social media, logging the complaint with the police force or the ombudsman. None of these routes are guaranteed to have a long-lasting positive impact or protect other potential victims.

People should be able to tailor their own digital identity. For example, one may be happy to share their travel details, but wants access to their health, financial and location details restricted. This ethos is in line with an 'intent to consent' model. This feeds into the ability to opt-in to sharing information rather than putting the onus on the public to opt-out of systems that they are automatically and often unknowingly added too.

Such guidelines must be very simple to ensure smooth global implementation. It is a tall order that must note the world's different economies, politics, cultural norms and rates of development. Other technologies under the umbrella of the 4th Industrial Revolution can also help strengthen the protection of digital identities, such as blockchain, biometrics and artificial intelligence. The latter two are already widely in use; using a thumbprint to unlock a mobile phone or looking at Google maps to gauge the time of your journey, respectively.

Regaining Control

The ability for powerful actors, whether corporations, authorities, hackers or others, to discover and explore the various different activities undertaken by the same individual is the real problem. Individuals must be able to directly manage the linkages among their various activities and who gets to see those linkages. The only way to be sure that data is not abused, or that the activities of individuals are not linkable against their interests, is to develop and maintain infrastructure that does not force users to associate all of their activities to the same identity. This is either via identifiers (such as taxpayer ID, credit card number, phone number, etc), or through the creation of profiles. Rather, infrastructure should allow individuals to speak, interact and transact on their own terms, with the option to create or withhold links between their different activities or contexts with full knowledge of what is being linked.

The property that is needed is polynymity: the ability of an individual to create and use different identities in different contexts, a form of freedom that we enjoyed in the days before technology facilitated the creation of a single "permanent record", that binds all of an individual's activities to a single, inescapable identity. Polynymity is undermined by the aggressive collection of identifying data, particularly by online services and retail payment networks. It is also undermined by biometrics, which makes it impossible for an individual to disconnect from associations forged in the past. No system can be entrusted with the keys to a record of all of an individual's actions; the individual ultimately must be the master of those connections.

That governments should offer internet access to everyone, as with telephony, seems like a good idea. But it does not address the core problem, which is that people are not in control of the links between their activities. It is cheaper than ever to collect, aggregate and analyse all of the online interactions, geolocation history and financial behaviours of individuals at a fine level of granularity. Knowing an individual so intimately a mere two decades ago would have been impossible.

Leading voices

The speed of digital advancement means legislation will struggle to keep pace. This puts even more emphasis on the need to uphold ethical standards and preserve the human right to privacy while encouraging innovation. The complex nature of this challenge means united efforts with a shared focus is key; one that encompasses governments, businesses, media and the public.

The European Commission has made huge strides to harmonize data privacy laws and address how organisations approach data privacy. The EU General Data Protection Regulation (GDPR) marked the most important change in data privacy regulation in 20 years when it came into force this May, fundamentally reshaping the way data is handled across every sector. But much more is needed on a national and cross-border basis to knit national efforts together and create a global safeguard for digital identities. The internet means our digital identities are not restricted to national borders; governmental solutions should not be either.

Conclusions

Businesses must address their cultural approach to digital identities. A starting point is to ask: are staff protected and are customers' personal details respected? Greater transparency is needed around potentially thorny morale issues, such as data scientists taking instruction from business executives who are working to competitive agendas. Plus, better alignment between policy makers and business would ensure policies detailed on paper are positively realised 'on the ground'. The public also has a deeply powerful voice – one that needs to be louder. The power of the people and regulation within the community can have a meaningful impact. Consumers can speak with their feet i.e. if they don't feel comfortable, then they resist or move on.

The public would also benefit from being more aware of their own digital identities and being more thoughtful of what they share. The media also plays an influential role, especially in education. Politician Edmund Burke coined the phrase 'Fourth Estate' in 1787, which encapsulates a protective and ever-present eye of a free press to preserve the narrative of truth. Amid a rise in fake news and misinformation, this role is more important than ever in raising public awareness and monitoring government and businesses.

Technology represents the 'plumbing' of how we interact. It is up to us – governments, businesses, media and the public – to create a safe and ethical digital ecosystem that leverages that plumbing. Equally, over-regulation could trigger knee-jerk reactions that strangle momentum for digital innovations. Fear of digital identity fraud cannot force the world into the digital dark ages. It is a very fine balance – one we each play a role in mastering.

> *"Personal information can be stolen and misused as laws are not sufficient; they cannot keep pace with technology."*

This panel consisted of public, private sector, academia and civil society representatives. As part of our mission towards informing leaders and policy makers, Global Thinkers Forum organises conversations among decision-makers and international experts in an effort to nurture accountability and values-based decision-making. We are grateful to all parties who participated in this important and timely discussion.

Global Thinkers Forum e: info@globalthinkersforum.org | w: globalthinkersforum.org

Contact us if you would like to discuss how to host a Global Thinkers Forum event.