



# BETTER THAN COMPLIANT: TRUST-CENTRIC ORGANISATIONS

How can you get ahead in  
a post-trust landscape?

Authors:

**Tessa Darbyshire**  
Strategist  
*Adeptiv UK*

**Anirban Basu**  
Visiting Research Fellow  
*University of Sussex*

**Natasha Dwyer**  
Senior Lecturer in  
Digital Media  
*Victoria University*

**Stephen Marsh**  
Associate Professor,  
Trust Systems  
*University of Ontario  
Institute of Technology*

# Why Read This Paper?



We're biased, but you should definitely read this paper. Compliance with the GDPR is like Fairtrade; it's simply a matter of brand hygiene, and customers expect it. There's an advantage to be had in going beyond it, proving that you're better than compliant. Here we include tips and tricks to design for trust, both technically, and in consumer facing messages. You can change the way your customers think about you, you just need to make trust the heart of your brand; bringing consumers closer to processes, empowering them to make their own decisions regarding digital contracts, and building longer-lasting, more personal relationships with every individual.





# Key Takeaways

- **The landscape is changing, only the fittest will survive**

As consumer privacy legislation continues to evolve, and media hype increases public awareness of the issues, the onus is on brands to support their customers.

- **Authority isn't enough to guarantee trust**

In the age of fake news, brands can no longer tell individuals what's good for them.

- **Significant is defined by the individual**

Consumers make their own decisions about what constitutes a breach of their trust, and therefore what has a significant impact on them.

- **Transparency, inclusion and dialogue are key**

Brands can win the trust game by building from transparency, which is a legal requirement, designing a culture of inclusion, and building processes that foster dialogue.

- **The shift is an opportunity, more than a threat**

The brands that get ahead are able to get closer to their customers, developing stronger, healthier long-term relationships.



# Introduction: A Changing Landscape

*A brief history of trust.  
New legislation and  
shifting goal posts.*

The world  
produces

**2.5**

exabytes of  
data per day

**90%**

of all existing data  
has been produced in  
the last 2 years

We are living in a time when the nature of trust is changing radically. Consumers are more reluctant than ever to tick the 'accept terms and conditions' box without understanding what it entails. However, whilst it is relatively simple to find the legal documents outlining precisely what you signed up for, understanding precisely what they entail for an individual can be almost impossible.

## How have we ended up here?

We're ten years on. The financial crisis of 2008 was a key trigger in the ongoing shift in consumer perception, undermining trust in institutions which was previously taken for granted, particularly in the financial sector. This is an ongoing issue. For example, the Australian Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry recently found that banks have been exercising draconian actions against some of their customers, including allowing individuals to take on loans that they could never repay with the result that they lost everything. The actions of the banks were legal but unethical. Stories like these in the news make more and more of us privacy aware, driving a desire for autonomy, rather than delegating to authority.

As consumers ask more questions, individuals become more aware of how contracts, that previously they would have simply signed, can be used against them. In recent years, concern has focussed specifically around personal data. Users of the internet generate, on average, 2.5 exabytes of data each day<sup>[1]</sup>, across a huge range of sites and applications.



**39%**  
year on year increase  
in martech solutions

**5000**  
martech companies by  
the end of 2017

GOOGLE STREET VIEW

**5 million**  
miles of images

**50%**  
iOS apps track location

**600%**  
increase in DuckDuckGo  
searches

90% of all the world's data has been produced in the last two years[2]. Increasingly, consumers are aware that this data is extremely valuable. Many brands use processing systems, including clustering, profiling and targeting, to determine what messages / content / offers they serve to individual consumers. This is partially the result of relatively unconstrained expansion in the martech space. The year on year increase of martech solutions has reached 39%, with more than 5000 companies in the space at the end of 2017[3].

Media hype around data breaches and misuses (including the Facebook-Cambridge Analytica scandal) further highlight the risk of unforeseen implications from allowing brands access to personal data. The giants of data own a huge amount of information: Google Street View has collected over 5 million miles of images[4] and 50% of iOS apps track and store your location data[5]. Concern around data practices is increasing. The exponential increase in traffic to alternative search engines, notably duckduckgo, can be used as a proxy measure for this shift. Queries per day made through the search engine have increased by over 600 times[6] in the past eight years (since launch), with marked increases resulting from specific events including the Snowden revelations.

# 9363

words in the Facebook  
Privacy Policy

# 9851

words in the Book of  
Revelation

## So, what's changed?

The answer is 'not a whole lot'. There is little evidence that individuals are taking their privacy into their own hands. For example, there has been no significant decrease in Facebook usage since Cambridge Analytica was in the news[7]. It seems that taking the time to learn what personal data a brand collects, and what precisely they do with it, is a greater pain point than any resulting issues in data use. This is unsurprising, given that the Facebook Privacy Pages contain 9363 words. For comparison, that's as long as the Book of Revelations. A recent study found that after sitting down to read social media policies, participants changed their use of their personal accounts: 35% used Facebook less and 30% used Google less[8]. These numbers tell you that, even though consumers aren't reading the policies, they absolutely care about what is in them.

The GDPR acts as a line of defense for consumers that takes the burden of making sure data practises are fair, away from individuals, and puts it squarely on companies. The legislation builds on the Data Protection Act of 1998 and the Privacy and Electronic Communications Regulations (PECR), which highlights just how overdue this latest development in data privacy is. In 1998, broadband was just starting to make an appearance in homes, and Google had just been founded. It's fair to say that the world of technology has come a long way since then. Next, we're going to look at the restrictions the GDPR brings to bear on automated processing, and how it impacts individual users.

**AFTER READING:  
THE PRIVACY  
OF POLICY**

**35%**  
OF people used  
Facebook less

**30%**  
OF people used  
Google less



# The GDPR: Significant Impacts

*How do you define significant?  
How does your customer define it?*

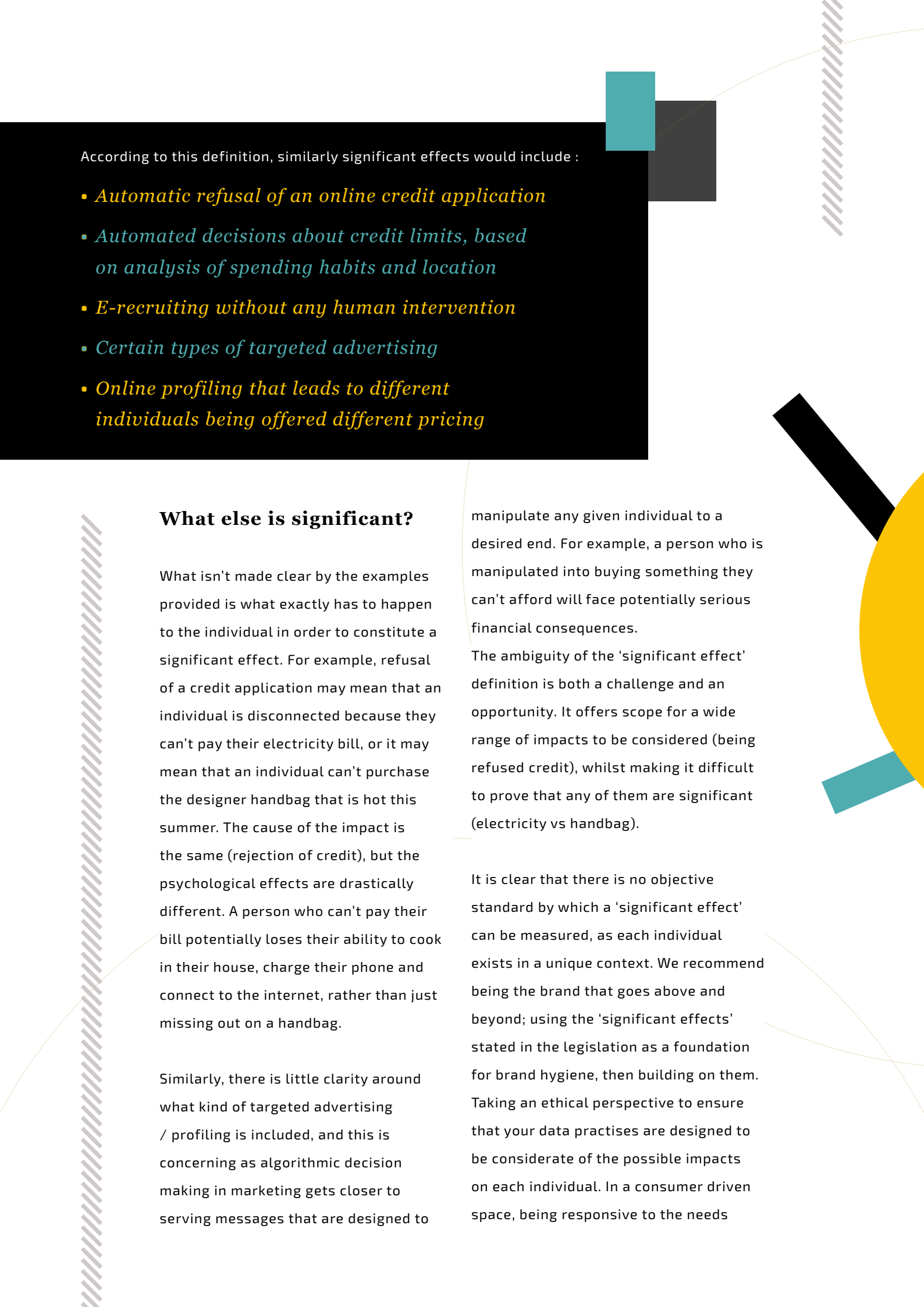
**We know, bear with us.**

Article 22(1)[1] of the General Data Protection Regulation addresses artificial intelligence (AI) in the form of automatic processing, and it states that any person — the data subject — has the right:

*“Not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her”*

Setting aside the legal effects, we will focus on the definition and implications of that which would constitute a ‘similarly significant effect’. The Article 29 Data Protection Working Party (WP 29), working together with the EU data protection authorities, have adopted the Guidelines on Automated Decision Making[2], which offer the following broad definition:

*“For data processing to significantly affect someone the effects of the processing must be more than trivial and must be sufficiently great or important to be worthy of attention”*



According to this definition, similarly significant effects would include :

- *Automatic refusal of an online credit application*
- *Automated decisions about credit limits, based on analysis of spending habits and location*
- *E-recruiting without any human intervention*
- *Certain types of targeted advertising*
- *Online profiling that leads to different individuals being offered different pricing*

## What else is significant?

What isn't made clear by the examples provided is what exactly has to happen to the individual in order to constitute a significant effect. For example, refusal of a credit application may mean that an individual is disconnected because they can't pay their electricity bill, or it may mean that an individual can't purchase the designer handbag that is hot this summer. The cause of the impact is the same (rejection of credit), but the psychological effects are drastically different. A person who can't pay their bill potentially loses their ability to cook in their house, charge their phone and connect to the internet, rather than just missing out on a handbag.

Similarly, there is little clarity around what kind of targeted advertising / profiling is included, and this is concerning as algorithmic decision making in marketing gets closer to serving messages that are designed to

manipulate any given individual to a desired end. For example, a person who is manipulated into buying something they can't afford will face potentially serious financial consequences.

The ambiguity of the 'significant effect' definition is both a challenge and an opportunity. It offers scope for a wide range of impacts to be considered (being refused credit), whilst making it difficult to prove that any of them are significant (electricity vs handbag).

It is clear that there is no objective standard by which a 'significant effect' can be measured, as each individual exists in a unique context. We recommend being the brand that goes above and beyond; using the 'significant effects' stated in the legislation as a foundation for brand hygiene, then building on them. Taking an ethical perspective to ensure that your data practises are designed to be considerate of the possible impacts on each individual. In a consumer driven space, being responsive to the needs



of your customers, allowing them to tell you which clauses in a complex agreement matter to them, is a great way to foster better relationships and build trust with individuals.

Our take here on 'trust' is expressed by a quote from a paper co-written by three of the authors of this paper: "trust is personal and idiosyncratic and can only be understood via the perspective of the user." (Dwyer, Basu and Marsh, 2013)[3]. An expanded definition of an 'effect', therefore, would be

*'The result of a breach of trust'*

And a 'significant effect', for the purpose of evaluating the impact on an individual, would be:

*'A breach of trust that has an impact upon an individual which is outside the scope of the understood agreement between the individual and the data processor.'*

There's one person at any party who will happily tell you why you're wrong on any subject, even one in which you have a PhD, by aggressively wielding the phrase 'well, actually...'. Don't be that person. Read your own terms and conditions, work out what exactly your customers understand it to mean, and decide if your data practises are in breach of that, rather than focussing on technicalities and loopholes.

## Beyond the GDPR

In theory, the GDPR panic should be over. Brands should be compliant (phew), or else resigned to paying the hefty fines for breach of legislation. However, it is critical to remember that this isn't the only piece of data privacy legislation up for review in the coming years (the Cookie Law looks likely to be next on the chopping block). Given this, being beyond compliant becomes a strategy for long term survival. The aim is to use this period of flux to establish data practises that will be watertight, whatever shape the new updates take.

The end-game for automated decision making is transparency. In cases where an algorithm is able to debate and stand for the decision explaining the factors behind it, there is accountability as well as a reduction of uncertainty. The sense here is that even if the individual does not agree with the outcome (of the automated decision), given the parameters and reasoning used for the decision, the individual is less likely to feel mistrustful of the interaction, and the brand, as a whole, resulting in an overall reduction of uncertainty. Building transparency into your communications with customers will create a sense of resiliency in a turbulent environment.



# What Can You Do To Build Trust?



*Looking to make your brand name future proof.*

Most of what brands can do, to address the change in consumer perception, is build reliability through various measures, called "trust cues". These allow people to take shortcuts in interactions, providing them with enough information to decide whether or not to trust, without overwhelming them. However, in the case of digital contracts in the form of terms and conditions, the detail is often provided in its entirety and is often immensely time consuming. For example, it takes 9 hours[1] to read the Amazon Kindle conditions in full.

Trust in digital interactions is predominantly blind, as people expect to be able to take the shortcuts and consequently tick the box without engaging with the content. As a result of this, a power gradient is created by the disparity of information. Decreasing the power of the individual, whilst increasing the power of the company, creates uncertainty and makes it challenging for an individual to identify a breach of trust, and the cognitive dissonance this creates may contribute to an individual becoming more unwilling to trust future interactions.

## That is not my dog

To illustrate this, we can take the physical world interaction of asking someone whether or not their dog bites. A true answer to the question might be 'no, not normally, though, once, on a Tuesday in June, several years ago'. The amount of detail in this answer is confusing, and it places the person who wants to trust the owner in the odd position of having to decide whether or not the dog poses a risk to them, for themselves. This highlights the fact that, in this interaction, we generally expect the owner to make that decision. We expect them to say 'yes' or 'no', and we treat the short form answer as a trust cue. It reduces the complexity of the situation, expresses the opinion of the owner, who has the most information, and allows all participants to focus on what matters.



We would also expect to be able to hold the owner responsible for the consequences of the interaction, as in the famous Pink Panther sketch: 'Ouch! I thought you said your dog did not bite?' 'That is not my dog'. In this case, it is reasonable to suspect that the hotelier who said their dog did not bite deliberately obscured the truth so the inspector would get bitten, but he cannot be held responsible for the outcome because it was not, in fact, his dog.

## Trick or trust?

The feeling of having been tricked creates a deep sense of mistrust, both in the individual (the hotelier) and in future similar scenarios. This is called a 'moment of truth', which is when somebody feels a moment of clarity in association with a particular person, organisation or scenario (Laukkonen et al 2018)[2]. The moment is usually accompanied by a feeling of confidence and it is very difficult to reverse the opinion of an individual once the decision has been made. In the case of digital contracts, the amount of time that needs to be invested to fully explore them amounts to expansion to absurdity.

Organisations place the burden of trying to understand the terms on individual users, despite the fact that the user may not have an adequate legal background which would enable them to do so. However, in a post-trust market, tick boxes no longer constitute adequate trust cues. The mistrust that users feel when being presented with the terms and conditions cannot currently be addressed by the individual, but it can be addressed by the companies.

By defining a significant effect as a breach of


trust which is outside the scope of the understood agreement, (it isn't a Tuesday in June, but the dog still bites), we can reasonably assume that such a breach would be a misuse of power along the gradient (the owner has more information than the enquirer), and we can establish what would be required for a contract to be considered accessible for an individual trust assessment.

- *First, it is the responsibility of those with more information (who are therefore higher up the gradient), to design processes that are worthy of consumer trust*
- *Second, the consumer perception of a process designer will be improved if they (the consumer) are moved up the gradient. It is therefore in the interests of the designer to reduce the information disparity*

## Design to empower

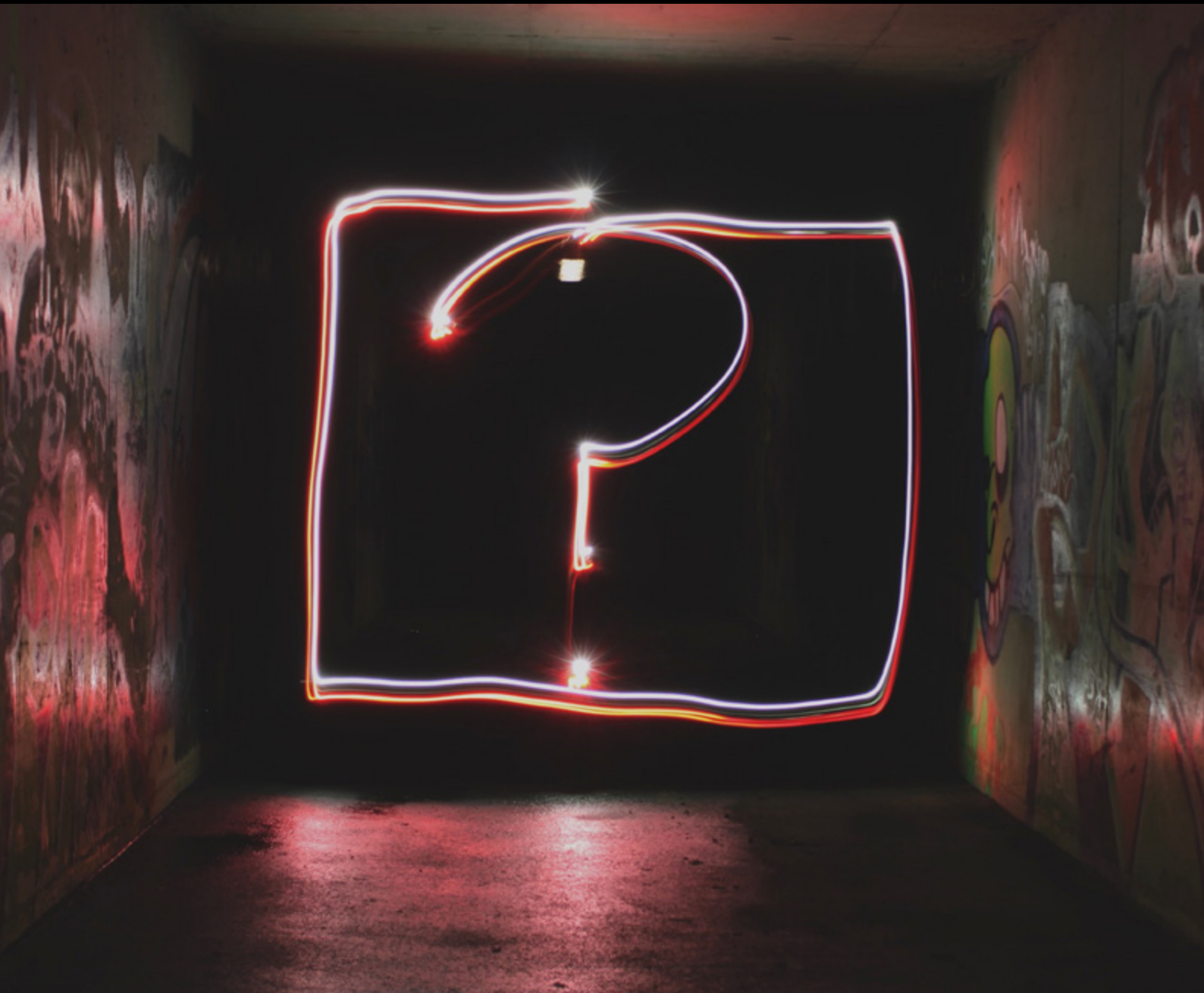
With this in mind, we argue that processes should be designed in such a way that they are trust empowering, instead of trust enforcing. This means that brands should focus on developing clarity in their interactions with consumers, focussing on making clauses surrounding data use explicit, so that individuals can make their own decisions about engaging, according to what matters to them.

In the next sections, we will look at who is currently winning the trust game and why, how brands can build trust into their processes, and how they can change consumer perceptions through contact founded in equal value exchanges. We will also identify tools that will allow both brands and consumers to place trust in digital interactions involving exchanges of data.



# Reputation and Legislation

*Just in it for the soundbites? Skip ahead to 'Empowering Trust' to get the answers before we dive into the questions.*






# Who Do You Trust?

*Looking to make your brand name future proof.*


**T**he 2017 Ipsos MORI Veracity Index<sup>[1]</sup> revealed that nurses are the most trusted professionals in the UK, whilst politicians are the least trusted. It's not likely that anyone will feel particularly surprised by that news. What is interesting, however, is why this is the case. Trust is a perception, often shaped by idiosyncratic ideas that draw information from a variety of places, including our past experience and what others find acceptable. In the case of politics, it is often individuals that give the vocation as a whole a bad reputation. The behaviour of specific politicians during the Brexit referendum, for example, amounted to the deliberate propagation of misinformation and heavily impacted the public perception of the entire process.

## **Flying high: Trust in airlines**

Digging deeper into trusted industries, we can ask; why do travellers (for the most part) trust airlines? The Malaysian Air Flight 370, which went missing in 2014 on a journey between Kuala Lumpur and Beijing, was a global news story which highlighted what happens when the technology fails. Months later, the airline's flight MH17 was shot down over Ukraine, with many blaming pro-Russian forces. Despite these two disasters in quick succession, consumers continue to buy tickets with Malaysian Air. The company considered rebranding, but were warned off it on the basis that the public would see through the superficial changes, and regard it as an admission of not having committed to more extensive reform.







Resnick concludes that the answer to the problem is to put mechanisms in place that engender commitment to non-changing identities within a system, reducing the likelihood of new identities being punished due to suspicion. In a simple reputation system, in which the barrier to identity creation is low, an attacker can create multiple benign looking identities that are centrally controlled with only one malicious motive. This is called a Sybil attack, and public knowledge of this kind of approach (encountered commonly through fake social accounts), creates distrust around new identities.

## Corporate identities on shifting sands

### The value of continuous identities

Long-term and strong identities are likely to be more trust empowering, even with swings in their reputations, than continuously changing identities. Regarding digital identities, Resnick (1999)[2] writes that;

*“Even in the physical world, name changes have always been possible as a way to erase one’s reputation. The Internet highlights the issue, by making name changes almost cost-free. This creates a situation where positive reputations are valuable, but negative reputations do not stick.”*

We cannot know what the outcome of creating a new identity for Malaysian Air might have been, but what is clear is that travellers are still making bookings with the airline. It is possible that this is based on convenience and practicality, as there are only three airlines on the AUS-KUL route, and the other two are budget services.

This is reminiscent of Deutsch’s evaluation of The Lady and The Tiger (1973)[3]. In deciding between two doors, one which hides a lady and the other a tiger, a prince chooses the door indicated by his lover. What motive could he have for this? Is it an honest expression of trust in his lover? Is it fatalism resulting from having no reason to choose the alternative? Is it ignorance of consequences, or simply impulsiveness?

The fable does not reveal the answer, but it does highlight the various reasons people having for



electing to place trust in an interaction. In the case of the airline, and of others that have managed to recover from similar disasters, it is likely that trust is a combination of lack of alternatives and belief that the industry is heavily regulated.

If you have concerns about a particular airline or flight, there are a number of authorities that you can turn to. Among them are government watchdogs, including the UK Civil Aviation Authority, industry monitors, including the Jet Airliner Crash Data Evaluation Centre (JACDEC), which publishes annual airline safety rankings, and independent watchdogs like Air Passenger Focus, which represent and support passengers.

In this sense travellers have yielded their trust making decisions to external

agencies, relying on identified experts to monitor, reward, and hold accountable all actors in the space. This is a sign of the maturity of the aviation sector; individual consumers no longer need to either understand the science of aviation or have complete knowledge of a flight provider in order to expect certain standards.

Autonomous planes would be an apparently obvious next step, as the human component could be completely replaced by algorithms trained to act in specific circumstances. However, one of the arguments against this is that the inclusion of a human pilot is critical because they understand that the consequence of failure to successfully fly the plane could be their own life. As was demonstrated by the Paris airbus crash (1988), an algorithm which prevents human intervention (because pulling out of the steep dive would have put strain on the structure of the plane), the outcome can be disastrous, (the plane crashed and all lives were lost). Leaving room for human creativity in marginal cases will be critical as we move towards a world governed by algorithms.



# Trust In The Digital World

***‘Trustless’ is trendy, but it isn’t the only solution***

**I**n the digital space, particularly in the many fields which fall under the umbrella of AI applications, wider public perception seems to be that no such trusted network of authority figures yet exists. Issues can be reported to privacy commissioners and other similar regulatory bodies, but there are questions regarding to what degree these entities can adequately regulate the sector.

Media hype around large corporations facing charges often results in reports of fines that seem to have no impact on their market share. Google was fined €2.4bn[1] by the EU in 2017 over manipulating search engine results, but the consumer facing impact has been minimal. The GDPR can be seen as a step in the direction of providing a foundation for accountability across the sector.


However, as the legislation is new it will take time to see the full effect both in terms of successful action against corporations and with regard to impact on public perception. Given, then, that the sector is very much still in its infancy, and faith in authorities has been extensively undermined, by the failure of traditional institutions, politicians declaring that we are tired of experts, media hype surrounding movements like ‘fake news’, and large corporations undermining faith in authority, who can consumers rely on?

## **Decentralised networks and ratings**

Enter, stage left, distributed trust networks.

Dunbar’s number[2] is a rule which states that any individual can only successfully maintain ‘name-to-face’ relationships with up to 150 people. As the relationship between individuals becomes closer, the number of people that you can successfully maintain relationships with decreases. However, online, consumers are relying on people they have never met to identify, rate and remove rogue actors from a given system. You can see this happening live as brands display their TrustPilot reviews front and centre, and startup unicorns like AirBnB and Uber build interpersonal trust through simple rating systems.

Critically, it isn’t trust in one person, but in the ‘wisdom of the crowd’. High reviews aren’t enough, however; the pillars of trust in the digital sphere are context bound. For example, in the case of AirBnB, ratings are based on overall experience, cleanliness, accuracy of listing, value, communication, arrival and location. These reflect the most important concerns of hosts and guests. Similarly, on the darknet, traders of substances are rated based on their ability to disguise products successfully, package them securely and deliver on purity.





## If only it were a perfect world

There are a few roadblocks in the rating system, for example, they can be gamed, as paid Amazon reviews have demonstrated, or a small sample size might present a clustering issue, as seen offline in the spreading of rumors in small communities, but these are often identified as anomalies over time. If a provider has high ratings but doesn't deliver the service, eventually they will be ousted by the wider community.

The signs of trust are a 'moving target'. Once a certain behaviour or symbol becomes associated with trust, there are some who attempt to emulate the trust sign to gain the trust of others, without, of course, acting in a trustworthy manner. An example can be found in the human resources industry. Human resources workers receive training to spot when job candidates are presenting fake signals. The candidates, through word of mouth, know about what trust signals to present and attempt to mask any negative signals (Möllering 2008)[3].

We need to note here that the ousting of rogue actors relies on the assumption of an initially 'perfect' environment of free agents. If, for example, an individual lived in a location where criticism of rogue actors could result in being penalised by the state or even non-state actors, the malicious parties are much less likely to be eradicated from the system. Any cluster of malicious actors would then be able to conspire freely to present an apparently high rating (gathered from other actors with the same malicious objective), repeatedly tricking individual, harmless entities, who may not trust the ratings against themselves, but would be unable to share the knowledge and prevent others from being targeted.

Factors that would contribute to the creation of such an environment include community pressure to abide by social norms (and not report negative interactions). Scandinavian Janteloven[4] (Jante Law) is an example of this kind of structure. The unofficial laws include the following ten rules, which form the basis for socially stigmatising people who break them:



# Jante Law

You're not to think you are anything special.

You're not to think you are as good as we are.

You're not to think you are smarter than we are.

You're not to imagine yourself better than we are.

You're not to think you know more than we do.

You're not to think you are more important than we are.

You're not to think you are good at anything.

You're not to laugh at us.

You're not to think anyone cares about you.

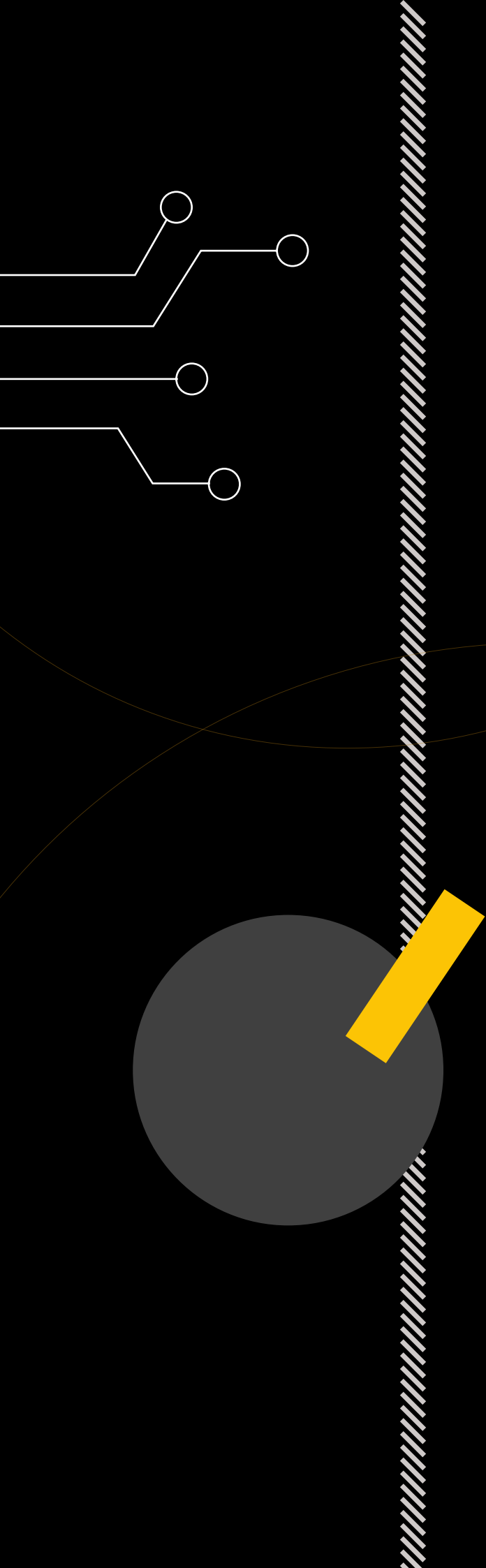
You're not to think you can teach us anything.



The ominous eleventh rule, known as the Penal Code of Jante, is:

**Perhaps you don't think we  
know a few things about you?**





As the author of the laws, Aksel Sandemose, wrote:

*“That one sentence (the eleventh rule), which acts as the penal code of Jante, as such was rich in content. It was a charge of all sorts of things, and that it also had to be, because absolutely nothing was allowed. It was also an elaborate indictment, with all kinds of unspecified penalties given to be expected. Furthermore it was useful, depending fully on tone of voice, in financial extortion and enticement into criminal acts, and it could also be the best means of defense.” (A Fugitive Crosses His Tracks, 1933).*

Social conventions are just one contributing factor to imperfect environments. Others may include the ineptitude of regulating bodies, the political power of organised criminal groups, and the victimisation of specific individuals. Designing mechanisms that empower users to overcome these imbalances, without putting themselves at risk, is critical.

One instance of this is the fear of reprisals. With regard to the platform, this issue necessitates preservation of anonymity of individuals who report their observations to a reputation system. Reporting models could also allow edits, as long as the history of their reports are visible to ensure transparency. The anonymity must be preserved at the system level so that no system designer or administrator can reveal the identities of the users if asked to do so.

## Ratings as trust proxies

Returning to the notion of ratings as trust cues, a high rating might be 9 out of 10, and objectively that looks great, but it is irrelevant without context. Brands should not say that an individual can trust them simply because of a high score, but rather that they can be trusted because the system's performance in previous interactions by some measure has a high score, (such a measure could be reputation). The individual may choose to use this information to decide whether to trust the system in a certain context in the next interaction.

Through the creation of crowd sourced trust cues, including ratings, consumers have, as in the case of airlines, offset the pressure and personal responsibility for making decisions regarding who to trust. It is critical, however, that brands build trust (or expectation management) into their mechanisms from the beginning, so that they can survive negative press and technological failures.

The friction between convenience and privacy adds a fascinating dynamic in the digital case. For example, despite the Cambridge Analytica scandal, there hasn't been a significant drop in the number of Facebook users. It could be that this is attributable to the fact that users are familiar with Facebook's

business model, and have grown to expect to trade their privacy for service.

## Who is winning the game?

The winners in digital trust are brands that use transparency as a base mark, and then consistently curate positive sentiment within their consumer base, by managing expectations and eliminating rogue actors quickly.

Rogue actors don't need to be malicious external users, there can be corruption at any point in the chain. For example, in 2011, Jack Ma, founder of Alibaba, had to deal with a large scale internal corruption scandal. His salespeople were cheating thousands of foreign merchants, and use of the platform was likely to plummet if he didn't act fast to restore trust. Within a week he had fired 100 culpable individuals[5].

This rapid elimination allowed other users to keep the faith in the system as a whole, and stabilised the issue. Given that this quick, transparent, action, founded in a solid ethical basis and delivering on that promise, appears to be the winning formula, how can you design your processes to secure trust in the first place, and how can it be maintained through consumer perception? The answer is simple; be inherently trustworthy, apologise if it goes wrong, and act quickly according to your ethical code.



# Designing For Digital Trust

*Exploring digital networks and mechanisms for creating trust*



One of the challenges for trust cues in the digital space is that online platforms are not always the best location for trust networks. A 2017 case, brought against Uber India by Jane Doe[1], is a clear example of this. A woman who was raped by an Uber driver was publicly promised full support by the company. However, behind closed doors, former executive Eric Alexander allegedly obtained the woman's medical records and attempted to use them to cast doubt on her credibility.

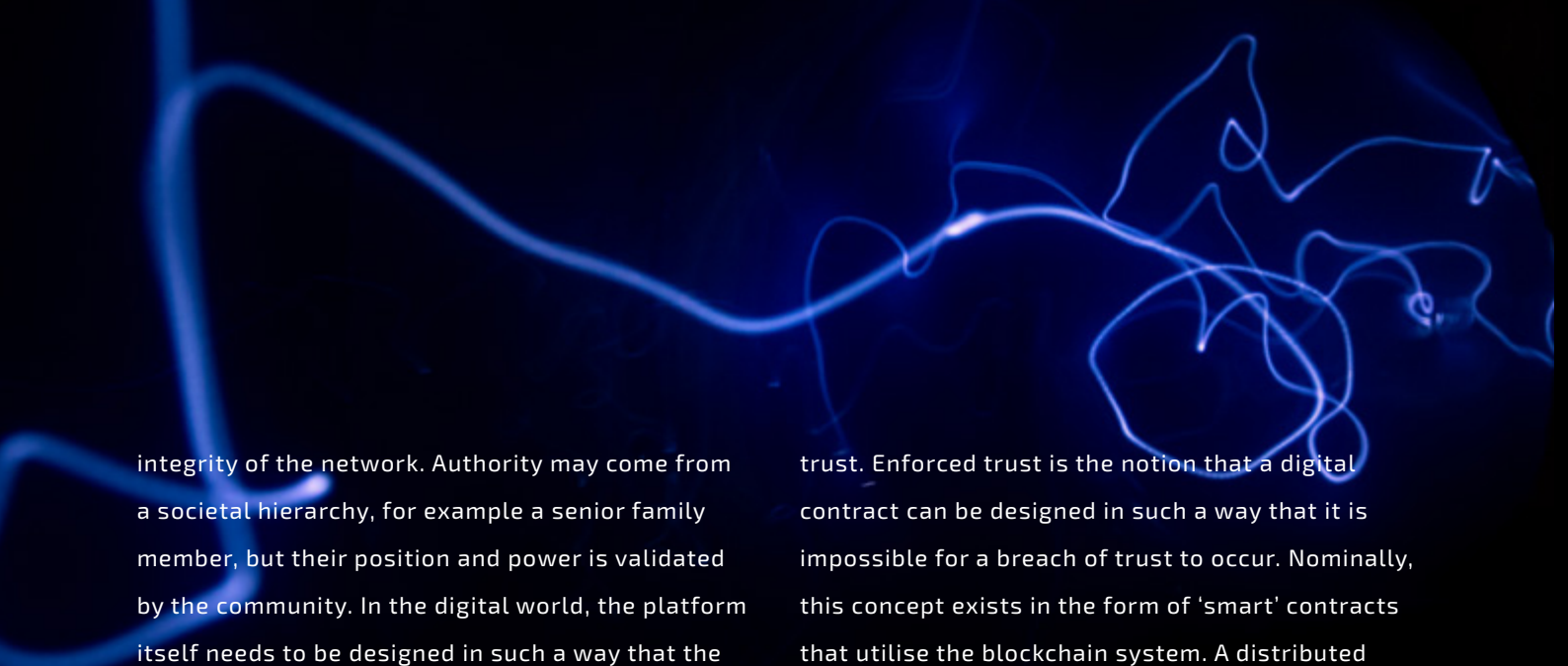
The character assassination included claiming that the woman was part of a conspiracy by a rival firm to damage Uber's reputation. This is an example of the corruption of a trust network that is being hosted on a digital network. Prior to Uber and the like, ride sharing platforms (in India as well as more widely), were often local.

## Computation in networks: local vs digital

Suppose Alice has a car, which she drives and can be hired as a rental car and driver. The way Alice used to get clients was through neighbourhood and local recommendations. Bob may have used her car before; or Charlie or Eve may know her family. Thus, when Dave from the neighbourhood wanted to use Alice's service, there was an offline, very established web of fully decentralised trust in place to help him decide. Bad reputation stories spread quickly, and could put Alice out of business within months. Even relatively less serious things like "lack of punctuality" would stick with her name and her implicit brand forever.

In this instance, the offline network of immediate connections is more successful at controlling rogue actors, whilst retaining the





integrity of the network. Authority may come from a societal hierarchy, for example a senior family member, but their position and power is validated by the community. In the digital world, the platform itself needs to be designed in such a way that the possibility for corruption of any participant, from the platform hosts, to service providers and the end users, is reduced to the greatest possible extent.

Additionally, It is necessary to ensure that the individuals who report their observations are indeed entitled to do so, e.g, a person who has purchased a particular item listed on an online shop is allowed to report any issues, but someone who has not made a purchase cannot make the same report. The constraint to ensure that the reports are made by authorised users may be satisfied through zero-knowledge proof systems.

Considering again the example of older car and driver hire models, this would allow criticism without fear of reprisal from authenticated members of the network, the only missing aspect is the social connections. Brands could go further in offering cues for trust empowerment by allowing users to access a social network graph, enabling them to understand their relation to those who have submitted ratings.

## Doing it the decentralised way

The focus on transparency brings us back to the distinction between enforced trust and empowered

trust. Enforced trust is the notion that a digital contract can be designed in such a way that it is impossible for a breach of trust to occur. Nominally, this concept exists in the form of 'smart' contracts that utilise the blockchain system. A distributed ledger system is an example of a decentralised network, in that there is no central authority responsible for maintaining a mutually agreed record of events. Instead, the consensus protocol in a distributed ledger helps define a 'trustless' environment, which collates information, typically into blocks, and chains them together using cryptographic hashes and signatures.

The 'trustless' argument is only there to distinguish these from traditional public key infrastructure based systems where the validity of signatures and the information depends on the trust on one or more central authorities, such as a root certificate agency. In a distributed ledger, the record of transactions is held by multiple members of the network, making it more difficult to corrupt than it would be if it was held by some centralised entities. Adoption of the technology is continually increasing, with McKinsey predicting commercial deployment of the technology at scale by 2021[2].

## Smart (and not-so-smart) contracts

Smart contracts are digital agreements which are coded on a blockchain. It is proposed that using this tool allows users to eliminate middle men, trusting the code to define the rules and penalties around a transaction, as well as trusting it to enforce them.



For example, there might be a network for selling unwanted live event tickets, and the code would automatically refund the purchaser if the ticket wasn't delivered within the agreed time frame, without the need for a third party. In the context of personal data contracts, to borrow the words of Jeremy Epstein, CEO of Never Stop Marketing[3]:

*“In a blockchain world, marketers will have to earn customer permission in an entirely new way. Identity will be controlled by the users.”*

Identity control is inextricably linked to data ownership. A study by the DMA[4] found that consumers are most incentivised to share personal data with brands when they receive tangible benefits and control over their data. Blockchain gives them the power to choose how they interact with brands, and the ability to dictate what precisely constitutes a tangible benefit.


However, the utopia promised by blockchain technologies is not always realised. The advantage of having middle men is that they mediate between parties. A lawyer, for example, is able to argue for you in court, so you do not need to have any legal understanding in your own right to be protected. The challenge with smart contracts is that there is no one to protect individuals from malicious actors or undetected loopholes. There have been numerous examples of smart contracts being manipulated by malicious groups.

For example, the Decentralized Autonomous Organisation (DAO) was a smart contract built on the Ethereum network in May 2016. It was designed to operate as a venture capital fund for the crypto and decentralized space. However, a hack resulted in a total of 3.6m Ether (\$70M) being drained in a matter of hours[5]. Due to the nature of the code in the contract, the attacker was able to ask the smart contract to give the Ether back multiple times before the contract could update its own balance. This issue was the result of the coders not considering the possibility of recursive call (repeatedly requesting the Ether), and the mechanism that delivered Ether before updating the balance.

## **Moving away from enforced trust**

The lack of a third party to act as a mediator or an enforcement authority means that if the system doesn't perform (e.g., due to malicious or faulty code), there is no way to stop the 'smart contract' and recover losses. This very point makes 'smart contracts' invalid in comparison with traditional legal contracts where intervention is built into the mechanism. Furthermore, with this sort of trust enforcement, while the user does not need to trust any single central authority in charge of running the smart contract code or maintaining the information on the distributed ledger, there is still implicit trust on the designer of the smart contract, the code itself and its execution environment, amongst others.





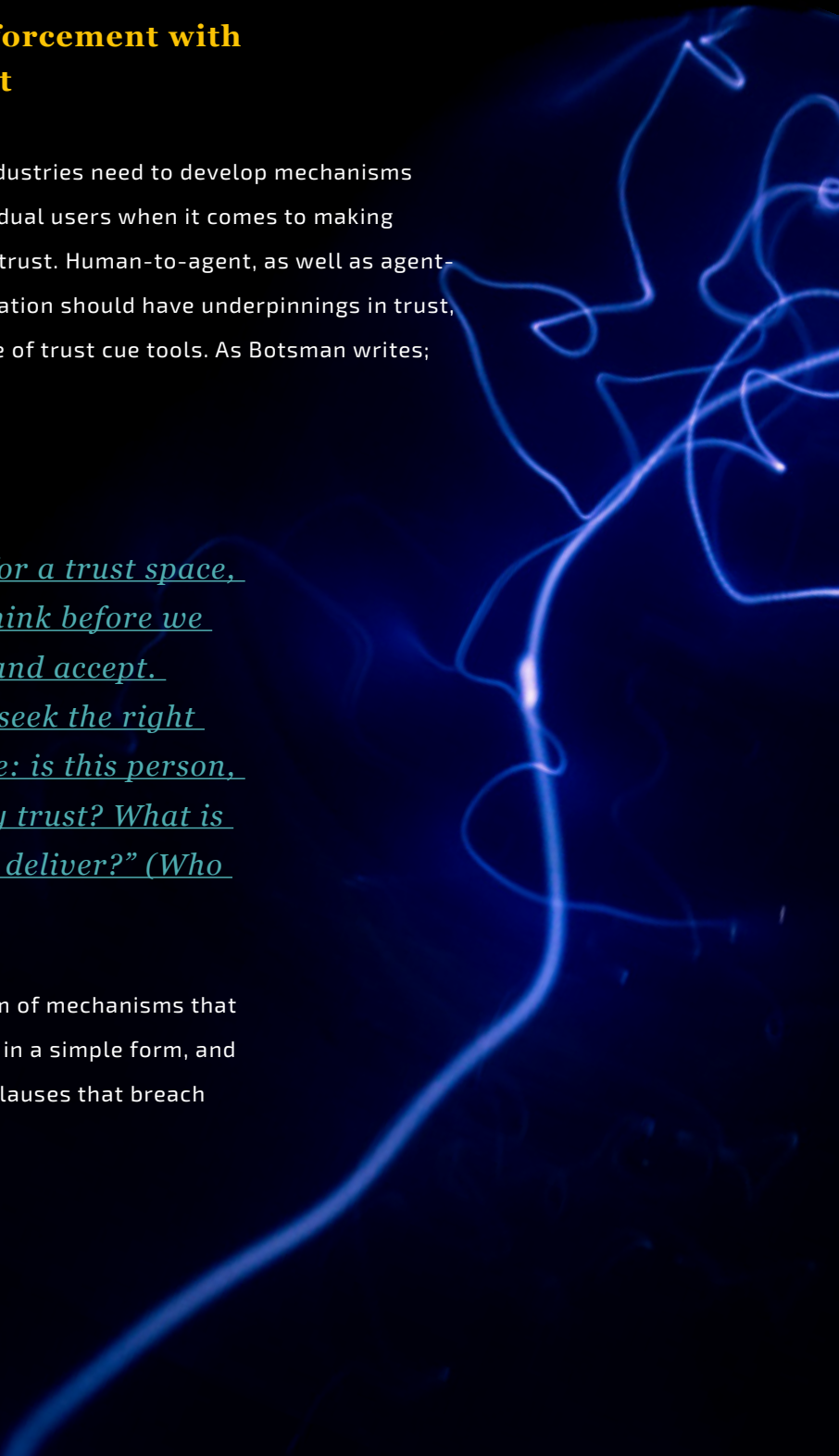
Returning to the aviation example to illustrate this point, punters previously trusted that there were rigorous processes, being run by experts, which monitor, evaluate and, if necessary, punish airlines and compensate individuals when things go wrong. The spate of recent flight disasters has shaken this faith, forming part of a perceived global mistrust in authority and expertise. Enforced trust, even through traditional authority, is no longer a practical solution.

### **Replacing enforcement with empowerment**

Brands across all industries need to develop mechanisms that empower individual users when it comes to making decisions regarding trust. Human-to-agent, as well as agent-to-agent, communication should have underpinnings in trust, derived from a range of trust cue tools. As Botsman writes;

*“Distributed trust needs to allow for a trust space, an interval in which to stop and think before we automatically click, swipe, share and accept. To ask the right questions, and to seek the right information that helps us to decide: is this person, information or thing worthy of my trust? What is it that I am trusting them to do or deliver?” (Who Can You Trust? 2017).*

Such trust spaces could be offered in the form of mechanisms that allows users to establish their own priorities in a simple form, and automatically scan any digital contracts for clauses that breach their personal preferences. (Basu, et al. 2016).



# Cross-sector Best Practises

*Profiles of brands that  
are racing ahead.*

## easyJet

Easyjet are doing a great job regarding transparency and inclusion in response to the GDPR. Their educational video<sup>[1]</sup> opens with the line 'we know that our privacy policy may not be the most interesting subject in the world, but keeping you, and your personal information, safe is important to us. So, we've made a little film, to help explain our privacy promise.' The video goes on to state that Easyjet promises to be open, regarding the use of personal data.

The content distinguishes between different kinds of data; that which is necessary to board the plane (name, email, destination and sometimes passport info), that which is necessarily shared with other organisations (including border control, airport security and ground crew partners), that which enables an additional opt in service (including providing a mobile number, or downloading the app), that which enables service improvement (including preference data and information from feedback mechanisms), and that which is used to provide targeted marketing (including third party packages and special offers).

This tiered approach to data use, providing clear consent opportunities at every level, makes it easy to understand how personal data is used by an airline. Interestingly, the graphic style of the video provides visual clues which are designed to demonstrate that each data transaction is inherently valuable to the consumer. For example, a parent watching the video, who has experienced the stress of travelling with a family, would feel that the message about 'data for additional services' resonates with them because a crying child is shown being looked after by an Easyjet staff member.

Easyjet also make it clear that an individual can change their privacy settings at any time, providing a feeling of security in the present as the opportunity to leave the contract remains. The 'right to be forgotten' is a legal requirement under the GDPR, but presenting it here as if it is part of the brand's ethos, is a relationship building tactic.



### **Digisafe**

What Easyjet doesn't offer, in their GDPR video, is decision making support for their consumers. A short advertisement video[2] from Barclays Digisafe is pushing a service which is designed to educate consumers regarding mechanisms that will allow them to take control of personal data online. They offer a definition of personal data, examples of where consumers are currently giving it away, a data dictionary of common terms, and directions for retrieving ownership.

There are also interactive challenges, designed to highlight behaviour that indicates misuse of data. The vishing challenge (voice phishing) is a recording of a call between a consumer and a fraudster pretending to be a bank. The player needs to hit the 'alert' button, whenever they detect suspicious activity. There are points available for not giving the fraudster your bank pin.

Interestingly, there are several other indicators of malpractice, including the caller saying 'I'm calling from your bank', rather than being specific about their affiliation, which are not highlighted as problematic by the designer of the challenge. This goes some way towards emphasising our argument that trust is entirely subjective. Overall,

however, this tool is a great way of making sure that consumers can not only access and understand the relevant information, but are also supported in developing their understanding and making personal decisions regarding trust.



### **Mozilla Firefox**

Brands are hitting the hygiene marks for trust and privacy once transparency and inclusion are at the heart of their approach. Given this, gaining an edge comes down in part to going the extra mile in the name of building meaningful relationships with consumers. Mozilla Firefox is a great example of this. They offer continual opportunities for dialogue, acting quickly on responses from their active community base. When they run data experiments, they blog[3] about how participants are selected, they actively offer the option of refusal, they seek permissions continually, and make the code they run in experiments publically available.

They also list the data practises for each experiment individually, for example, participants are given a random ID for the experiment that is not associated with any other identifier. By offering their content up in this way, they encourage interaction and conversation, playing into their consumers' desire for co-creation. Through these mechanisms they are enabling accessibility,



but without compromising on user privacy or autonomy. They keep data and processes sensitive by, for example, making only code run on raw data available.

### **The champion formula**

The winning formula for brands is, first, to ensure that transparency and inclusion are the foundation for their product / service, and second, to use dialogue enabling tools to get closer to consumers. Identify what engaged consumers want, whether it's the delegating attitude of airline passengers, or the community involvement attitude of tech startups, and create a brand position that is responsive to their desires.

Getting closer, without breaching the trust of a given individual, and supporting them in navigating products and services according to their own priorities, will provide a foundation for fundamentally trustworthy interactions. In the next section, we will identify practical steps that organisations can take to achieve this.



# Conclusion

*If you're the sort of person who looks in the back of textbooks, welcome to the cheat sheet.*





# Empowering Trust

*Designing a new model for success  
in the post-trust world.*

Given our focus on consumer empowerment, it's clear that, in order to achieve this, organisations and brands will need to yield some of their power, distributing it in order to reduce the disparity of information. This brings consumers closer to the processes, and, in theory, puts the owners of the processes at risk of being questioned, caught out and reported. It also supports consumers in deciding that a particular terms and conditions document breaches their personal conditions for trust, and that they therefore won't use a particular product or service.

In these cases, brands may lose customers who would previously have given up somewhere about page 2 of the legalese, and ticked the permissions box. However, whilst this appears to be a threat at surface level, it is also an incredible opportunity for the brands. A brand might lose 75%<sup>[1]</sup> of its subscribed market base, due to GDPR, but those who remain, and those who are acquired later, should constitute an informed and engaged consumer base.

## **Trustworthy to the core**

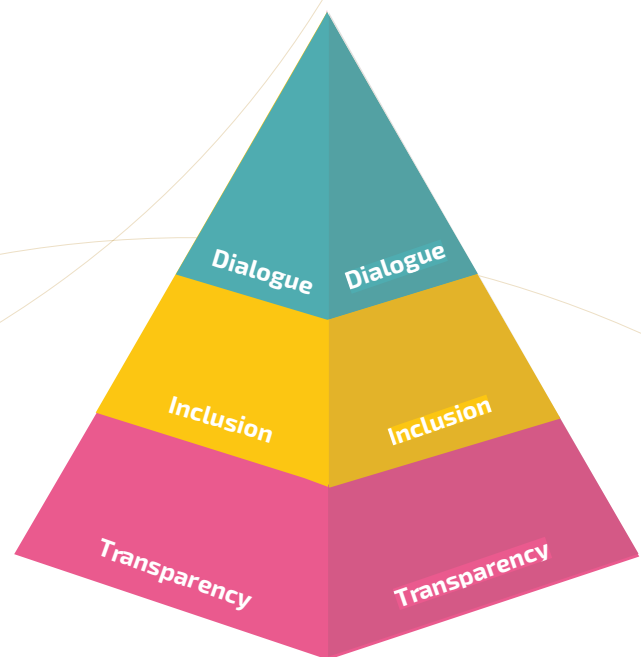
As Glen Urban (2005)<sup>[2]</sup> says, in order to truly trust-enable, organisations must have a trustworthy product/service at the core of their practise. A shift to this culture of trust-centricity matches the longer term consumer trend, and provides brands with a foundation for truly earning consumer trust. However, ensuring that the perception of the consumers changes in line with the brand behaviour is a more nuanced challenge.

The pillars for communication in this space are transparency and inclusion, with the opportunity for dialogue as an additional requirement. Below we have defined these terms in this context:

**Transparency** - Consumers can access information on any contract aspect, including data processing mechanisms, profiling tools etc.

**Inclusion** - The information is made available in such a way that consumers are easily able to understand the terms and conditions, and are supported in making informed decisions regarding their trust priorities.

**Dialogue** - Consumers can query and feedback anything at any point in their journey, and receive timely, accurate and comprehensible responses.



These three concepts form a layered structure. Transparency is a foundational necessity, and often a legal requirement under legislation. Brands have the opportunity to go beyond the legalities, and view the shift in consumer perception as an opportunity to build relationships with individuals. Allowing users to view contracts, supporting them in understanding the processes, creating dialogue with them and involving them in co-creation, makes trust earning a continual part of the relationship.

# Recommendations

*How to start as you mean to go on.*

**T**o close the paper we turn to practical steps organisations can take to build trust in from the start. For clarity, we will discuss them within the transparency, inclusion, dialogue framework that we discussed earlier.

## Starting with transparency

The first key consumer interaction is the initial presentation of the terms and conditions, often in the 'tick this box' format. To achieve transparency, the communication of the contract, as well as of any ensuing issues, needs to be completely clear. Therefore, simplifying your legal and contractual conditions is an excellent starting place. The excuse that - 'the customer should have read it in full' is not a viable justification for malpractice, and any attempt to obfuscate the details through long and complex legalese will be a trust turn off for your customers.

Trust can be earned by adding layers of nuance regarding the implications of a contractual agreement and the intention behind a clause. Why has the business included a particular detail? Naturally, some users are going to be more interested than others, so brands should create an interface that can reveal more detail on request. Allowing users to access as much,

or as little, information as they require to form a basis for trust creates a relationship founded in consideration of users, rather than an antagonistic (power imbalanced) legal stance.

## Building inclusion

Sustaining trusting relationships requires continual attention. Giving consent shouldn't be seen as a one-hit-wonder that gives brands permission to act without further involving the individual. Ideally, consent should be continually given, and users should be able to query any aspect of a brands behaviour at any point.

Brands should build simple interfaces that allow users to question an organisation or service. If users can query why an algorithm has arrived at a particular outcome or recommendation, then they can begin to shape the design of a service. Users know when they are locked out of decision making process, and can sense when the power dynamics are not in their favour. It is a trust turn-off.

Brands should also make updates more engaging. Roll out new work in a way that creates a sense of inclusion, inviting users to interact



with, and review, the changes. This builds an atmosphere of co-creation, a factor which drives long term loyalty and brand resilience, but also ensures that users feel comfortable with any changes.

## Enabling dialogue

Your organisation's marketers need to re-educate themselves, if they haven't already. Marketing was once about a controlled and glossy service, and these goals for a traditionally coherent brand made sense in what now feels like another era. Users are now more exposed to the failures of leaders and companies and are cynical about their placation.


Brands need to find new measures for trust and offer fair value exchanges and returns on investment. Rather than using simple measures that value only when users trust, regardless of whether or not they have been duped, you need

to develop ways to understand more nuanced indicators. For example, do customers feel comfortable raising an issue? Do they know how to ask questions? Such measures are difficult but the investment can create a unique selling point in a saturated market.

An investment in trust means that a company is ready to adapt to new contexts and expectations quickly and stay ahead of other businesses that do not understand new social dimensions. Critically, it isn't enough simply to count trust indicators. Brands need to build feedback modules, and develop a culture of responding quickly to queries, and evolving in line with consumer desires. This shift to a dialogue based model, particularly if it is encouraged between users, as well as directly with a brand, creates a sense of networked trust.



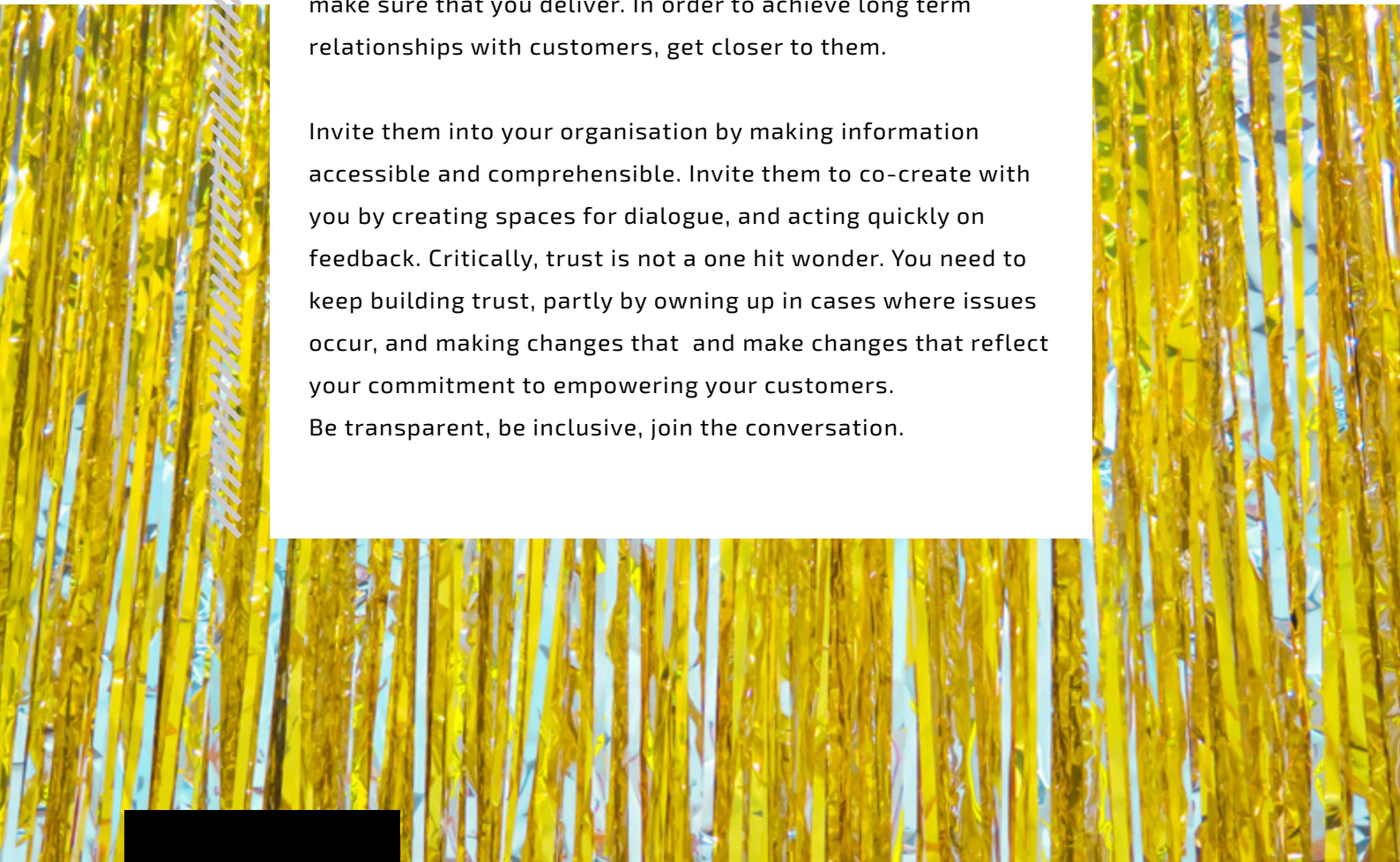
# The Grand Finale



Place trust at the heart of your organisation. Build it into your ethical codes, practises, processes and communications. However, talking in the talk to develop the appearance of trust, without ensuring that you have the tools to deliver on the promises you make, will only result in a negative moment of truth, damaging your reputation in the eyes of even those who are most willing to engage with you.

You can never demand or enforce trust through messaging, you can only earn it based on the subjective decision of your customers. Trust in itself is a confluence between expectations and actualisation. If you, as a brand, raise expectations by offering a relationship to your customers, you need to make sure that you deliver. In order to achieve long term relationships with customers, get closer to them.

Invite them into your organisation by making information accessible and comprehensible. Invite them to co-create with you by creating spaces for dialogue, and acting quickly on feedback. Critically, trust is not a one hit wonder. You need to keep building trust, partly by owning up in cases where issues occur, and making changes that and make changes that reflect your commitment to empowering your customers. Be transparent, be inclusive, join the conversation.





# References

## Introduction

- 1 <https://www.northeastern.edu/levelblog/2016/05/13/how-much-data-produced-every-day/>
- 2 <https://www.sciencedaily.com/releases/2013/05/130522085217.htm>
- 3 <https://www.salesoptimize.com/2017-martech-landscape/>
- 4 <https://www.engadget.com/2012/06/06/google-street-view-20-petabytes/?guccounter=1>
- 5 <https://www.cio.com/article/2460616/mobile-apps/user-beware-that-mobile-app-is-spying-on-you.html>
- 6 <https://duckduckgo.com/traffic>
- 7 <https://www.theatlantic.com/technology/archive/2018/06/did-cambridge-analytica-actually-change-facebook-users-behavior/562154/>
- 8 <https://www.whoishostingthis.com/blog/2013/05/29/internet-privacy-infographic/>

## The GDPR

- 1 <https://gdpr-info.eu/art-22-gdpr/>
- 2 <https://www.twobirds.com/en/news/articles/2017/global/article-29-working-party-guide-lines-on-automated-decision-making-and-profiling>
- 3 Reflections on Measuring the Trust Empowerment Potential of a Digital Environment (Dwyer, Basu and Marsh. 2013)

## What can you do to build trust?

- 1 <https://www.theguardian.com/australia-news/2017/mar/15/amazon-kindles-terms-unreasonable-and-would-take-nine-hours-to-read-choice-says>
- 2 The Eureka Heuristic in Multisensory Identification (Laukkonen and Tangen. 2018)
- Reputation and legislation: Who do you trust?
- 1 <https://www.ipsos.com/ipsos-mori/en-uk/politicians-remain-least-trusted-profession-britain>
- 2 The Social Cost of Cheap Pseudonyms (Resnick and Friedman. 1999)
- 3 The Resolution of Conflict (Deutsch. 1973)

## Reputation and legislation: Trust in the digital world

- 1 <https://www.theguardian.com/business/2017/jun/27/google-braces-for-record-breaking-1bn-fine-from-eu>
- 2 <https://www.theguardian.com/technology/2010/mar/14/my-bright-idea-robin-dunbar>
- 3 Inviting or Avoiding Deception through Trust? (Mollering. 2008)
- 4 <http://www.scandinaviastandard.com/what-is-janteloven/>
- 5 <https://www.forbes.com/forbes/2011/0411/features-jack-ma-alibaba-e-commerce-scandal-face-of-china.html#7acbcd2b4af5>

## Designing for digital trust

- 1 <https://www.theguardian.com/technology/2017/jun/15/uber-india-woman-rape-lawsuit>
- 2 <https://bravenewcoin.com/news/mckinsey-sees-blockchain-technology-reaching-full-potential-in-5-years/>
- 3 <https://www.forbes.com/sites/sap/2017/03/27/marketing-meets-the-blockchain-whats-a-fair-price-for-customer-data/#6b1aae9407a8>
- 4 [https://dma.org.uk/uploads/ckeditor/Data-privacy-2015-what-consumers-really-thinks\\_final.pdf](https://dma.org.uk/uploads/ckeditor/Data-privacy-2015-what-consumers-really-thinks_final.pdf)
- 5 <https://bitcoinist.com/the-explosion-dao/>

## Empowering trust

- 1 <https://www.campaignlive.co.uk/article/gdpr-will-render-75-uk-marketing-data-obsolete/1441738>
- 2 Are the Drivers and Role of Online Trust the Same for All Web Sites and Consumers? (Urban. 2005)

## Cross-sector best practises

- 1 <https://www.youtube.com/watch?v=o199qdIdOso>
- 2 <https://www.youtube.com/watch?v=RszVPiZbPeg>
- 3 <https://medium.com/firefox-context-graph/context-graph-its-time-to-bring-context-back-to-the-web-a7542fe45cf3>