Trust in Technology

May 2017

HSBC

"There is one thing which, if removed, will destroy the most powerful government, the most successful business, the most thriving economy, the most influential leadership, the greatest friendship, the strongest character, the deepest love... That one thing is trust."

Stephen M. R. Covey, The Speed of Trust

Contents

Foreword

Digital technology is rapidly changing the world. The number of mobile banking users is forecast to double between 2015 and 2019 to 1.8 billion, representing more than one quarter of the world's population. As one of the world's largest banking and financial services organisations, serving more than 37 million customers across 70 markets, we need to anticipate and be ready to respond to that change.

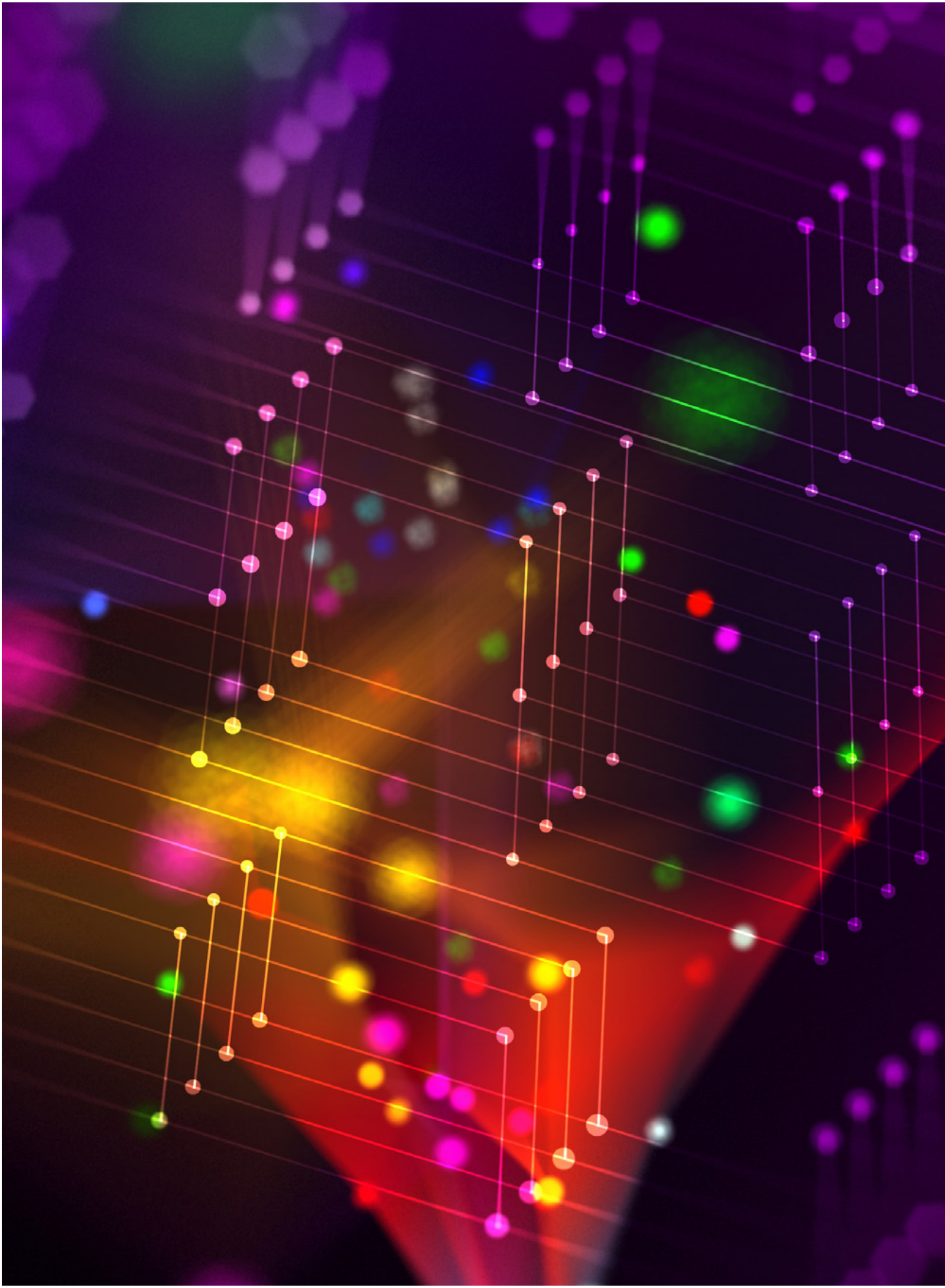
Our Trust in Technology research explores public opinion about the new technology banks and consumer-facing businesses are developing, and its impact on daily lives. In this international study we examine people's awareness and understanding of new technologies – their trust in them and the impact of this on adoption rates; and what people think the future looks like in terms of new innovation.

The report explores some of the top technology topics of the moment, like artificial intelligence, biometrics, digital wallets and data driven nudge applications.

We will apply the insights this research provides to our own business, as well as sharing them broadly with the financial services industry and other stakeholders.

Digital demands vary from customer to customer and market to market, but the long-term direction is clear: customers should be able to bank with us when they want, in the way that they want. At HSBC, we want to apply proven digital technology to make our customers' experiences simpler, better, faster and more secure. We will continue to adapt as their needs change, to provide banking services on their terms.

John Flint
Global CEO, HSBC Retail Banking and Wealth Management



Why we need to study the nature of trust

This is an age where the dreams of science fiction are becoming a reality. The list of new technologies being released is dazzling.

Life expectancy is hitting record highs thanks to ground-breaking new processes. A team at Harvard Medical School has grown heart tissue from adult skin cells. The prospect of transplant organs grown from scratch is on the horizon.

Artificial intelligence is going mainstream. The success of Amazon Echo and Google Home smart speakers show there is an appetite for AI assistance in the home. Autonomous cars are being test driven. Sometime in the next decade it will be normal to be chauffeured by an AI.

Financial services are being re-invented by new technology. Apps make it quick to send money and check accounts. Online consultation services, nicknamed robo-advisors, are bringing expert guidance on investment and pensions to a wider audience. Security is becoming quicker, simpler, and more reliable through fingerprint, voice and iris scanning, a collection of technologies based on unique elements of people's bodies called biometrics. Even the cadence of typing and swiping can be included in the security mix – a tactic known as behavioural analysis.

Naturally, this deluge of new tech is a challenge for users. There are early adopters, keen to experiment with each new product release. And behind them are more cautious users, waiting to see if a new technology deserves their time and money.

The speed of adoption is regulated by a number of factors such as price and availability, and an essential component of trust.

No one buys anything unless they trust it. Advertisers spend a fortune building trust, and designers work hard to foster it. Without trust, a technology can be ingenious and cheap, but will remain on the shelf untouched.

The bedrock of trust is reliability. Will the product do what it says it will?

Security is a key concern. Stories of data leaks and unauthorised data sharing are all too familiar. There can be no trust unless these worries are overcome.

As artificial intelligence takes on more duties, the question gets a little trickier. For example, autonomous vehicles are close to launch, and questions are being asked whether they can be trusted to behave in adverse conditions.

This report is an exploration of the state of trust in technology. The findings are supported by an exclusive survey of over 12,000 consumers across 11 major economies that looks at opinions on trust internationally. It reveals the level of trust in biometric security, the gap in attitude between generations, and what we really feel about entrusting our lives to a robotic intelligence. Qualitative research drills deeper into individual perspectives.

The more technology enters our lives, the more critical the issue of trust becomes. A FinTech startup can't win customers without winning their trust. A bank can't keep customers without being trusted. In order to deliver life enhancing new products they need to know what trust is, and how to win it.

The goal? The philosopher Onora O'Neill put it well: "The aim is to have more trust. Well frankly, I think that's a stupid aim. It's not what I would aim at. I would aim to have more trust in the trustworthy but not in the untrustworthy. In fact, I aim positively to try not to trust the untrustworthy." This report offers some suggestions on how we reach that goal.■

The state of trust in technology today

Technology continues to develop at a rapid pace with faster, simpler and more secure innovations being launched on an almost daily basis. But what is the public appetite for creative new tech? HSBC commissioned a survey across 11 major international markets to understand how people trust in technology to manage their financial affairs and daily lives.

Our research shows a lack of trust and understanding is holding back the adoption of new technologies.

The survey began by establishing a baseline of trust – how optimistic and generous people tend to be in general. The results are positive. By default, there is a high level of social trust. People give each other the benefit of the doubt, with 68% saying they will trust a person until proved otherwise, and 48% believe the majority of people are trustworthy compared to 20% who disagree. The outlook on life is positive, with 65% confirming they are always optimistic about their future, and half saying "things that seem bad normally turn out okay in the end," triple those disagreeing.

This warmth extends to using technology, with 76% saying they feel comfortable using new technology, and 80% saying they believe technology makes their life easier.

Then respondents were asked about fields of emerging technology. The sunny outlook quickly fades.

Artificial intelligence is a booming field, with engines such as IBM Watson and Wipro Holmes able to diagnose cancer, analyse retail data, and communicate through ordinary spoken and written language. However, AI is not yet trusted, instead it struggles to win support. Only 8% would trust a humanoid advisor programmed by experts to offer mortgage advice, compared to 41% trusting a mortgage broker. For context, 9% would be likely to use a horoscope to guide investment choices, and 10% would be likely to be influenced by the flip of a coin.

Robotics is advancing through links to AI. How about allowing a robot to conduct a surgical operation? Only one in seven (14%) would trust a humanoid robot programmed by leading surgeons to conduct open heart surgery on them, just five percentage points

ahead of the rather unnerving prospect of a family member doing the operation supported by a surgeon (9%).

Biometric security is another field with huge potential. It's possible to use fingerprint, voice, iris, and facial patterns to confirm an identity. Security experts regard biometrics as a potential breakthrough in the fight against identity theft.

However, trust is yet to be fully achieved in biometric technologies. Iris recognition is trusted by 26% to replace alphanumeric passwords, a combination of letters, symbols and numbers to confirm their identity and prevent unauthorised access, with voice recognition and facial recognition both trusted by 18%.

Even quite straightforward technology is regarded with scepticism under certain circumstances. For example, skydivers are usually equipped with an automatic failsafe triggered by an altimeter. But when asked what they'd trust to open a parachute on a skydive, 65% opted for "an instructor with me", 53% trusted themselves to pull the rip-cord, and 16% would trust a pre-programmed release mechanism.

Winning and breaking trust

The results reveal a fundamental tenet of trust in technology. Unlike people – who we trust until given cause to think otherwise – trust in technology is earned, not given. Caution is the default.

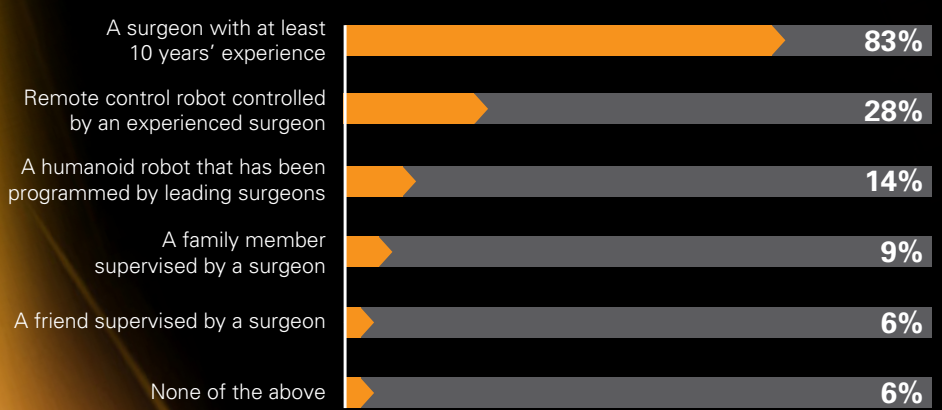
In-depth interviews conducted as part of this study looked deeper at the thinking behind trust. Consumers were interviewed across international markets, and the results were then discussed by a panel of technology experts.

Trust in people produces testimony brimming with emotion and enthusiasm. An interviewee from Hong Kong produced a photograph and said, "My best friends since secondary school. I truly trust everyone of them due to our deep bonds. Though we're in different universities and experiencing different university life, we are also the best listeners to each other and truly consider each other as brothers."

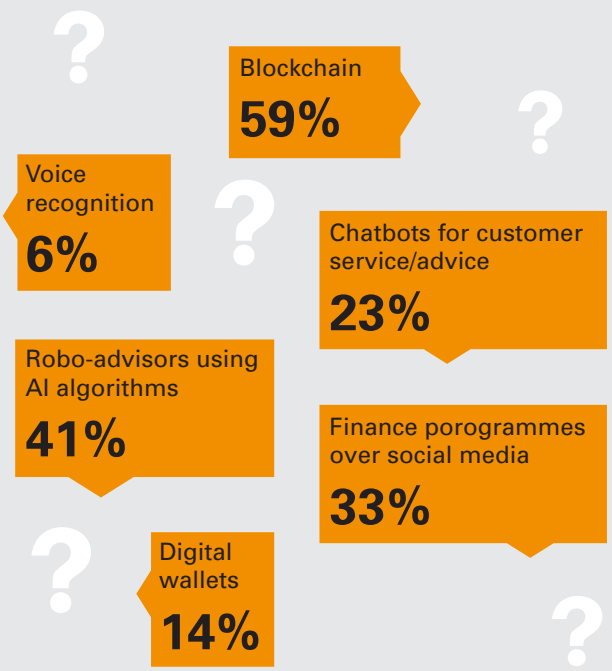
By contrast, trust in machines was expressed as transactional. Performance is what matters. A Chinese interviewee expressed their logic on what to trust: "It [Trust] is being sure that the thing will not fail or disappoint you with its quality, operation and/or handling. Being sure that it will do what you expect it to."

Will Highams, a cultural trends expert, reviewed the qualitative responses, and says, "Technology can build trust on one level. If you create something useful, that is seamless, that does things well and I can rely on it then that is brilliant. But the other form of trust is a human relationship

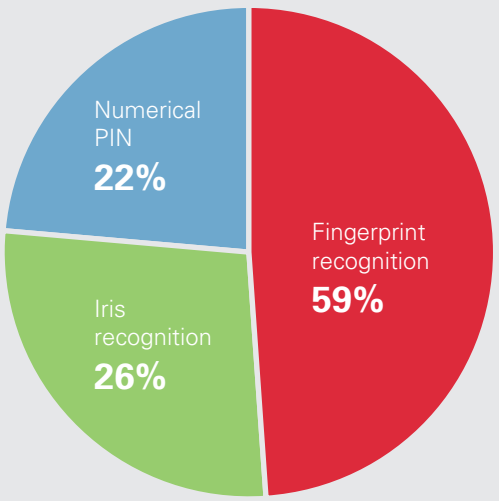
Who would you trust to perform surgery?



I've never heard of this technology



What do you trust to replace passwords?



which is a different form of trust."

The principle that trust in technology is built over time, based on hard evidence, explains the hesitancy around new products and services. Chatbots, AI and biometrics are developing fast, and are yet to prove functional reliability to doubters.

Many consumers are still unaware that emerging technologies even exist.

More familiar concepts generate higher levels of trust. This is highlighted by perceptions of fingerprint technology. Fingerprint identification has more than a century of use by police forces. It is a familiar method of identification. Fingerprint recognition is already used by 21% of respondents to identify themselves internationally, rising to 40% of respondents in China and 31% in India. The status of the technology reflects this familiarity, with 46% overall saying they trust a fingerprint to replace passwords. Financial services companies will need to cater to this demand: 38% said they regard fingerprint login as a very important or essential service for their bank to offer.

Consumers are also familiar with the track record of innovators to bring new concepts to market, hence the widespread expectation for this record to continue. When asked whether artificial intelligence based services were already available or would be available in the next five years, 88% expected to see AI involved in nudging financial behaviour, and 59% expected virtual reality bank consultations. The integration of bank accounts with social media will soon be a common offering, said respondents: 88% expect to see it arrive within five years.

Current attitudes to emerging technologies should therefore be taken with caution. Trust can be won as each technology becomes part of normal life and develops a track record. Businesses can help this process by raising awareness and educating consumers.

On balance, consumers are confident that innovation is moving in the right direction: two-thirds (67%) believe advances in technology will make the world a better place.

The optimism of the East

Attitudes to technology vary from nation to nation, and the survey reveals the key factors. Openness is correlated

Trust in technology is earned, not given. Caution is the default.

Trust can be won as each technology becomes part of normal life and develops a track record. Businesses can help this process by raising awareness and educations consumers.

to social and economic change, with rapidly developing markets in the East far more experimental with innovation than in the leading mature economies of the West.

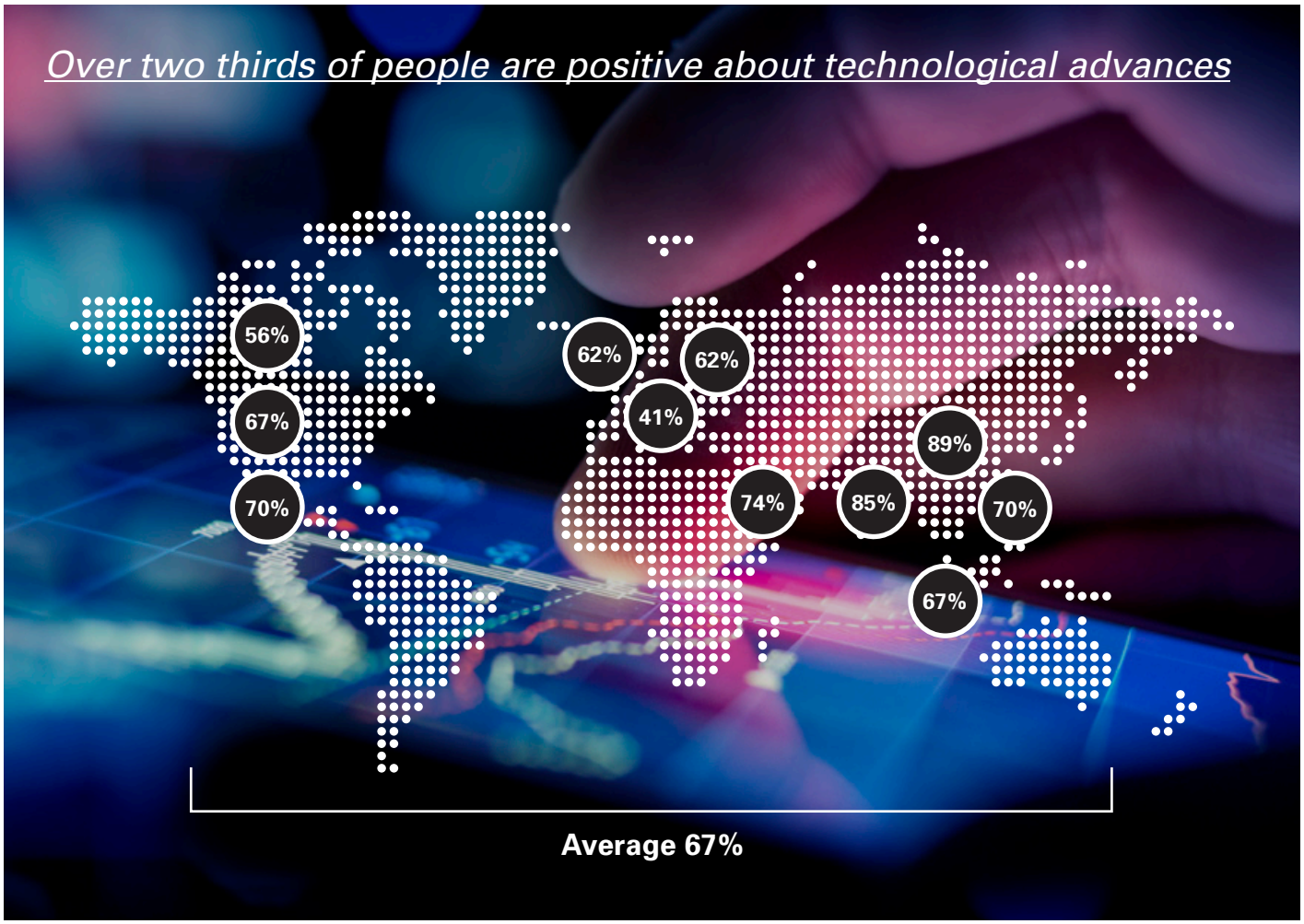
China and India are the most open to new technologies. France and Germany are the most cautious of the 11 nations surveyed. For example, 41% of Chinese and Indian respondents said they were "likely or very likely" to trust a hologram assistant to help them make choices around their money or investments. In France and Germany the figure is 7%.

France stands out as the most reluctant of the 11 nations polled to embrace new technology. In 18th Century France the philosopher Jean-Jacques Rousseau became famous for his view that science and the arts had corrupted mankind. In France today the belief that technology will make the world a better place is held by 41% of respondents, by far the lowest of the 11 nations surveyed. It also has the lowest general sense of trust, with 28 per cent of respondents believing the majority of people are trustworthy, more than half the level in Canada and the UK. The spirit of Rousseau lives on. In China, 89% believe that advances in technology will make the world a better place, the highest, and 70% think the majority of people are trustworthy.

The research sheds light on why trust in Western societies is lower than in the East.

A Canadian interviewee explained their reticence to trust corporations: "It's hard to trust blindly these days, especially with technology and companies. You hear about trust being violated all the time-personal information being compromised, shared, hacked, and breached. Giving trust to companies is a big leap these days."

An interviewee from Mexico explored one of the causes – repeated breaches of trust: "I've had my trust



Who do you trust to keep you safe?

UK

Canada

broken many times when buying products and services that promise something specific, and then when you have them in your hands and operate them, it is all just marketing."

The vocabulary of participants illustrates the mindset in Western countries. There has been an erosion of trust combined with an empowerment in technology. The result is greater self-reliance.

The East is more optimistic. There is greater trust in traditional institutions in nations such as China and Singapore. A Chinese participant said, "Under the leadership of the Chinese government, China's position in the world is rising; our living standards are rising. Therefore I give the Chinese government a high degree of trust."

Chris Gledhill, a FinTech commentator and founder of social-networking app Secco, was one of the expert reviewers of the qualitative research. He says the mood of participants in India and China, expressing eagerness for creative new technologies and a willingness to experiment, matches what we know about the societal trends in those two nations: "In India or China [there are] humongous movements of people from working class to middle class and suddenly people have wealth and are getting educated. Some people are seeing all these things as a ticket or a passport to something new and they're jumping on it, they're grabbing it with both hands and saying, 'We totally want this'."

This sense of adventure is matched by a hunger for new products. In China 61% believe we will use only biometrics to access banking services in the next ten years, compared to 43% in Germany.

Lead researcher Tom Anderson saw the East-West divide again and again in the interviews: "We asked people to imagine the future of personal finance. The most extreme example we had was a woman in India who said she hoped by 2030 if she went into a shop the shop would recognise her through her DNA. If she left the shop she wouldn't have to do a transaction, the shop would

In Western countries there has been an erosion of trust combined with an empowerment in technology. The result is greater self-reliance.

All generations worry about similar events. The three age cohorts are, with margin of error, similarly likely to worry about personal data being leaked, credit card cloning and identity theft. This puts to bed the idea that older people are particularly nervous about technology.

automatically debit her account. We had somebody in the UK says it's 2030 and they have raised the contactless limit to £30!"

Age is a poor predictor of tech adoption

Generational differences were tracked. It is often assumed that younger people will be more tech savvy than older generations. That, it seems, is not quite the whole picture.

The survey compares Millennials (born after 1981), to Generation X, and the generation born in the two decades after 1945, known in America as the Baby Boomers owing to the huge post-WW2 surge in births.

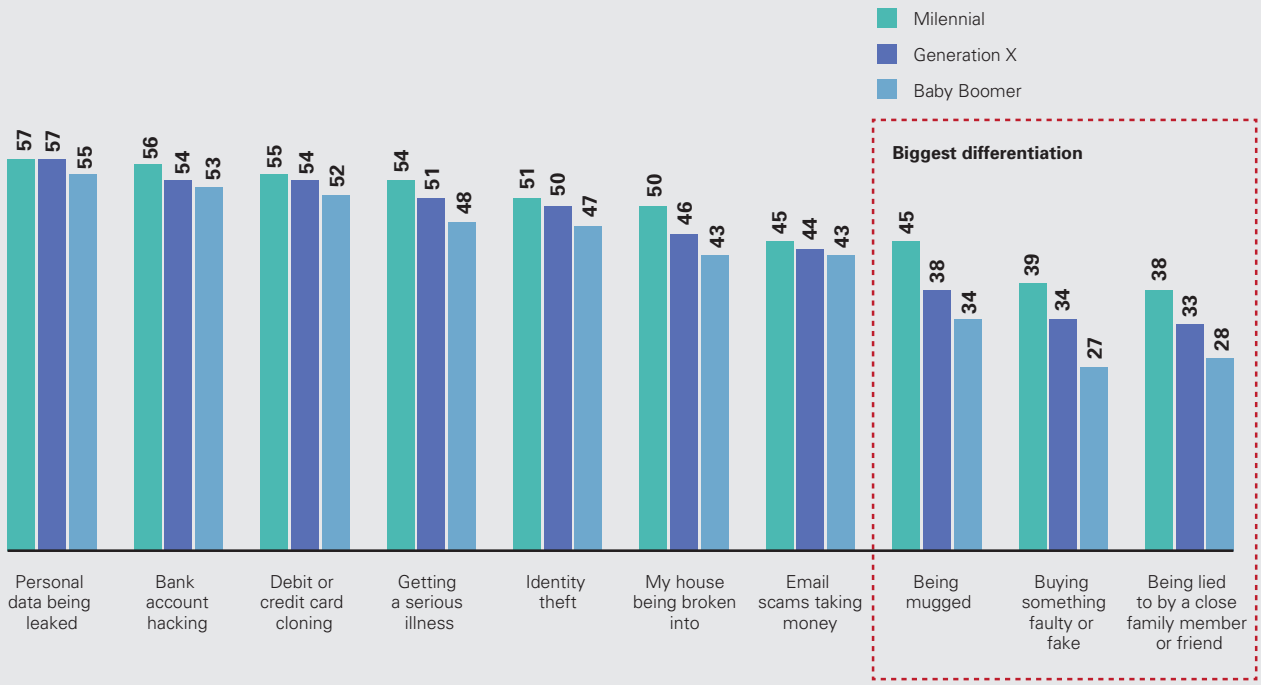
The youngest cohort certainly regards itself as more adept, with 52% saying they are usually "the first to try new things", compared to 39% of Generation X, and 27% of Baby Boomers. The younger generation is more vocal in calling for innovation: 43% believe fingerprint logins are very important or essential as an offering from their bank, compared to 29% of the Baby Boomers. They are twice as likely to want video conferencing with a human advisor (30% vs 17%) and integration with social media (28% vs 13%). And they are better informed – being twice as likely to know about fingerprint logins, and twice as likely to know about voice recognition.

But the reality is different. There is little difference in habits across generations. Online banking is used identically by all three age bands - around 67% on average across the age bands bank online. There is also roughly equal use of P2P payments such as PayPal (averaging 33%). And millennials are visiting bank branches to manage money – 37% do, only slightly less than Baby Boomers at 47%.

All generations worry about similar events. The three age cohorts are, with margin of error, similarly likely to worry about personal data being leaked (56% on average), credit card cloning (54%) and identity theft (50%). This puts to bed the idea that older people are particularly nervous about technology.

Common concerns in day to day life

% that are concerned or very concerned about these issues



How financial services organisations should react

The principle of withholding trust in technology until confidence is won is highlighted in the finance sector. Caution is amplified when money is at stake. The priorities are stability and rigour. The attractions of new FinTech services rate below these mandatory factors.

Just 16% of respondents said seeing a rival bank with better technology would cause them to lose trust and switch, although the number leaps in markets such as the UAE (29%) and India (32%).

Old fashioned complaints are far more likely to trigger a switch of bank. Being hacked into and having money stolen (52%), and finding out the bank does not have the customers best interest at heart (36%), are more popular reasons to switch.

Consumer priorities are basic. Banks need to keep money safe, with 87% calling this as very important or essential, and the same number demand security of personal data.

Banks are conservative adopters of technology, and consumers appreciate that prudence. There's a view that banks are not the right organisations to experiment – 61% agree that banks should only use new technology which has been tried and tested elsewhere. Regulation plays a role in guaranteeing consumer faith in banks when introducing new technology, with 75% saying it is essential or very important that new technology is independently regulated for security.

That said, there is a clear opportunity. There is phenomenal trust in financial institutions. They are seen as cautious, knowledgeable, and extremely good at keeping data private. These are big assets.

For example, the vast majority of respondents say they are happy to share personal details with their bank if it meant receiving a better banking service, with only 16% refusing to do so. By contrast 57% would withhold personal information from social media platforms such as Facebook and Instagram – triple the rate. That's a decisive win on trust for banks.

There could be more room for the finance sector to roll-out clever new services in the West. As the chart above shows, consumers in the West are at ease with the technology employed by their bank. Travel East and consumers are experimenting with new services. In India consumers send payments via WhatsApp. In China new payment services such as Alipay and platforms such as WeChat have changed the market. Kevin Martin, Head of RBWM, HSBC Asia-Pacific, has seen this first hand: "China's consumers are years ahead of their counterparts in many developed economies in terms of how they ship and pay for what they buy."

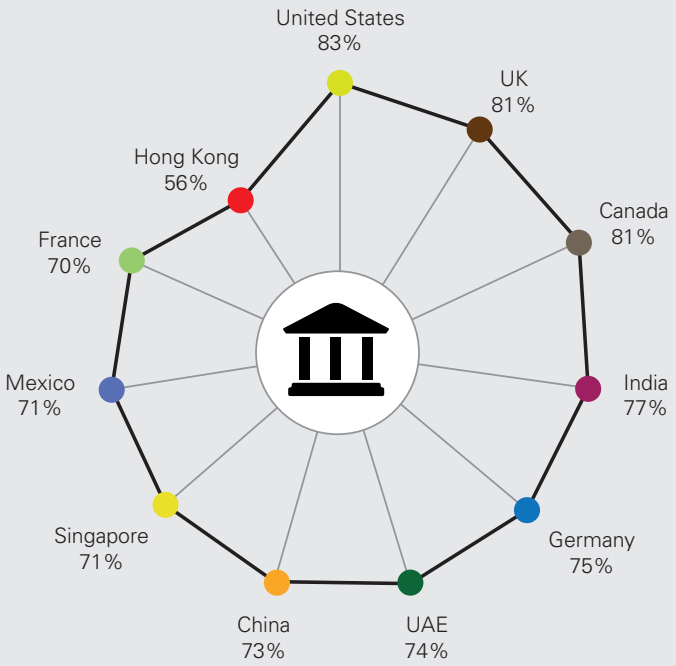
The implication is that Western consumers are underwhelmed, possibly underserved, with the level of innovation offered to them.

It is also clear there can be better communication with consumers, particularly to educate them about new services like robo-advice and biometrics. Awareness is low.

Above all, financial services providers can challenge the nature of the relationship with consumers.

An interviewee in the UAE captured a common view of the current

My bank is good enough for what I need it for



Caution is amplified when money is at stake. The priorities are stability and rigour.

Consumers are eager to see new services. However, trust in technology takes time. Reliability must be proven.

situation: "I don't really feel a personal relationship with my bank. I don't feel that they are reaching out to try to help me a bit more. They only call me [with] offers, meaning life insurance et cetera."

A Chinese interviewee said, "There is a purely monetary relationship between me and my bank, that is to say I use the bank as a savings vehicle and it is not involved in any other aspects of my life."

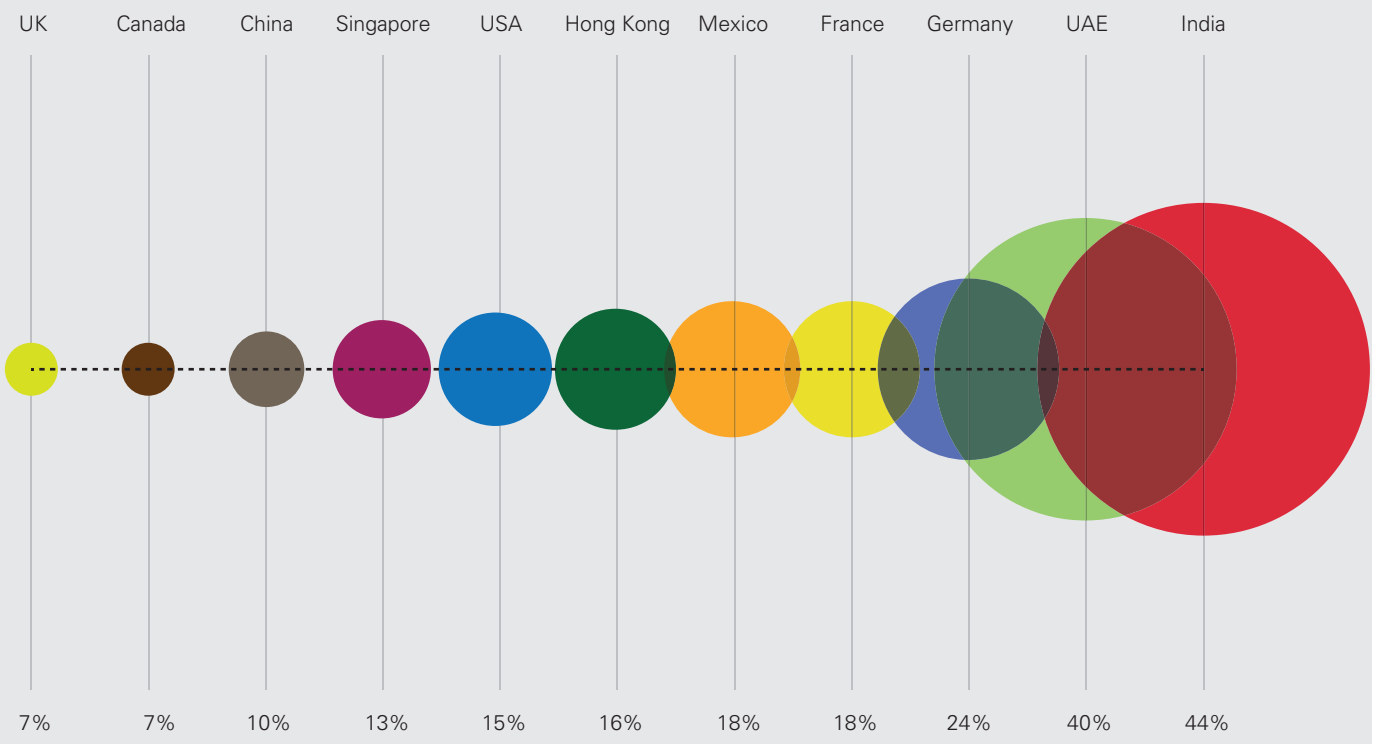
There may be an opportunity to change this. Converting the assets identified in this study – trust, competence, high level of data privacy, faith in the ability to innovate – can be used to roll-out helpful new services.

Julian Ranger, a technology and privacy expert, says the equation is favourable to finance organisations, if they take the initiative: "What they've got to do is trade on the trust that I've got in the apps to ask me for data to allow me to have richer, deeper life engagement. Give me advice. Give me algorithms that show me my credit worthiness. Why isn't the app permanently calculating my credit worthiness for me, and giving me tips and advice on how to improve it, so I can have a lower loan?"

Financial services providers are alive to the opportunity. "People's personal lives are being transformed by digitalisation, but in their corporate lives expectations have been lower," says Niall Cameron, Global Head of Corporate & Institutional Digital at HSBC, "We're now seeing that mindset start to change. People are saying, if I can use an app to order and track a taxi, why can't I have that level of ease with my transaction banking, or my treasury management?"

Consumers are eager to see new services. However, trust in technology takes time. Reliability must be proven. Users need to understand how a technology works, and what the downsides are. When that is achieved, trust is granted and adoption can soar.■

I find the technology I am offered overwhelming



Byte-size discoveries

What the *Trust in Technology* survey tells us – at a glance

THE NEED FOR EDUCATION

- 24% don't understand or have not heard of voice recognition technology
- Trust in biometrics tripled after a simple explanation
- 69% have not heard of robo-advisors
- 80% don't understand blockchain

HUMAN TO HUMAN TRUST

- 68% will trust someone until proven otherwise
- But only half (48%) believe most people are trustworthy
- 65% say they are always optimistic about the future

SECURITY

- 26% would trust iris recognition to replace passwords[1]
- 70% rely on traditional passwords[1] ****
- 21% use fingerprint recognition
- 6% use voice recognition

THE ADOPTION OF NEW TECH

- China (44%) and India (38%) most predisposed towards financial advice from computers
- China #1 in fingerprint technology adoption (40% now use it)

THE PERSISTENCE OF OLD TECH

- 39% of people in India own a pager
- Mexico has the biggest use of non-smartphones (43% use one daily)

1. Alphanumeric passwords

MEN AND WOMEN

- Men think they are the first to adopt technology but they are the biggest users of PCs, landlines and pagers
- Women are the biggest users of wearables, apps, and tablets
- Twice as many men as women own a smartphone but have never used it

HUMAN TO MACHINE TRUST

- 80% believe technology makes their lives easier
- 74% feel comfortable using new technology
- 84% would share personal data with their bank if it meant better service

"Would you trust a robot[2] to..."

- ...give mortgage advice **21%**
- ...open your parachute **20%**
- ...conduct open-heart surgery **14%**
- ...set you up on a date **11%**
- ...open a savings account **7%**

EAST BEATS WEST

Use of fingerprint technology

- 40% China
- 31% India
- 25% UAE
- 14% Canada
- 9% France
- 9% Germany

- In China and India, 41% are likely to trust a hologram assistant to help make money or investment choices versus 7% in France and Germany
- Germany has the lowest adoption of smartphone banking (4%)
- 50% of people own a fax in Germany
  50% of people own a fax in China

MONEY

Most common banking channels are:

- Online **67%**
- ATMs **55%**
- Branch **41%**

- 16% would change their bank if offered better technology
- 87% believe the security of data is as important as the security of money

2. Humanoid robot programmed by experts

Love, lust, and convenience

A common assumption in the theory of trust is that you either have it or you don't. This reductionist approach ignores the different intensities of trust. Love for humans tends to be deep. Emotion pulls us together, and when trust breaks the consequences are painful.

Human trust can trigger heart warming and colourful responses. One of our interviewees was asked about trust and answered: "Trust is one of the most important elements in our life that link us to one another. Without trust, there will be no friendships. There will be no relationships. We will end up being alone. When there is trust, everything is like rainbow."

By contrast, trust in machines is functional. It lasts so long as the device or service delivers a result. An interviewee in Hong Kong said that, "To trust something means to believe something that is true or correct or reliable that you can rely on it. Like my mobile phone or the lock of my house."

The different types of trust can be mapped against time and depth.

Where trust is deep and long-term there is love. Family members and close friends are in this quadrant. Long-term institutions for whom we have modest levels of trust are necessary features in our lives – there's a quadrant to reflect those values. Some services we use also to achieve a functional goal, but we take them to heart a little more. Search engines and online shops are functional in this way – we rely on them, and trust them to work, but we might abandon them if something better came alone.

Then there's the zone of frivolity – lust. Startups with unproven business models might catch our eye for a moment. Lust is shallow and short term. Buying a new gadget can feel like a quick fling – exciting, and experimental.

In Asia there is more trust in institutions and the government. Trust in financial institutions is shallow by comparison. Naturally, families sit tightly in the top left, loved and trusted now and forever.

The goal for any innovative brand is to move out of the lust zone by building deeper levels of trust. Long term use by customers can achieve this. A Canadian interviewee expressed their personal experience: "I have been using PayPal for a very long time, and I really enjoy the convenience and constant support from the company. Facebook I trust because of the number of times I have used it."

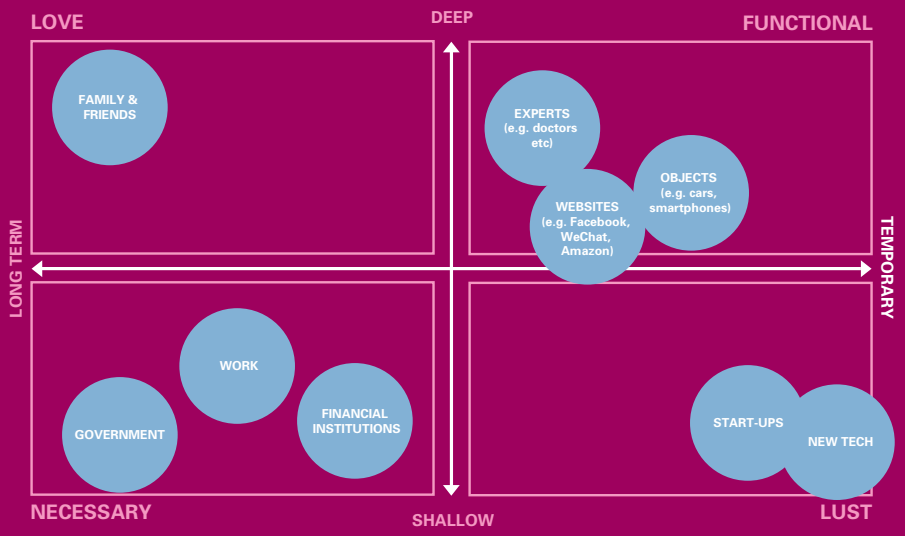
There are other ways to deepen trust. Tom Bailey, the technology editor of Shortlist magazine in the UK, says, "When you think about today's technology, things like washing machines, microwaves, coffee machines; most people understand how they work and so that removes one of the major barriers for trust. Whereas when it comes to things like robots and driverless cars the average person's not going to understand them at all so that is going to make trust very difficult, I think."

It is possible to break into the love quadrant. The "fanboi" phenomenon in smartphones is enduring. Fans take their chosen manufacturer to heart as much as a football team.

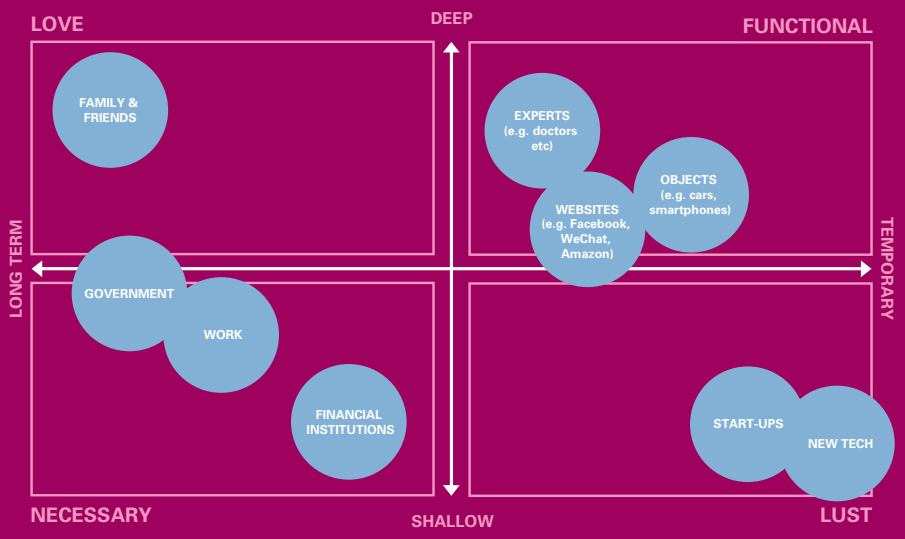
Currently only humans sit in the love zone. It's possible to move a brand closer. The key is to foster the same "human" elements such as compassion, understanding, integrity, and safety.

Financial AI that delivers some artificial humanity will be able to deliver genuine benefits to consumers, deepen relationships, and build trust over the long term.■

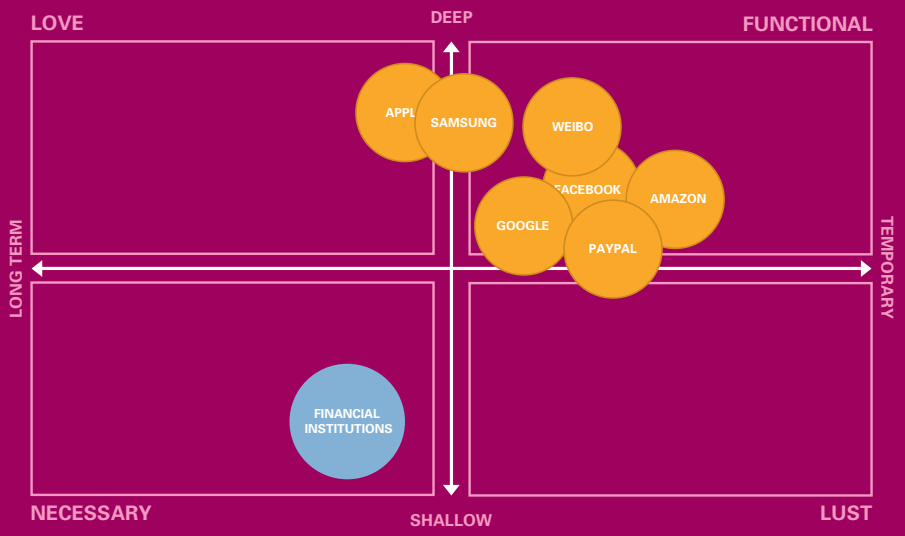
The West



Asia



Tech companies



How security fears undermine trust

Building trust in technology takes time. It requires familiarity with a product, and repeated results. As the understanding grows, trust builds. The process can be fragile in the early days. The research examined why so many technologies are struggling to get through an initial period. Respondents were asked to rank worries in life, and the top-rated concerns were "personal data being leaked" (56%) followed by "bank account hacking" (55%) and "debit or credit card cloning" (54%). These outrank a fear of serious illness or being burgled. In finance, security of finances, and security of personal data, are both rated by 87% as essential or important for banks to offer. This suggests that security and privacy are critical issues and could be preventing a higher adoption of devices.

The issue needs addressing. Industries including financial services are working hard to produce new services and security measures which enhance the lives of customers. Lower-income consumers in particular will enjoy advanced services delivered by technology, such as investment and pension advice. If scepticism can't be cured, these benefits will go unrealised.

It's easy to see why security is such a big worry. The explosion in malware and hackers is a fact of life on the internet. The UK National Cyber Security Centre annual review remarked, "The past year has been punctuated by cyber attacks on a scale and boldness not seen before. This included the largest recorded cyber heist, the largest DDoS attack and the biggest data breach ever being revealed."

The Cisco 2017 Cyber Security report that spam accounts for 65 per cent of all email volume, and up to 10 per cent of spam could be classed as malicious. Nearly a quarter of companies surveyed suffered an attack and lost business in 2016. Four in ten said those losses were substantial. One in five lost customers due to an attack.

News like this filters down to consumers. Combined with stories around corporate data breaches, and personal anecdotes of bad experiences, it's easy to see why so more respondents worried about data security than crime.

How to address security

Increasing confidence in security means addressing upgrading software and hardware to meet the challenge. The industry will claim that's being achieved. The number of vulnerabilities for hackers to exploit fell in 2016. Two-thirds of IT security professionals said they rated their security as very or extremely effective. Sophos anti-virus principal research scientist Chester Wisniewski says, "Practice good cyber-hygiene and you shouldn't get too worked up. Business as usual."

The problem is that consumers often aren't always taking the right precautions. In the survey only 33% said they always protect their devices with up to date security software. Only one in three always uses different passwords for different banking products – in breach of guidelines.

Worse, they often don't know what to do. An Instagram photo posted by Facebook founder Mark Zuckerberg in 2016 revealed his laptop had tape over the webcam and microphone. A necessary precaution? The former FBI director James Comey admitted he did something similar: "I put a piece of tape over the camera because I saw somebody smarter than I am had a piece of tape over their camera."

This is candid, and cuts to the heart of the problem. Technology can be brutally hard to understand. Even an expert can struggle.

The solution is to make life easier for consumers. Optimum security settings should be installed by default. User interfaces must be intuitive. This is illustrated by the green browser padlock displayed on browser address bars. The padlock assures the user the connection is encrypted, and address displayed is genuine.

Better information can cure concerns

Education has a key role to play. In the survey, biometric security polled low levels of trust, with iris recognition trusted by one in five respondents to replace passwords in the future, and voice and facial recognition trusted by under one in four. Even fingerprint recognition, which is now a standard feature on smartphones, is supported by a little under half of respondents. These results are at odds with the security industry which regards biometric as a long-term solution to identification.

A common worry with biometrics is a breach of the central database. If there's a leak of biometric data, the theory runs, the system would be invalidated.

This is a fundamental misunderstanding of the authentication process, says Jason Chaikin, president of Beijing-based Vkansee, a manufacturer of ultra-high resolution optical fingerprint scanners. "Tokenisation means there's no database to hack. Your fingerprint stays on your phone, and my fingerprints on my phone. It's not even the fingerprint, it's a template, and it's stored in a secure zone. For Apple it's called the Secure Enclave, and on the Qualcomm platform it's called the TrustZone. Even if you got this you wouldn't be able to print out a fingerprint and try and touch it to a sensor."

This concept needs to be explained, if the benefits of biometric security are to be realised.

For additional reassurance, the results of biometrics are being reinforced by multi-factor security. Multi-factor means two or more security systems are used together. For example, a text message can be sent to the user's phone with a one-time entry code to confirm possession of the device. Our survey shows 46% of Chinese respondents use third-party authentication to confirm their identity.

"Consumers need to be taught about multi-factor security," says Professor Kevin Curran, a senior member of the international IT body IEEE. "My mother got a text message to login to Facebook, and she thought it was a scam. What percentage of consumers know about it?"

The ideal multi-factor system takes

> *What is needed is education, combined a push by the security industry to develop easy to use tools.*

the initiative away from the users. This is the goal of behavioural analytics. Keyboard typing rhythms, voice pitch, mouse movement, walking gait, and speed of swiping can be tracked to create a "digital fingerprint". Swedish company BehavioSec looks at the angle a user holds a phone, how much of a finger touches the screen, and how quickly fingers move when typing. In August 2016, Pentagon CIO Terry Halvorsen announced that the US Department of Defense is moving to iris security supported by behavioural analytics.

Darryl West, Chief Information Officer, HSBC, says biometric and behavioural analytics offers a step change in convenience and security: "My objective when I finish my career in this industry is to eliminate passwords completely."

The instinct for privacy

A further worry for consumers is fear that data is being shared. Our poll shows security of personal data is rated as important as security of finances.

The wearables sector is particularly affected. Fitness trackers and health bangles have the ability to improve health outcomes. A survey by health information website Healthline found 80% of fitness wearable device keeps owners motivated to stick to an exercise routine. If used responsibly, retailers can use wearables to provide tailor made offers and coupons. The potential is only just being explored.

However, privacy is hitting adoption. A report by PWC on wearables found privacy was the biggest concern: "No one wants their personal data compromised and very few are interested in having it shared socially. Even among Millennials, only 14% of consumers were willing to have information about their shopping habits shared with friends and family." A survey of American and British adults by Rackspace Hosting found 51% cited privacy concerns as a barrier to adoption of wearable technology.

If this is addressed the gains could be huge.

The rise of ad-blocking

The latest conflict in data security is browser privacy. Consumer concern can be seen in the explosive growth of ad blockers. These browser add-ons act as a firewall, stopping tracking codes called cookies being distributed. As of December 2016, 615 million global devices had ad-blocking installed, a rise of 30% in a year, and 40% in Asia Pacific. Three-quarters of ad-block users say they are prepared to leave websites which prevent the use of ad-blockers.

Consumers are only just starting to realise the extent of the surveillance on the web, says Dr Markus Huber of the St. Pölten University of Applied Sciences, who recently co-authored the largest study of the effectiveness of ad blocking software: "The user searches for something sensitive like advice on depression or burn-out, and then sees ads on Facebook relating to what they've searched for. They are being spied on." Worse, he says, criminals use online ads to spread malicious code.

Third-parties can even track a user without any cookies using the unique attributes of the computer or smartphone such as browser version, installed fonts and screen resolution,

a method called stateless tracking. One study found 94.7% of browsers with both Flash and Java could be identified this way. "Stateless tracking is a really important issue," says Huber.

It is possible to block intrusive adverts and trackers using browser add-ons such as Ad Blocker Plus, Ghostery, Disconnect and Privacy Badger. But consumer knowledge of the options is poor, says Huber. Worse, some solutions are compromised by commercial concerns. "The most popular solution is Ad Block Plus," says Huber. "It has a bit of a dodgy business model, where it whitelists certain ads, making it the least effective. Can a reasonable consumer be expected to make the right choices? I don't know. Even some of my computer science students chose Ad Block Plus, which is the worst option." He recommends uBlock Origin in combination with Ghostery.

The fact that ad blocking now numbers in the hundreds of millions shows what a big issue this has become. It may get worse. New laws in the United States and United Kingdom potentially allow the gathering of people's browsing history for inspection by a wide variety of public bodies. Internet security journalist Kieran McCarthy wrote, "It is difficult to underestimate the impact that the shift away from data privacy to open season on personal information sales may have...it may result in significant societal changes."

The danger is that legitimate businesses and services are interrupted. Newspaper sites depend on advertisement revenue. Tracking cookies help websites deliver consistent experiences, such as keeping users log-in during multiple visits. A report by analytics firm Optimal predicts ad-blockers could remove revenue worth $12bn by 2020 in the United States alone.

The way forward

Add up these complications and it becomes clear why consumers struggle to know what to trust. Even a director of the FBI is unsure.

Fortunately, the right technologies exists to deal with the main worries. What is needed is education, combined with a push by the security industry to develop easy to use tools.

If these policies are pursued the uptake of new technology may be faster than the polling data suggests. Artificial intelligence is proving the point. Our survey data says consumers are reluctant to let an AI offer mortgage advice, let alone allow an AI robot to perform something as delicate as surgery, according to the our poll. And yet AI is surging in popularity. Smart speakers such as Amazon Echo and Google Home are a smash hit, with 33% of our respondents owning one.

Tom Bailey, technology expert, says the industry was taken by surprise: "If you look at things like Amazon Alexa, a lot of technology experts believed that consumers would never talk to technology, it would just be too weird, but amazingly it's happened almost overnight."

As technologies come to market with the potential to improve the way we handle money, motivate us to keep fit, and connect us more closely to the world around us, it becomes more imperative than ever to promote trust in technology.■

The case for robo-advisors

Robo-advisors are one of the most exciting new technologies in financial services. These consultants take the form of a web service. The robo-advisor poses questions to the user, and then outputs the best course of action based on the evidence. The process can account for risk appetite, age, investment goals, awareness of financial matters, and many other critical factors just as a professional financial advisor would. The service is hailed as a way to offer financial advice to a broad audience, delivered at their convenience via the web.

Popular fields include pensions, investment and savings advice.

Our survey set out to establish the level of trust in robo-advisors at this early point in their development.

Overall 19% would trust a robo-advisor to help make choices around investments, rising to 38% in India and 44% in China. There are sceptics. Just over half (53%) of people would be unlikely or very unlikely to trust a robo-advisor that makes recommendations based on AI algorithms. In France only 9% would be likely to trust an AI robo-advisor, and 6% in Germany. Giving the robo-advisor a user-friendly make-over offers no gain – hologram assistants have similarly low levels of trust.

There are pros and cons of the robo-advisors. Critics say the inputs are rigid and struggle to cope with unique situations. Regulation of robo-advisors is still developing. But the robo-advisors are growing in usage.

In order to increase trust in robo-advisors it will be necessary to communicate the advantages they bring. Here are the seven main strengths of these digital consultants. If these ideas can be explained to users it may be possible to accelerate adoption of this valuable concept.

1
Harness the wisdom of multiple experts

Talk to a human and you reap the knowledge of a single person. If you are lucky they may be an industry veteran with a detailed knowledge of the subject matter. Or you may land a novice still mastering the basics. Robo-advice offers a stark contrast, as it can be programmed by not just one expert, but a committee of experts each contributing their specialist knowledge. The advice is inspected, reviewed, and tested to ensure the users receive the highest possible quality of advice. All users access the elite advice of many outstanding minds.

4
Frequent upgrades

Human consultants need to work hard to keep up to date with their field. For robo-advisors constant improvement, and near unlimited, accurate memory is a way of life. The programmers can add new functions at will. Users benefit from the moment the changes are set live. Feedback from clients can be incorporated. New legislation and new products can be rapidly integrated. And the robo-advisor never forgets the new material, or relapses into obsolete advice.

5
Real time information

A robo-advisor can be plugged into market data to match advice to market changes. For example, mortgage deals change frequently, with new interest rates, fees and time periods. A robo-advisor is purpose built to examine the full range of market options, and adapt advice in real time. Human consultants may struggle to keep abreast of the information, and often resort to using their own robo-advisor to augment their knowledge.

2
Low cost

A major factor in the rise of robo-advice is the cost, which often under-cuts human consultancy fees. This means savings for users. It also makes financial advice available to a cohort of young and lower-income consumers who were previously priced out of the market (more likely not in a position to invest). Since the overheads of providing a robo-service differ from a human consultation the low cost need not reflect the quality of service.

3
Friendly user experience

Robo-advisors are accessible from any PC or mobile device. This makes them convenient for people who live in remote areas, or work unsocial hours. The online format is an appealing alternative for anyone too shy to book an appointment with a human advisor. "Reckless conservatism" through inactivity is all too common in financial planning. Furthermore, the user experience can be refined over time through multivariate testing – running many versions, each slightly different - so the experience improves over time.

6
Rebalancing

Investing is an ongoing process. Changes must be made to asset allocation as time passes. Robo-advisors are formidable at this role. They can track portfolio values, identify potential changes, and implement whatever strategy they are programmed to follow. Clients can be prompted to retake the questionnaire at regular intervals. Ongoing portfolio rebalancing is now seen as a main strength of robo-advisors.

7
Works together with humans

In the early days of robo-advice it was suggested that humans would be supplanted by their silicon rivals. Instead we've seen a happy collaboration arise. Robo-advisors take the simpler and more onerous duties, such as offering early consultation to would-be investors, and answering basic questions. This liberates human counterparts to focus on specialist activities.

"There is an advice gap in financial services. Unless you have a certain amount to invest asking a professional adviser doesn't make sense, and that is where a robo-advisor can really help a big chunk of society. The technology is actually quite simple, using 'if then' decision logic. The results are crafted by our best advisors and consistent with the regulatory framework, so everyone gets a very high standard of advice.

There's also a category of self-directed people who can benefit from robo-advisors. They can be sophisticated traders, but have not been given the tools necessary to think through their risk appetite and the risks of what they are doing. Tools are being developed to help these people.

Robo-advisors can help review an investment strategy on an ongoing basis. Life changes, things happen, and we can give customers nudges to suggest they should look again at their investment strategy. Gains like this are why we are so excited by robo-advisors."

Charlie Nunn, HSBC Global Head of Wealth Management

Trust at the outer limits of technology

The potential for artificial intelligence to change new markets such as health, energy, transportation and education is only starting to be understood. The next generation of AI engines will be more powerful and creative than anything we've seen to date. They will have the ability to supplement human endeavours in bold new ways, and even challenge human performance in previously closed fields. The arrival of these engines will provoke profound questions. Here are three of the most challenging conundrums. In each case, human users need to assess how far they they trust an AI to complete a task.

Case study 1: Would you trust a machine to set you up a on a date over a family member?

As artificial intelligence becomes more sophisticated, the realms where human judgement is supreme is shrinking. Yet surely there are some fields where the personal touch beats the cold numerical skills of an AI?

Dating is a classic case. Can an algorithm beat human judgement in selecting a partner romance?

Our research says not. A friend is trusted by 48% of respondents to find the right person, and over third would trust a family member (37%). Only 8 per cent trust a humanoid robot programmed by experts in relationships.

Could we get respondents to think again? In fact we can do a deep analysis of the machine's chances. The popularity of internet dating means we have vast reservoirs of data to draw from, and the findings are truly surprising. They tell us about the power of machines to guide our lives, even to tell us about our unconscious desires.

Christian Rudder is a pioneer of internet dating. He founded dating site OK Cupid, now owned by IAC, which also runs Match.com and Plenty of Fish. Rudder studied mathematics and Harvard and became obsessed with looking for patterns in the data. IAC's sites offered him 55 million American users – that's one account for every two single people in the US. He noted, "I could go and look at what actually happens when, say, 100,000 white men and 100,000 black women interact in private. The data was sitting right there on our servers. It was an irresistible sociological opportunity." He published the results in Dataclysm: Who we are when we think no one's looking.

Rudder sifted through vast pools of data to identify which traits are important. Take looks. Attractive people are in demand. They get disproportionate attention, receiving vastly more messages and getting a higher reply rate to their own messages.

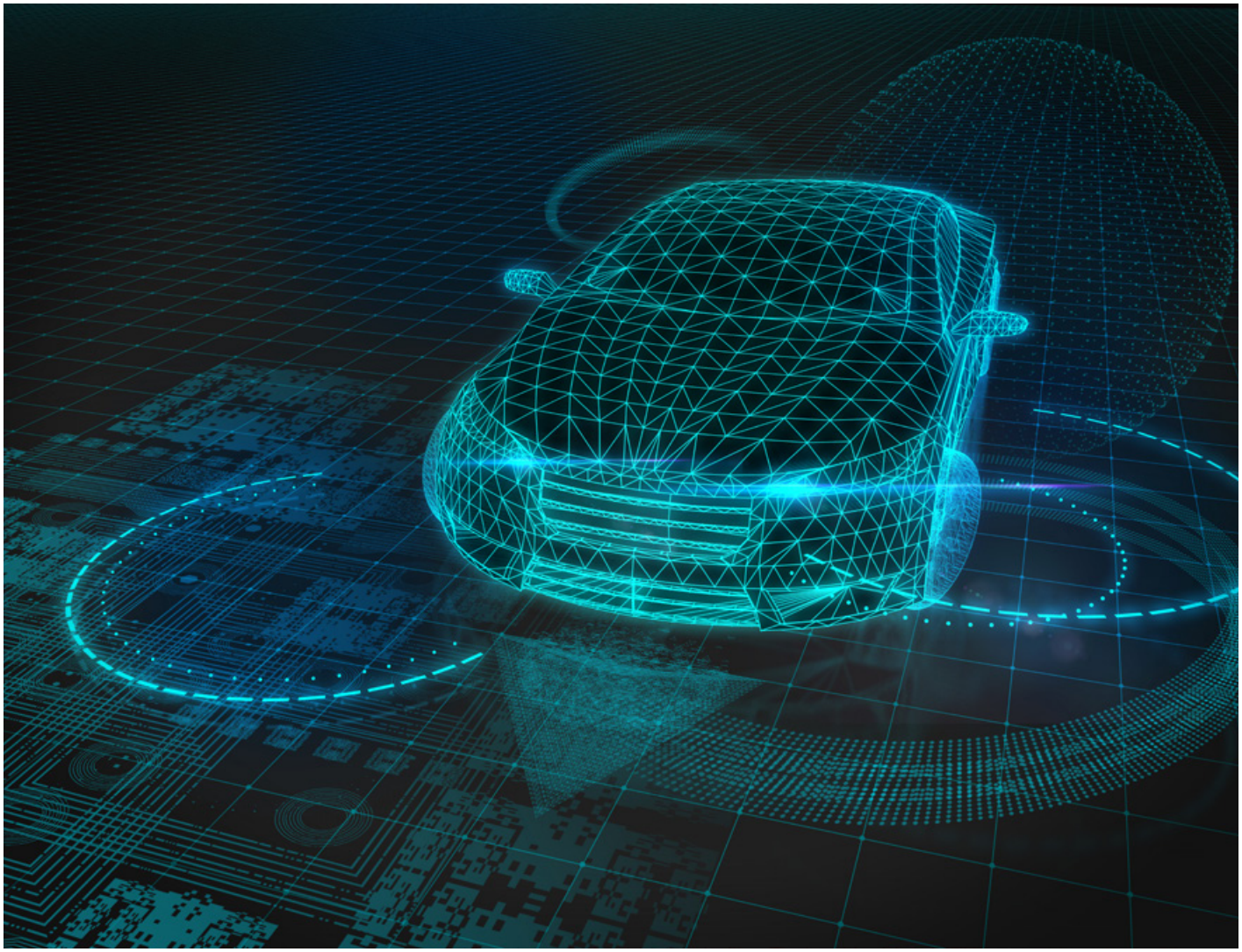
Yet when OK Cupid ran a "blind date" scheme, withholding images and using only a compatibility score to create matches, satisfaction rates soared. Looks were irrelevant. Rudder said, "No matter which person was better-looking or by how much - even in cases where one blind-dater was a knockout and the other rather homely - the percent of people giving the dates a positive rating was constant. Attractiveness didn't matter."

The same is true in the partner checklist. Priorities such as religion, politics, and smoking are usually rated "mandatory". Yet two oblique questions have superior predictive power: Do you like scary movies? and Have you ever travelled alone to another country? Three-quarters of long-term couples brought together answered the same way, either yes or no to both. Rudder notes, "People tend to overemphasize the big, splashy things: faith, politics, and certainly looks, but they don't matter nearly as much as everyone thinks. Sometimes they don't matter at all."

The data is clear: we don't know what we want and what is important in a partner. A machine can correct for this. If a family member is picking a date by listening to your priorities, the chances of a good match are lower.

The message stretches beyond dating. Machines can use the power of big data to draw insights into our desires that even we are blind to.■

Case study 2: Who should an autonomous vehicle protect?



Machine ethics was once the preserve of science fiction writers like Isaac Asimov with his three laws of Robotics. Now the question is real. Manufacturers are grappling with what moral code to install.

The leading realm is autonomous vehicles during a crash scenario. In theory driverless cars should be a lot safer than human drivers. The US highways chief talks about "a world where we could potentially prevent or mitigate 19 out of 20 crashes on the road," saving millions of lives worldwide. But from time to time an AV will crash. Which raises the question – if someone's going to suffer, should it be the passenger or a pedestrian? How about ten pedestrians versus one passenger?

Jean-François Bonnefon at the Toulouse School of Economics partnered with MIT computer scientist Iyad Rahwan to find answers by crowdsourcing. His team conducted six online surveys using the Amazon Mechanical Turk platform. A total of 1,928 participants answered moral questions involving an autonomous vehicle (AV). The results were published in Science magazine in June 2016.

The mainstream view is that the AV should protect as many lives as possible. In one example the choice was 10 pedestrians versus one passenger. A decisive 76 per cent of participants voted for the AV to sacrifice the lone passenger and save the ten pedestrians.

As the ratio of pedestrians to passenger falls, so did approval for sacrificing the passenger. When one

passenger faced one pedestrian, only 23 per cent thought it moral for the car to sacrifice the passenger.

Then the academics asked separate question. How likely are you to buy a car programmed to act ethically? Or would you prefer a selfish AV which protects you? The researchers observed "even though participants still agreed that utilitarian AVs were the most moral, they preferred the self-protective model for themselves".

Government regulation might fix this selfish tendency, but the survey reveals intervention has negative consequences. "Our findings suggest that regulation for AVs maybe necessary but also counterproductive", concluded the report. "First, most people seem to disapprove of a regulation that would enforce utilitarian AVs. Second - and a more serious problem - our results suggest that such regulation could substantially delay the adoption of AVs, which means that the lives saved by making AVs utilitarian may be outnumbered by the deaths caused by delaying the adoption of AVs altogether."

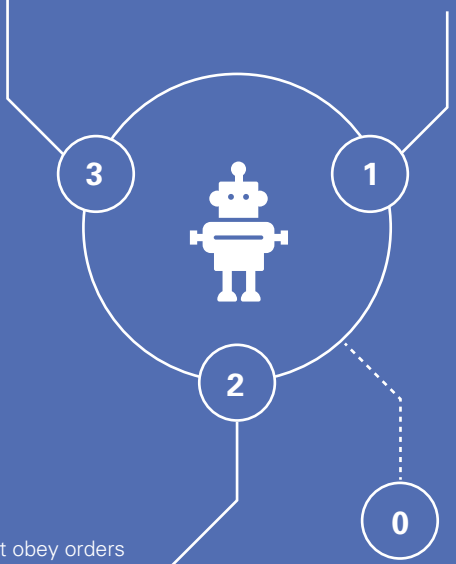
The question of whether a user can halt an AI if needed is also pertinent. AI house DeepMind, which became famous for beating an elite player of the Chinese boardgame Go using a self-taught AI called AlphaGo, published a paper calling for a "big red button" to allow an AI to be switched off in case of an emergency. The authors explain that AI agents are "unlikely to behave optimally all the time." They conclude, "If such an agent is operating in real-time under human supervision, now and then it may be necessary for a human operator to press the big red button to prevent the agent from continuing a harmful sequence of actions - harmful either for the agent or for the environment - and lead the agent into a safer situation." ■

Isaac Asimov's Three Laws of Robotics

Science fiction writer Isaac Asimov wrote more than 500 books and is know as one of the most perceptive explorers of the shape future technology might take. He devised this three laws in the 1942 short story Runaround. They are regarded as the prototypes for writing an ethical code for machines.

A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.

A robot may not injure a human being or, through inaction, allow a human being to come to harm.



A robot must obey orders given it by human beings except where such orders would conflict with the First Law.

Asimov also added a fourth, or zeroth law, to precede the others:

0. A robot may not harm humanity, or, by inaction, allow humanity to come to harm.

Case study 3: How much should we use nudge technology to improve behaviour?

Economists Dick Thaler and Cass Sunstein invented nudge theory, and the pair are brimming with examples of how effective it can be. In their book Nudge they describe a pension scheme which harnesses the concept of "loss aversion" - the idea that consumers hate losing something more than they enjoy the gains. Loss aversion explains why pension contributions are lower than they should be. The pair created a pension plan in which no contributions are made until a pay rise. Then a percentage is paid in. The saver therefore never sees a reduction in income. The idea was a triumph. Contributions rose 200 per cent.

Nudge theory often works without participants noticing. The pair cite a school which wanted to promote healthy eating. Without changing the menus, the food display was changed and the layout re-arranged. This approach altered the consumption of food items by 25 per cent.

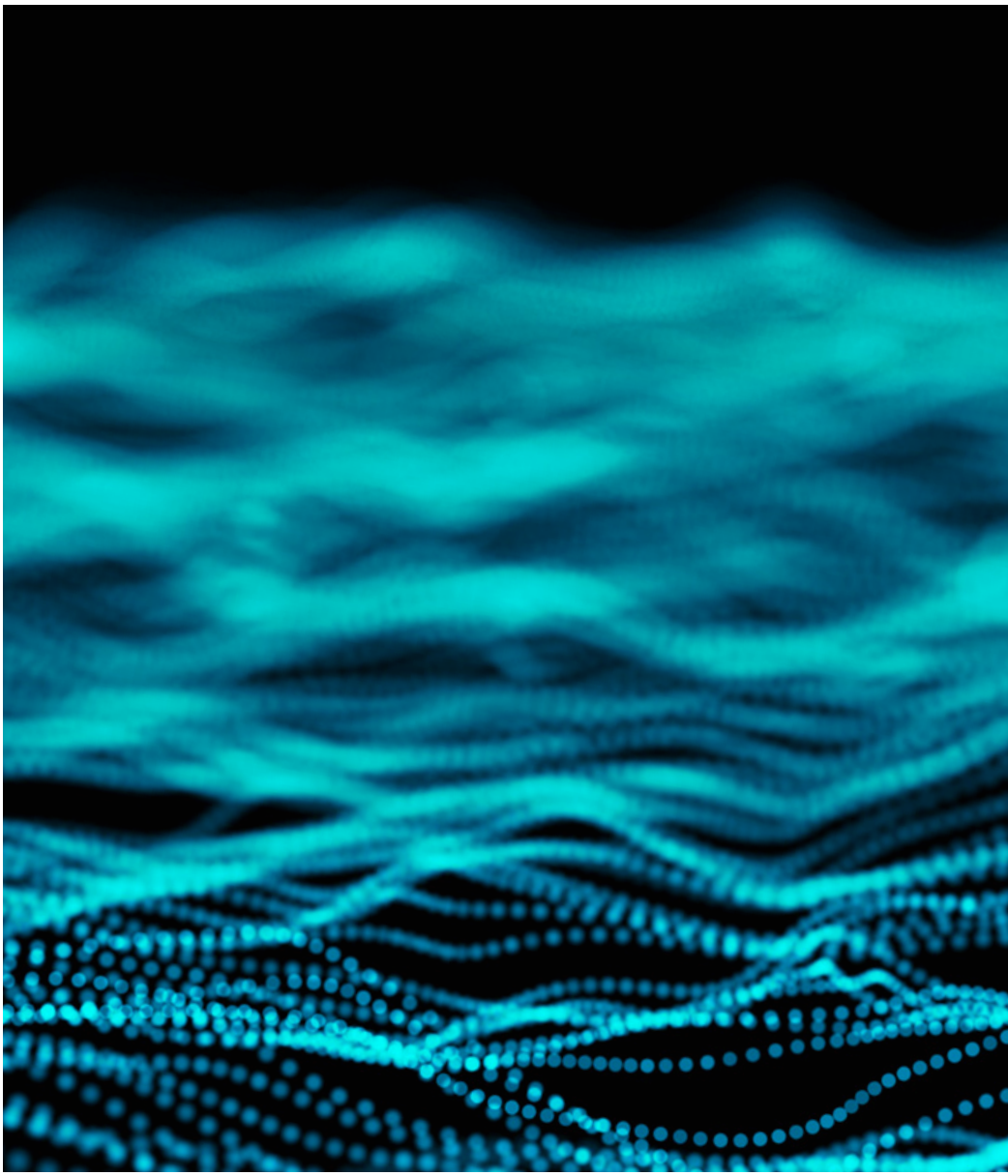
When used effectively a nudge can produce net benefits. An app called SmartSave developed with a FinTech company called Pariti helps increase the amount people save. The app can be linked to any account, and automatically diverts money into a savings account according to user-defined rules. For example, purchases resulting in a few pennies over or under a round pound results in the change going to the savings account. No action required. It prompts users when it's "safe to save". As a result, money accumulates in the savings account without effort.

The question is, how far should the concept go?

Nudge theorists are so good that behaviour can be manipulated to extreme degrees. Casinos are designed with one thing in mind: to keep gamblers gambling. Clocks are removed, daylight eliminated, and the games are fined tuned to keep rewards unpredictable. The result a twilight world that's impossible for some people to leave behind.

The minds behind casino design are now refining websites and apps to maximise engagement. Adam Alter, Associate Professor of marketing at New York University's Stern School of Business, has examined this in a new work called Irresistible: The rise of addictive technology. He warned, "As an experience evolves, it becomes an irresistible, weaponized version".

Consumers are aware of the potential of nudge theory. Our survey shows 88% expect nudges in financial behaviour to be powered by



AI engines within 5 years.

Does that mean there's an open license for nudging? The author of the theory isn't too sure. Cass Sunstein published a follow up work called The Ethics of Influence looking at the dangers of over-use. He raises the issue of consent. There the question of responsiveness - stress can make people more reactive to nudging. Might it lead to lower-income workers getting harder nudges than the well off? And the issue of incentives – who is really benefiting?

Qatar, the UK, Australia, and Germany have nudge units. The potential for good outcomes is huge. The question is, should consumers always consent to nudges? The balance between paternalism and manipulation is hard to strike.

Sunstein states, "Certainly choice architects should be focused on the welfare of choosers, rather than their own". He notes the extreme sensitivity to issues of manipulation, particularly in nations with a history of poor human rights. Nudge theory is a potent tool. But if used to excess then the good it can do may be curtailed.■

Definitions

Algorithm

An algorithm is a series of sequential steps, like a recipe in a cook book. When the steps are followed an outcome is achieved, and the algorithm can begin again. Simple algorithms are used to tackle tasks such as routing engineers to jobs in the shortest possible distance, and pricing airline tickets dynamically. Artificial intelligence is built on algorithms.

Machine learning

An AI engine can be endowed with the ability to learn beyond its programming. Machine learning happens when an AI engine sifts through data to discover new patterns, and builds a knowledge base on its own initiative. It's similar to the way the human brain works. The concept allows machines to operate beyond the bounds of human tuition. DeepMind's engine AlphaGo learned the boardgame Go using machine learning. When it mastered the basics, AlphaGo was replicated, and the engine played other instances of itself to improve to world-class strength.

Weak AI

The artificial intelligence of today is task-specific. It can tackle well defined tasks. A translation bot can translate and a medical algorithm can interpret and X-Ray, but two can't swap jobs. Sophisticated AI engines such as IBM Watson, Wipro Holmes, Salesforce Einstein, and Ipsoft Amelia, are collections of task-specific AI faculties operating under a single umbrella to provide the appearance of general intelligence.

Strong AI

In time the power of AIs will grow to match the versatility of humans. They will operate across fields, and be able to tackle challenges beyond their immediate programming. Also called strong AI, there is considerable debate as to how it will be possible to determine the arrival of Strong, or General, AI. Apple co-founder Steve Wozniak invented the Coffee Test to identify a Strong AI, in which a machine must go into an American home and figure out how to make coffee. The next stage of Sentient AI, in which an artificial mind truly experiences sound and colour, rather than merely processing data, is a potential variation of General AI, though there is no agreed methodology for identifying such a machine.

H2M versus H2H

How machine interactions differ from human relationships

Strong user experience (UX) design is vital in winning the trust of users. To do that it is necessary to unpick the logic of human to machine interaction to identify concerns. How does H2H differ from H2M? The differences start with the physical presence of a human. The human face is expressive, communicating all sorts of nuanced information. Web interfaces and robots offer less information – no smiling, frowning, or blushing. Then there's the distinct nature of human intelligence, in which information from many different fields can be pulled together at will. Machines are task specific, for now at least.

A good user experience can anticipate the needs of users, and correct for shortcoming in the machine. If done well, the user may start to feel there is little a human can offer over a machine.

Here are some of the key differences, together with potential solutions.

Common sense

Dutch tourist Milan Schipper recently ended up in the wrong Sydney after booking his flight online. Mr Schipper accidentally booked a ticket to Sydney, Nova Scotia, and only realised when he arrived in Toronto: "The plane was really small and so I figured, would that make it to Australia?" Amusingly he met a woman from the US in the same predicament. It's a classic example of lack of common sense in machines. A human would most likely have checked which Sydney he meant.

Solution: Common sense is increasingly programmable. Machine learning tracks common behaviour and flags unusual activity - now proving a major asset in the fight against fraud.

Early warning signs are absent.

A computer crash comes as a shock. There's rarely a warning sign, just a sudden switch to a blue screen or error sign. As a result users struggle to estimate the reliability of a system at any given moment. Human to human interaction offers helpful clues of impending malfunction, such as sweating, voice intonation, and posture.

Solution: Incorporate status indicators. For example, aeroplanes include low-fuel alarms, and Siemens' latest H-Class gas turbines are fitted with 1,500 sensors to warn engineers when performance is falling below optimal.

Where are you?

It's important to know who we are talking to, and where they are located. Data protection rules mean this information must be conveyed. Websites tend to obfuscate this information. Time can also be unclear – when was a webpage written? The information might be ten years out of date.

Solution: Make it clear when data is being transmitted and stored internationally. Date stamp information.

Unclear qualifications

Doctors and lawyers display professional certificates on the practice wall. It helps clients confirm they hold the right exams. Technology can withhold important information such as the qualification of programmers and authors to provide advice.

Solution: Financial services providers and other skilled professions should cite regulatory compliance and, where appropriate, expertise. A leading medical organisation, the Mayo Clinic, offers online advice accompanied with the biographies of the writers.

Intrusive upgrades

A source of mistrust in technology is questionable upgrades. An app can develop new and unwelcome characteristics. For example, it has been known for apps to activate Bluetooth, GPS and microphone functions to gather data on user activity – something not specified in the original release version.

Solution: A code of practice should forbid invasive upgrades.

May I see the manager?
Get served bad food in a restaurant and it's easy to ask for redress. By contrast technology can often be a closed environment, with no obvious route of recourse when things go wrong. Our survey showed 74% of respondents believe it is essential or very important customers can know where to go when things go wrong.

Solution: List support options, such as email, online chat, and phone numbers.

Digital answers for analogue problems
The human vocabulary is blessed with myriad qualifiers, intensifiers and equivocations to offer nuance to statements: "I think...it might be the case...I'm almost certain." Crude UX programming can strip out this useful information, and present answers with a misleading sense of reliability. For example, online journey planners state the driving time from Florence to Pisa is 71 minutes, but never with a degree of probability.

Solution: UX designers need to incorporate reliability indicators where needed.

Consequences of an error
A rogue employee acting in an unacceptable manner can be isolated, blamed and removed. An error in technology can't be handled so efficiently. Users tend to regard technology as representative of the brand. The blame game offers no reassurance. As a result standards must be higher for technology.

Solution: Develop reliability parameters. Impose service level requirements appropriate for the context.

Tailor-made advice
An experienced human advisor adapts their thinking to the client. In this way a sophisticated client can be given high levels of information, and a first-time applicant offered simplified material. All too often machines deliver the same service to all users. At most there is an "advanced" or "basic" menu, although toggling between them is sometimes a skill in itself.

Solution: Machines should identify the knowledge of the user, and adapt fluidly.■

Conclusion
The path to high trust

Trust is a critical concept in the adoption of new technology. High trust means early adopters are prepared to play with new concepts. Breakthrough ideas get trialled and validated. In financial services, high trust means banks can roll-out new services which improve lives and open new opportunities. It's a virtuous circle. High trust means consumers adopt better security tools like biometric identification, leading to fewer breaches. Low trust suppresses innovation. Great ideas are ignored. Co-operation is slowed. Costs rise.

This report shows there is a need to focus on improving trust, and offers insights into what can be done. Here are the five essential lessons for policy makers and brands.

1
Invest in education

There is always a gap between technology and public awareness, and education is the key to minimising this gap. Great work is currently being done. Google India is working on educating the public on safe internet browsing. The FIDO Alliance is promoting understanding of tokenisation in the biometric industry – essential if consumers are to understand there's no central database to be hacked. Technology can play a role. CybSafe is a start-up using behavioural analytics to identify worker's areas of vulnerability, tailoring tuition to cover their specific needs. Even small gestures can help. Our survey showed trust in biometrics rises 6 percentage points after a short briefing. The march of technology is remorseless. Education will ensure no one is left behind.

2
Kitemarking

The complexity of technology means consumers and businesses need a straightforward guide on what to trust. International cyber security standards such as ISO 27001 and 27002 are useful technical protocols, but are not seen as useful guides by the general public. Kitemarks are a simple way to display compliance with official standards. Progress is already being made by organisations such as the GSMA, and the Internet of Things Security Foundation. Kitemarks elevate standards, as demonstrated by the UK's government's Cyber Essentials programme which issues a certification logo to organisations meeting security standards. The goal should be to provide an intuitive set of symbols to guarantee minimum levels of security and performance.

3
Simplified interfaces

User behaviour is to a large part dictated by the structure of the user interface. If good choices are easy to find and select, and poor choices are excluded or hard to find, then it is possible to increase performance and trust. Interfaces should be standardised whenever possible. For example, the internet browser green browser padlock makes it simple to see if a connection is encrypted and the address bar genuine, but the green bar is displayed differently on each browser, leading to unnecessary confusion.

4
Accelerate biometric and behavioural security

The trade-off between convenience and security is not a constant one. It is possible to enhance security whilst minimising annoyances for users. Biometric security offers a clear way to speed up authentication whilst reducing inconvenience. Behavioural analytics is a complimentary technology, typically working without the consumer needing to do anything at all following enrolment. Multifactor security should be promoted where high-level security is needed.

5
Regulation, including transparent algorithms

The poll shows emphatic support for independent regulation, with 75% believing it is important when banks introduce a new technology. This tallies with other sectoral surveys, such as the IOActive poll of IT professions showing 83% support. Regulation needs bite. The European Union's General Data Protection Regulation will offer greater guarantees when it comes into force in 2018, but appears to have omitted rights in certain areas, such as the right to explanation of decisions made by automated decision-making systems. A report by Sandra Wachter, Brent Mittelstadt, and Luciano Floridi, a research team at the Alan Turing Institute in London and the University of Oxford, calls for an independent watchdog to police AI, and offer redress for people who believe they have been discriminated against. There is a strong case to examine the need for transparency in algorithms and AIs used in public contexts.

Final thoughts

These measures directly address the trust deficit. The impact could be significant. The world is at risk of creating distinct classes of technology users, with less-able users increasingly left behind.

A few thoughtful steps, like promoting biometric security and developing simplified interfaces, can spread the benefits of technology to the widest possible number of people. Education can help even novices get involved.

This is more than economic prudence. The human race is moving into an era where technology shapes our lives. It's a journey we should be taking together, so we can create a world in which we all benefit from the fruits of innovation.

Sources

How security fears undermine trust

Wearables
www.pwc.com/us/en/technology/publications/assets/pwc-wearable-tech-design-oct-8th.pdf

Rackspace
blog.rackspace.com/uk/category/newsroom

Healthline
www.healthline.com/health-news/consumers-concerned-about-privacy-personal-health-data-wearables-mobile-apps-072815

Kieran McCarthy
www.theregister.co.uk/2017/03/28/congress_approves_sale_of_internet_histories/

Ad Blocking revenue lost.
www.theguardian.com/media/2016/may/17/adblockers-us-growth-remove-12bn-advertising-2020

The case for robo-advisors

The social dilemma of autonomous vehicles by Jean-François Bonnefon, Azim Shariff, Iyad Rahwan

www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm

www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

www.washingtonpost.com/news/wonk/wp/2016/08/18/why-a-computer-program-that-judges-rely-on-around-the-country-was-accused-of-racism/?utm_term=.508be009b4a2

Vanity Fair article for Elon Musk quotes
www.vanityfair.com/news/2017/03/elon-musk-billion-dollar-crusade-to-stop-ai-space-x

H2M versus H2H: How machine interactions differ from human relationships

www.siemens.com/innovation/en/home/pictures-of-the-future/industry-and-automation/Remote-Services-Early-Warning-Systems-for-Turbines-and-Tomographs.html

www.theguardian.com/world/2017/mar/31/teen-accidentally-flies-to-sydney-nova-scotia-australia

Mayo Clinic
www.mayoclinic.org/about-this-site/meet-our-medical-editors

Rik Ferguson
twitter.com/rik_ferguson/status/854979511498289152

Interviewees

Brian Lord, former deputy director of GCHQ, now managing director of PGI Cyber

Daniel Hulme, founder and chief executive of Satalia.com

Jason Chaikin, president of Vkansee

Dr Markus Huber, of St. Pölten University of Applied Sciences

Professor Kevin Curran, senior member of the IEEE

Chet Wisniewski, principal researcher of Sophos

Ken Munro, director of Pen Test Partners

Alice Thwaite, founder of the Echo Chamber Club

Expert panel

Devie Mohan, FinTech Expert

Julian Ranger, Technology and Privacy Expert

Will Higham, Cultural Trends Expert

Tom Bailey, Technology Trends Expert

Chris Gledhill, FinTech Influencer

This report has been written independently for HSBC. The information and / or opinions provided do not necessarily constitute HSBC's view.

The study represents the views of 12,019 people from 11 countries and territories: Canada, China, France, Germany, Hong Kong, India, Mexico, Singapore, The United Arab Emirates, UK, and the US.

Populus conducted the qualitative research in March and April with 66 members of an online community, including six members from each of the 11 nations in question. All respondents answered all questions and their contributions have been made available separately for use in the media. Populus also consulted twice with a panel of experts to research in-depth opinions and expertise on the topic.

Ipsos MORI conducted quantitative research with over 12,000 participants in total. 2,000 of those participants were from the UK and 1,000 participants came from each of the remaining countries. The quantitative findings are based on a nationally representative survey of people of aged 18 and over in each country, and the research was conducted in March/April 2017. Information and/ or opinions provided within this report constitute research information only and do not constitute an offer to sell, or solicitation of an offer to buy any financial services and/or products, or any advice or recommendation with respect to such financial services and/or products.