Crowe

Trust and ethics

As trust becomes an increasing factor for the customer, demonstrating the ethics of how data is to be used, managed and protected will become a competitive differentiator.

Neil Currie

In assessing how trust and ethics are a factor, this paper considers a number of assertions affecting both company and individuals' data, covering some of the key regulatory, industry, individual and economic factors. It looks at the forecast trends in data availability, consumption and use that will affect business in the coming years.

Assertions

1. The introduction of General Data Protection Regulation ('GDPR') didn't just bring more regulatory change for companies to deal with and a lot of 'noise' around issues such as 'consent' and privacy notices – it kick-started in many businesses a long-overdue and neglected focus on data protection risks and practices.

2. The business world's current fascination with the potential opportunities for, and risks from, artificial intelligence and machine learning is driving a focus on Data Ethics.

3. Customers are expressing and acting upon their growing expectation of being able to trust the companies they interact with.

4. The link between assertions 1, 2 and 3 will have a direct and increasing impact on customer acquisition costs and the economic value of companies.

5. Going forward, we believe that companies will need to respond to this expectation of trust by providing more tangible, evidence-based, indicators of that trust and how it is being sustained and communicated with customers on this basis.

Assertion 1

“The introduction of General Data protection Regulation (‘GDPR’) didn’t just bring more regulatory change for companies to deal with and a lot of ‘noise’ around issues such as ‘consent’ and privacy notices – it kick-started in many businesses a long-overdue, and how neglected focus on data protection risks and practices.”

The results of the UNCTAD (United Nations Conference on Trade and Development) data protection tracker, last updated in April 2018, identified that 58% of countries had data protection legislation in place and a further 10% had legislation in draft.[1] These numbers indicate a regulatory response to consumers’ growing awareness of their personal information and its value, where it is used, and how it is managed and protected.

As is highlighted in the IBM survey[2] individuals’ behaviours and choices will likely reflect the trust they place in other parties. The increase in data protection regulation and the current frequency and visibility of data breaches is making companies aware of the need to protect their relationship with customers by upping their game in the areas of cyber protection, data retention and governance regarding the data they use, hold and manage.

Moreover, considering the risks related to their third parties, and aware that their reputation with customers is affected by their choices about who to do business with, companies are becoming more careful in choosing their suppliers and partners, and are implementing more formalised third party risk management processes.[3]

As next-generation technologies continue to proliferate, data protection legislation has sought to further protect the trust and rights of individuals by granting specific powers to them in respect of decisions made through automated processing. In other words, when an organisation employs automated systems in the decision-making process based on individuals’ personal data, the legislation gives to those individuals the right to request the review of such decisions. In this environment, demonstration by companies of the ethical basis for their decision making processes will influence customers’ trust, behaviours and actions.

A simple example of this hypothesis could be an examination board that uses an automated system to mark multiple choice exam sheets, and whose system is programmed with the correct answers required to achieve pass and distinction marks. Scores are attributed automatically to the individuals based on the number of correct answers and the results are then made available online. In such a scenario, if the candidate believes there is an error in the outcome of the exam, they can request the examination board to provide a different evaluation, reassessing the test using human review and judgment.[4]

In a recent paper published by the European Union on Research and Innovation the opening statement is “Data protection is both a central issue for research ethics in Europe and a fundamental human right. It is intimately linked to autonomy and human dignity, and the principle that everyone should be valued and respected. For this principle to guide the development of today’s information society, data protection must be rigorously applied.”[5]

This principle is embodied within the GDPR, and the ‘avalanche’ of new and updated data protection legislation now rolling across the globe highlights the increasing focus on the ethical basis for companies’ activities and their decisions being based on data.

Assertion 2

"The business world's current fascination with the potential opportunities for, and risks from, artificial intelligence and machine learning is driving a focus on Data Ethics"

A recent Gartner survey highlights that despite the fact that artificial intelligence ('AI') will accelerate and broaden across all types of business functions and industries, it will continue to be limited by its ability to reliably discern truthful content from false information. "Through 2020, AI-driven creation of "counterfeit reality", or fake content, will outpace AI's ability to detect it, leading to digital distrust. Moreover, by end 2021, more than half of digital banking initiatives will fail due to their inability to deliver an authentic human experience that customers trust."[6]

The establishment of the UK's Centre for Data Ethics and Innovation has highlighted the UK government's growing awareness of the need to respond to constituent concerns about how AI and Machine Learning ('ML') technologies will affect them. The centre is just one of a number of new representative bodies globally that are becoming focused on the issue of data ethics.

Example of ethical considerations are where natural bias is introduced by historical data which reflects historical trends that no longer apply, and racial bias by non-representative postcode distributions. These examples highlight the need to understand your data before applying AI over it.

Within a company, leaders must have confidence that their AI systems are functioning reliably and accurately, and they need to be able to trust the data used. Yet this remains an area of concern; in a recent survey, nearly half (48%) of the respondents cited a lack of confidence in the quality and trustworthiness of data as a challenge for enterprise-wide AI programs. Amid these considerations, it is increasingly clear that failure to adopt good governance and ethical standards that foster consumers' trust in AI will limit organisations' ability to harness the full potential of these exciting technologies to fuel future growth.[7]

In particular, the "black box"-like effect of the algorithms in these new technologies, and the challenges in auditing them appropriately, has given rise to the need to ensure that companies agree appropriate risk-based ethical assessment criteria up front and in advance of their use.

It is difficult to execute a search on Google regarding data protection, AI or ML that does not feature a reference to data ethics on the first page of the results. This highlights the interests of people searching Google and the need for companies to have a clear strategy and to develop a specific approach to address this area. While many different criteria have been proposed, the approach adopted for any company will need to fit the maturity, scale and risk appetite of the organisation concerned e.g. Axciom a listed US corporation has pioneered in its creation of a position of Chief Data Ethics Officer, in an effort to respond to the focus on this topic.

Assertion 3

"Customers are expressing and acting upon their growing expectation of being able to trust the companies they interact with"

A recent survey carried out by IBM of 10,500 adults across UK, US, Germany, Brazil, China, India and United Arab Emirates found that 77% of adult customers consider the ability of a company to keep their information safe before buying a product or service from them. 82% of UK adults surveyed will not buy a product or service from a company if they don't trust it to protect their data.[2]

Across 20 countries surveyed globally, an average of 65% of customers indicated they would stop shopping with a given merchant after experiencing fraud or a data breach.[9]

"Trust is an important legal concept in common law, widely used for owning property - any UK property owned by two or more people is technically held in trust"[8]

The UNCTAD report goes on to point out that significant changes in data protection regulation have reduced drastically the opportunity for companies to access and analyse customers' data, with a consequent increase in its value. Those companies that are willing to collect and use personal information are forced to develop deep trust from the individuals concerned, by proving to them that their personal data is in safe hands.[1]

Evidence suggests that, increasingly, customers are dealing with this lack of trust by seeking recompense through the courts, as evidenced by the class actions implemented by affected customers whose personal data has been breached e.g. recent actions against Morrisons, British Airways, Facebook and Marriott.

Assertion 4

"Customer trust will have a direct and increasing impact on customer acquisition costs and the economic value of companies"

Facebook is a significant and concrete example. As the news about Cambridge Analytica emerged, 3 million users in Europe unsubscribed from the social network, and Facebook's share price dropped 19%. After the firm communicated to investors that user growth had slowed due to the scandal, the market value of the company decreased by more than £90 billion. The company's CFO, David Wehner, commented on the situation: "Our total revenue growth rates will continue to decelerate in the second half of 2018, and we expect our revenue growth rates to decline by high single-digit percentages from prior quarters sequentially in both Q3 and Q4. Looking beyond 2018, we anticipate that total expense growth will exceed revenue growth in 2019." The share price at end 2018 fell to a new low of $132.

Following the cyber-attack on TalkTalk, which involved the personal details of thousands of customers and resulted in a £400,000 fine from the ICO, the firm's profits fell from £32 million in the prior year to £14 million. This fall reflected contributing factors such as £42m in costs as a result of the attack and a loss of 95,000 customers in the third quarter of that year alone. On the plus side Dido Harding, its Chief Executive, said: "…the business bounced back strongly in the final quarter following the cyber-attack in October."[11]

A 2017 study by Centrify and the Ponemon Insitute, across 113 companies that had suffered a data breach, found that immediately following its disclosure they experienced an average stock price decline of 5%.[12] Beyond financial penalties, organisations that do not embrace this opportunity to take stock and make change risk losing the trust of their consumer base. This is of fundamental importance, given that a global study shows that 45% of consumers have switched providers because they lost trust in their initial choice. [13]

The impact of these breaches of both security and trust shows a clear financial impact in terms of capital value and customers. What has yet to be quantified is the change in the costs of acquiring new customers that is the natural consequence from having to recover from these reputational 'hangovers'.

But as the high profile problems at companies such as Facebook and Marriott continue to remind consumers about the risks to their data, all companies will feel the costs and pressure to deliver tangible evidence regarding trust and ethics now demanded by their valued customers.

With the onslaught of factors attacking consumer trust, companies are now turning to AI and ML to assist them to lower or improve the customer acquisition costs with models for "customer propensity to buy". This can be not just a growth strategy for those companies, but a critical part of revenue protection against the inevitable customer churn. Putting in place appropriate governance models will be essential in these environments, to demonstrate to customers that organisations can be trusted with the use of their data.

Assertion 5

"Going forward, we believe that companies will need to respond to this expectation of trust by providing more tangible, evidence-based, indicators of that trust and how it is being sustained and communicated with customers on this basis"

A recent Gartner survey highlights that despite the fact that AI will accelerate and broaden across all types of business functions and industries, it will continue to be limited by its ability to reliably discern truthful content from false information. "Through 2020, AI-driven creation of "counterfeit reality", or fake content, will outpace AI's ability to detect it, leading to digital distrust. Moreover, by end 2021, more than half of digital banking initiatives will fail due to their inability to deliver an authentic human experience that customers trust".[6]

For companies to be regarded by their customers as having met the new threshold on trust based on tangible evidence, they will need to have in place communications programmes that have taken those customers through a personalised education process, rather than doing this urgently, after the fact, following a data breach. Customer trust will be created and preserved through a dialogue, with a historically unprecedented disclosure of internal controls and governance as a show of good faith. This education process should include the activities that the company will undertake in the event of any breach occurring in the future.

The July 2018 'Annual Cost of a Data Breach' study by the Ponemon Institute reported that the probability of a Data Breach is now 1 in 4 and increasing.[14] Clearly, this infers that all companies need to be preparing for this eventuality and how to protect customer trust.

Recognising that not all consumers will be willing to share their personal information, and notwithstanding its value, companies have been developing a range of solutions to allow their users to manage personal data that can be accessed by websites and apps, navigate the internet anonymously, and encrypt their phone calls, messages, emails and internet browsing e.g. DuckDuckGo, Blackphone, Indie Phone, Ghostery and numerous others.[15]

In educating customers, companies will need to better understand the decisions that their models make, the ethics and basis behind those decisions, the governance associated with them and any potential bias in the data. An example is useful in this regard[16]:

A medical department was trying to predict the risk of complications in its pneumonia patients, considering that lower risk patients could receive outpatient treatment. When the team applied machine learning in the judgement, the automated process decided that because those pneumonia patients who also had had asthma experienced only a few complications, they could be sent home. However, the real reason for this situation was that they had received intensive care at the hospital, and the essential link between the patients' complications and the type of care they received in the hospital was not considered by the machine algorithm. In this case, the team was able to understand the error easily and correct the system, consistent with the clear ethical outcomes involved i.e. "the well being and improvement of patient care". However, if the algorithm had been more complex, as is the case for most AI and ML processes, use of the model could have brought severe consequences upon the patients concerned and also the hospital, through the significant and potentially irreversible deterioration of its relationship and trust with patients.

Conclusion

Consumer trust is a precious and fragile commodity that is increasingly under threat from a number of angles, including technology advancement, malicious intent and a lack of appropriate data controls and governance. Without doubt, the introduction of the GDPR in the EU and the resultant global roll-out of updated or new data protection legislation has heightened consumers' awareness about their personal data and the value and risks attached to it. High profile data breaches have created added sensitivity for a vastly increased number of consumers – both across those directly affected by the breach and others – and the desire among consumers to take a measure of control over their data.

It is clear that organisations have the opportunity and capability to obtain a competitive advantage from any lack of interest in this topic by their competitors, through taking the opportunity to be a leader, teacher and ambassador for their customers. One key element in that is to implement suitably robust data controls and governance to reflect this new environment. Another key element is for companies to consider returning to a partnership with customers - albeit a digital one - making them aware in advance and on an ongoing basis of the risks to them from using their data, and how it is being protected and managed.

Definitions

Cynics
Cynics are sceptics, they act in their own interests in the belief that the entity they are dealing with cannot be trusted. They do their own research trusting their own views. They spend and invest cautiously, worried that because their views and lack of trust someone will take advantage of them.

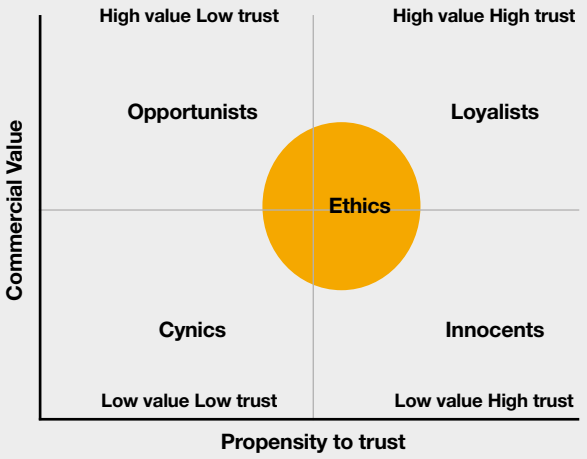
Cynics will view themselves as highly ethical but the question the ethics of others.

Opportunists
Opportunists are similar to the cynics, as they are sceptics operating in their own interests. But they accept that there could be benefit in trusting an entity and having a longer relationship. However, because each opportunity and entity is viewed independently ethical standards tend to vary based on perceptions, timing, value and brand.

Opportunists will apply different ethical considerations depending on the entity they are dealing with, and will expect the entity to treat them in the same way.

Innocents
Innocents believe everybody and every entity operates to their standards. By default they will assume that everybody can be trusted and will be forgiving when something doesn't work assuming all 'parties did their best'. For these reasons they are unlikely to be of high value as its probable they have suffered loss from previous purchases or investments as a result of this.

Innocents will view themselves as highly ethical and will assume that the entity they are dealing with is the same, believing that the entity will behave the same way they do.



Loyalists
Loyalists will spend with and be loyal to an entity. Once loyalty is established they will purchase or invest with that entity before looking elsewhere, changing entities only when what they want cannot be obtained. The visibility of the entity and will reinforce their view of trust.

Loyalists will view themselves as very ethical and require the entities they are dealing with to demonstrate their ethical standards before accepting them but once this is proven will remain loyal to those entities through multiple dealings.

As this example chart for 'Propensity to Trust' indicates, in general there is potential opportunity and value for companies in taking steps to identify and move current and potential customers on the left across to the right.

As an example, a company can look to secure a significant element of its future, predictable growth by identifying and focusing on the 'Opportunists' i.e. those who are of high commercial value and who have the propensity, through education and a demonstration of behavior that engenders trust, to be moved to become 'Loyalists'.

Relative to traditional approaches and ways of thinking, a company's frameworks and operating models for managing data-related risks in today's and future environments need to be far more capable of:
adapting to cope with the speed of technology adoption and change that is now taking place; and
managing and influencing customers' attitudes and the level of trust they have in the company's use of their data.

Crowe

About the author

Neil Currie is UK Head of Data Management at Crowe's consulting team in London. He focuses on data strategy, governance, culture, protection and value.

As the current generation of consumers becomes increasingly mobile and borderless, leveraging and managing technology effectively through machine learning and artificial intelligence initiatives becomes a real and practical challenge for an increasing number of firms. Neil works with client stakeholders to help them think through and consider issues such as how the 'black box' effects of these technologies impact their data protection risk exposures and governance models. Working in partnership with Crowe's Head of Data Analytics, he looks at the opportunities and challenges brought by data analytics, machine learning and artificial intelligence and how these are impacted by data ownership, trust and ethics.

Contact Neil: +44 (0)203 752 3503, neil.currie@crowe.com

Crowe – a highly effective and trusted consulting partner

Crowe's risk heritage and broader capabilities help us to reinforce that risk management should be as much about leveraging opportunities as 'protecting the downside'. This is an important mindset when it comes to helping our clients to succeed in today's heavily data-driven and rapidly changing business environment.

For each of our clients, whether large or small, we keep their business objectives, priorities and specific cultural characteristics at the heart of what we do. They are fundamental to delivering outcomes with our clients that will be sustainable well beyond 'the project'. Our progressive approach and the way in which we consult, collaborate and partner with our clients, and being trusted by them to work with us again and again, is a key factor in our ongoing success and growth.

www.crowe.com/uk-risk

Reference sources

1. https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx
2. https://newsroom.ibm.com/Cybersecurity-and-Privacy-Research
3. https://www.consumersinternational.org/media/155133/gdpr-briefing.pdf
4. https://www.infoworld.com/article/3255948/machine-learning/building-trust-in-machine-learning-and-ai.html
5. http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf
6. Gartner-100-data-and-analytics-predictions-through-2022.pdf
7. https://www.ey.com/en_gl/digital/how-do-you-teach-ai-the-value-of-trust
8. https://www.ftadviser.com/protection/2018/08/09/why-gdpr-will-impact-trust-disputes/
9. https://www.aciworldwide.com/-/media/files/collateral/trends/2017-global-consumer-survey-consumer-trust-and-security-perceptions.pdf
10. https://www.theguardian.com/technology/2018/jul/26/facebook-market-cap-falls-109bn-dollars-after-growth-shock
11. https://www.theguardian.com/business/2016/may/12/talktalk-profits-halve-hack-cyber-attack
12. https://www.centrify.com/media/4737054/ponemon_data_breach_impact_study.pdf
13. https://gdpr.report/news/2018/01/23/general-data-protection-regulation-trust-consumer/
14. https://securityintelligence.com/series/ponemon-institute-cost-of-a-data-breach-2018/
15. https://www.accenture.com/t00010101T000000Z__w__/gb-en/_acnmedia/PDF-32/Accenture-Guarding-and-Growing-Personal-Data-Value-POV-Low-Res.pdfla=en-GB#zoom=50
16. https://www.infoworld.com/article/3255948/machine-learning/building-trust-in-machine-learning-and-ai.html