If GDPR Embodies the Rules of the Road for Data Privacy and Protection, Trustworthiness is the Fast Lane

Eamonn Begley

M.Sc. in Management of Information Systems

2018
Declaration

I declare that the work described in this dissertation is, except where otherwise stated, entirely my own work, and has not been submitted as an exercise for a degree at this or any other university. I further declare that this research has been carried out in full compliance with the ethical research requirements of the School of Computer Science and Statistics.

Signed: Eamonn Begley

Eamonn Begley

10/06/2018
Permission to lend and/or copy

I agree that the School of Computer Science and Statistics, Trinity College may lend or copy this dissertation upon request.

Signed: 

Eamonn Begley

10/06/2018
Acknowledgement

I would like to thank my supervisor Paula Roberts for all her advice, guidance, and support throughout the course of this dissertation.

I would also like to thank my wife Mary, and my children Niall, Colm and Eva who granted me the time and space to complete this dissertation.
Abstract

This research examines the question of whether trustworthiness provides a viable approach to resolving the concerns raised by the General Data Protection Regulation (GDPR) for data driven business, using as examples the premium exponents of platform based advertising companies such as Facebook and Google. The important and practical difference between trust and trustworthiness is evaluated and a set of dimensions of trustworthiness particularly applicable to data privacy and protection are specified, including Honesty; Benevolence; Competence; Reliability; Vulnerability; and Communication. The difference between trustworthiness and GDPR compliance is examined, followed by an in-depth assessment of the nature of data driven business, its benefits and opportunities, weaknesses and threats and the likely effects of GDPR on that trajectory. A conceptual model for data privacy and protection is developed which takes account the impact of GDPR on the user – organisation relationship. An evidence based approach to measurement of trustworthiness is proposed based on -2 to +2 scale, drawing evidence from regulatory enforcement agencies in the US and EU and also from applying data privacy and protection based statements consistent with an identifiable status of an aspect of trustworthiness, ‘very honest’, for example. The conclusion arrived at is the trustworthiness provides an avenue beyond compliance to thrive in data driven business in a more regulated business world.
If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane

Table of Contents

Declaration ........................................................................................................................................... i
Permission to lend and/or copy ........................................................................................................ ii
Acknowledgement ........................................................................................................................... iii
Abstract ............................................................................................................................................... iv
List of tables ....................................................................................................................................... 1
List of figures ....................................................................................................................................... 2
List of Abbreviations .......................................................................................................................... 3
Chapter 1: Introduction ..................................................................................................................... 4
Chapter 2 Establishing a conceptual understanding of trustworthiness and the General Data Protection Regulation .......................................................................................................................... 5
   Distinguishing between Trust and Trustworthiness ........................................................................ 5
      Dimensions of trust and trustworthiness ..................................................................................... 5
   Dimensions of Trust and Trustworthiness in the context of Data Privacy and Data Protection ........ 8
      Honesty ......................................................................................................................................... 8
      Competence ................................................................................................................................. 8
      Benevolence ............................................................................................................................... 9
      Reliability (Predictability / Consistency of behaviour / Expectation) ........................................ 10
      Vulnerability / Balance of Power ............................................................................................. 10
      Context ....................................................................................................................................... 11
      Risk ............................................................................................................................................ 11
      Communication, Openness, and Transparency ......................................................................... 12
      Identification / Similarities / Shared Values ............................................................................. 13
      Calculative Trust ......................................................................................................................... 14
      Risk Tolerance and Adjustment ................................................................................................. 15
      Alignment of Interests ............................................................................................................... 15
      Emotional Attraction ................................................................................................................. 15
      GDPR ....................................................................................................................................... 16
      The GDPR Principles .............................................................................................................. 16
Trustworthy versus compliant ................................................................. 18
Summary..................................................................................................19

Chapter 2. The relationship between Data Driven Businesses and GDPR .......... 19
Introduction............................................................................................ 20
What are Data Driven Business Models?.................................................. 20
DDBM types ............................................................................................ 20
The macro-economic outlook for big data and data flows ...................... 23
Benefits of Business Models in General.................................................. 25
Benefits of Data Driven Business Models ................................................. 26
Weaknesses of Data Driven Business Models .......................................... 29
Modest gains .......................................................................................... 29
Reliance on abundance of data ............................................................... 29
Lack of data scientists and analytics tools ................................................. 29
Environmental cost of data storage ........................................................ 30
Threats .................................................................................................... 30
Regulation ............................................................................................... 30
Negative Media Exposure .................................................................. 32
Cyber-attack threats ............................................................................. 32
The Effects of GDPR on data driven business ....................................... 33
Effect of GDPR on the Benefits of Data Driven Business ......................... 33
Effects of GDPR on the Weaknesses of Data Driven Business ................ 35
The Effects of GDPR on the Threats to Data Driven Business ................. 35
Conclusion ............................................................................................. 36

Chapter 3: A Trustworthiness Model for data Privacy and protection .......... 37
Introduction ........................................................................................... 37
Investigation of trust and trustworthiness models .................................... 37
Organisational and User domains ................................................................ 37
Constructing a data privacy and protection model .................................... 39
Model, Concept or Theory ................................................................... 39
Data Privacy and protection Trustworthiness Model .................................. 39
If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane

| Evaluation of the Data Privacy and Protection Trustworthiness Model | 43 |
| An approach to measuring Trustworthiness | 45 |
| Evidence of trustworthiness or untrustworthiness | 48 |
| Regulatory Sources | 48 |
| Privacy Statements | 49 |
| Visibility of Trustworthiness | 51 |
| Conclusion | 52 |
| Chapter 4 Discussion | 53 |
| Trustworthiness – and the benefits of data driven business | 53 |
| Strategy and Ethics | 55 |
| Trustworthiness – GDPR and the weaknesses of data driven business | 58 |
| Modest Gains | 58 |
| Reliance on an abundance of data | 58 |
| Lack of Data Scientists | 58 |
| Environmental cost of data storage | 58 |
| Trustworthiness - GDPR and the threats to data driven business | 58 |
| Research Question Answered | 53 |
| Chapter 5 Recommendations, Limitations and Future Research | 59 |
| Recommendations | 59 |
| Limitations | 59 |
| Future research | 59 |
| References | 61 |
| Appendices | 67 |
| Appendix 1. Sample Trustworthiness dimension standards matching proposed scale | 67 |
| Appendix 2. Sample of Facebook’s Privacy Policy 7th February 2018 | 70 |
If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane

List of tables

- Table 1 Summary of dimensions of trust/trustworthiness ................................................................. 6
- Table 2 Based on the principles of GDPR as outlined by (IAPP, 2018) .................................................. 17
- Table 3 The relationship of GDPR to trustworthiness dimensions adapted from (IAPP, 2018) .............. 19
- Table 4 Summarised from types of DDBM start-ups identified by (Hartmann et al., 2016) .................... 21
- Table 5 Adapted from (Armerding, 2018) – 17 largest data breaches 2000-January 2018 .................... 33
- Table 6 Trustworthiness model development considerations ................................................................. 43
- Table 7 Seven criteria for evaluating models (Mayer, 1989) applied to the data privacy and protection trustworthiness model. ........................................................................................................... 44
- Table 8 Measures of trust and trustworthiness of banks (Ennew and Sekhon, 2007) ............................. 46
- Table 9 Measures of the drivers of trustworthiness of banks (Ennew and Sekhon, 2007) ....................... 47
- Table 10 Sample honesty status statements ......................................................................................... 48
- Table 11 Examples of sources of evidence of trustworthiness ............................................................... 49
- Table 12 Sample trustworthiness dimension standards matching proposed scale ............................. 69
- Table 13 Sample of Facebook’s Privacy Policy 7th February 2018 (Facebook, 2018) ......................... 72
If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane

List of figures

FIGURE 1 GDPR principles as precursors to trustworthiness dimensions .......................................................... 17
FIGURE 2 Overview of the model of consumer personal data collection (CMA, 2015) ................................................. 22
FIGURE 3 Predictive Analytics vs. Prescriptive Analytics (Boire, 2016) ................................................................. 23
FIGURE 4 Top 10 predictions for IT industry (IDC, 2017) ......................................................................................... 25
FIGURE 5 Porter’s value chain model – recreated by (Butler, 2011) ................................................................. 28
FIGURE 6 Share of the digital advertising market (Desjardins, 2016) ................................................................. 34
FIGURE 7 A framework for measuring trust in financial services (Ennew and Sekhon, 2007) ............................... 38
FIGURE 8 Characteristics and key antecedents of corporate trust proposed by (Van der Merwe, 2013) .......... 38
FIGURE 9 Data privacy and protection model ........................................................................................................ 41
FIGURE 10 A model for trust (Hurley, 2006) ........................................................................................................... 45
FIGURE 11 Trustworthiness Tree ......................................................................................................................... 51
FIGURE 12 Complexity of relationship - both user and customer .................................................................. 53
FIGURE 13 Types of Corporations (Moon et al., 2011) ......................................................................................... 55
FIGURE 14 Shifting corporate social responsibility to corporate social opportunity through creating shared value (Moon and Parc, 2017) ............................................................................................................. 56
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BT</td>
<td>British Telecom</td>
</tr>
<tr>
<td>CMA</td>
<td>Competition &amp; Markets Authority</td>
</tr>
<tr>
<td>CSO</td>
<td>Corporate Social Opportunity</td>
</tr>
<tr>
<td>CSR</td>
<td>Corporate Social Responsibility</td>
</tr>
<tr>
<td>CSV</td>
<td>Corporate Social Value</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FCC</td>
<td>Federal Communications Commission</td>
</tr>
<tr>
<td>FTC</td>
<td>Federal Trade Commission</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>IAPP</td>
<td>International Association of Privacy Professionals</td>
</tr>
<tr>
<td>IMF</td>
<td>International Monetary Fund</td>
</tr>
<tr>
<td>KPI</td>
<td>Key Performance Indicator</td>
</tr>
<tr>
<td>ND</td>
<td>No Date</td>
</tr>
<tr>
<td>OECD</td>
<td>Organisation for Economic Co-operation and Development</td>
</tr>
<tr>
<td>US</td>
<td>United States</td>
</tr>
</tbody>
</table>
Chapter 1: Introduction

The General Data Protection Regulation (GDPR) introduces wide ranging changes to data privacy and data protection as and from 25th May 2018. GDPR will have a global impact on every organisation within the EU, and outside, that acquires and/or processes personal data of anyone within the EU, with the cost of compliance and even more costs in penalties for no-compliance. This research asks the question, ‘Does trustworthiness resolve the concerns raised by GDPR for data driven business?’ The research, completed just as the GDPR deadline is passed, examines the relationship between trustworthiness and the GDPR principles, evaluates the impact GDPR is likely to have on data driven business such as those platform companies like Facebook, Google and Amazon and analyses whether focussing on trustworthiness overcomes the potential obstacles and impacts that GDPR places on these data driven businesses. Chapter 1, while examining the existing research into trust and trustworthiness, argues for the value to the organisation of focussing on trustworthiness rather than on perceptions of trust, isolates dimensions of trustworthiness most applicable in a data privacy and protection environment and identifies the differences between trustworthiness and compliance. Chapter 2 focusses on the concept of data driven business, its strengths, opportunities, weaknesses and threats, and examines the potential impacts GDPR will have on the trajectory of this emerging aspect of the digital age of transformation, analytics and artificial intelligence. Constructing a data privacy and protection trustworthiness model to understand the relationship between the place of trustworthiness of an organisation, GDPR and the user, and identifying potential measurement approaches, is the focus of Chapter 3. Chapter 4 evaluates whether trustworthiness is a viable and fruitful approach to resolving the concerns raised by GDPR for data driven business. Chapter 5 proposes an approach to becoming a trustworthy data driven business and identifies limitations of the research and suggests future areas of study.
Chapter 2 Establishing a conceptual understanding of trustworthiness and the General Data Protection Regulation

Distinguishing between Trust and Trustworthiness

There appear to be many academic examinations of trust relationships in industries, including internet-based industries, though there are remarkably fewer that investigate the concept of trustworthiness. Those studies investigating trustworthiness seem, with few exceptions, to focus on the trustors’ perception of trustworthiness rather than on a rational evidenced examination of an enterprise’s trustworthiness. Although trust and trustworthiness are closely related, there are important, practical and useful differences.

(Van der Merwe, 2013) describes the connection between trust and trustworthiness as opposite sides of the same thing and define the link between the two concepts as the former relying on the latter. Focussing on trust rather than trustworthiness implies a responsibility or action upon the trustor to regulate the trust relationship between trustor and trustee, which may be to trust the untrustworthy less, whereas focussing on trustworthiness is far more reasonable and appropriate (O'Neill, 2013) and which may, if approached correctly, deliver the benefits of a trusting relationship.

Dimensions of trust and trustworthiness

A representative sample of the considerable academic research into trust and trustworthiness is presented in table 1. Various synonyms or variants of labels have been used by researchers and therefore, in order to categorise the appropriate characteristics usefully, these have been clustered together where appropriate. Table 1 forms the basis on which this research into trustworthiness is founded.

(Van der Merwe, 2013) refers to the trustworthiness of an organisation as something that has the characteristics of being intrinsic and objective where corporate decisions and behaviour are guided by an ethical standard. (Van der Merwe, 2013) also considers that all their stated trustworthiness antecedents must be present in order for an organisation to be considered trustworthy. Therefore, an organisation that is competent and reliable but also proven to be dishonest and or not at all benevolent towards its stakeholders cannot reasonably be considered to be trustworthy.

(O'Neill, 2013), identifies three central elements of trustworthiness, 1) Competence, 2) Honesty and 3) Reliability and stresses the need to provide evidence of trustworthiness. A central tenet of being trustworthy is to be vulnerable to the person from whom you seek to be trusted (O'Neill, 2013).

(Van der Merwe, 2013) contends that there are seven key antecedents that enable corporations to demonstrate their trustworthiness. These include 1) Ability, 2) Benevolence,
3) Integrity, 4) Ethical Behaviour, 5) Identifiability, 6) Transparency, and 7) Likeability. Although Van Der Merwe’s list of the antecedents of trustworthiness is more extensive, with variances in terminology compared to O’Neill’s, both specify the demonstrability of, and in O’Neill’s case the importance of providing evidence of, trustworthiness. Ability and competence are synonyms, whereas honesty can be considered to be reasonably comparable to both integrity and ethical behaviour, in combination if not separately.

Table 1 Summary of dimensions of Trust/Trustworthiness

(Hurley et al., 2013) posits that one could decide to trust another person on the basis of six different types of signals, as follows: 1) Common values, 2) Aligned Interest, 3) Benevolence, 4) Competence, 5) Predictability and integrity, and 6) Communication. (Hurley, 2006) proposes a model for trust that distinguishes between decision-maker factors and situational factors on a scale of low to high, resulting in a decision to trust or not to trust. Decision-maker factors include the concepts of risk tolerance, well-adjustedness, and relative power, whereas situational factors informing the decision to trust include security, similarities, alignment, benevolent concern, capability of trustee, evidence of predictability and integrity, and good communication.
(Ennew and Sekhon, 2007) conceived of a framework by which to measure trust in financial services institutions. While the framework placed organisational trustworthiness at its centre, the focus of their study was based on the trustworthiness as a collective including; benevolence; Integrity; Ability/expertise; Shared values; and Communications, as perceived by a randomly selected population sample, responding to telephone interviews. The trust framework, importantly captures the concept of perceived trustworthiness and also encompasses the customers’ disposition to trust and the cognitive and affective effects on trust in the organisation. (Ennew and Sekhon, 2007) engage with the complexity of the relationship between trustor and trustee, including the trustor’s disposition, cognitive and affective factors. The factors that affect an online consumer’s willingness to purchase, rely on a complex blend of influences including their level of income, their culture, family influences, social factors and life experience’ (Verhagen et al., 2006).

(Roy and Shekhar, 2010) build on the work of (Ennew and Sekhon, 2007) examining the underlying dimensions of trust in Indian retail banking, focussing on trustworthiness in terms of; customer orientation; integrity and honesty; communication and similarity; shared values, expertise and ability; and consistency, which they ultimately modelled as competency, openness, and benevolence.

(Brenkert, 1998) identifies three levels of trust; 1) basic trust, 2) Guarded trust, and 3) Extended trust, comprising of incremental conditions, culminating in all conditions (commonality of motives, consistency of behaviour, competence, and openness) being met in order for extended trust to prevail.

(Büttner and Göritz, 2008) assess the perception of the trustworthiness of online shops by asking a sample population for responses to questions under the headings; ability, benevolence, integrity, and predictability, to determine the degree of trustworthiness, finding that “intention to buy” is promoted by perceived trustworthiness and that relationship duration may have a moderating effect on trust. (Ennew and Sekhon, 2007), similarly set out to measure trust in financial services by asking a sample population whether they agreed or disagreed with statements related to the trustworthiness of financial services institutions. (Kobsa, 2007), when considering privacy protection tools, specifies ‘privacy statements need to be considered and privacy policies appropriate.

Trustworthiness can be enhanced by adherence moral guidelines or principles, and the absence of an ethical code can be mitigated by an agreement on standards of behaviour when considering management relationships with subordinates (Bews and Rousseau, 2002).
Dimensions of Trust and Trustworthiness in the context of Data Privacy and Data Protection

Honesty
In order to examine honesty more closely in the context of data privacy and protection, it is reasonable to provide a generally accepted definition of honesty. The Merriam-Webster online dictionary defines honesty as ‘fairness and straightforwardness of conduct’ and also ‘adherence to the facts’ (Merrian-Webster, ND). (Bews and Rousseau, 2002) found an emphasis in interpersonal trustworthiness of management by employees relied on communication that is open and honest, while (Verhagen et al., 2006), examining the risk as perceived by consumers and trust associated with buying e-retailers, references honesty as immutably linked to trust. Honesty also features as a first order factor of trustworthiness of financial service providers (Roy and Shekhar, 2010).

It seems obvious that the degree to which an individual or a company can prove, if not definitively, at least provide some evidence that they are honest or as a poor second, not dishonest, needs to be a central component of an organisation’s perception of its trustworthiness. A mechanism selected by a number of studies uses an interrogative method for assessing the perceived honesty of an organisation. Asking customers or users of a service if they consider whether it adheres to generally accepted standards of behaviour, such as and fairness and honesty (Hurley, 2006), or if they shows high integrity (Ennew and Sekhon, 2007). In a data privacy and data protection context, applying the principle of honesty as dimension of trustworthiness suggests a number of questions that an organisation might consider. For example, 1) What personal data is collected? 2) Is it necessary to collect this personal data for the purposes of the service being sought? 3) Has the organisation explained clearly, the necessity for collecting the personal data? 4) Is it clear that the data will be used only for the purpose for which it has been legitimately collected? 5) Is the personal data protected from loss or misuse or viewing by other parties? 6) Has the organisation been found to be deceitful in language or practice in relation to its treatment of its customers or users data in the past? 7) If a data breach occurs, does the organisation respond by confessing to the breach quickly or does it delay and cover up the breach? An inability to answer these questions would suggest that there are areas for concern with regard to the trustworthiness of the organisation.

Competence
Competence is central to most conceptions of trust as proposed by (Brenkert, 1998), (Hurley, 2006), (Büttner and Göritz, 2008), (Ennew and Sekhon, 2007), (O'Neill, 2013), (Van der Merwe, 2013). Competence or ability provides the trustor with the confidence that the trustee will deliver on their end of the transaction. For example, goods purchased online will
If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane

not go astray, be unduly delayed, or will be substantially different from what was ordered. (Johnson and Grayson, 2005) established that there are strong causal links between an organisations expertise, the performance of their products, and satisfaction with their prior interactions and their level of cognitive trust. However, from a data privacy perspective, the effect of competence or expertise on trustworthiness may be somewhat more complex. Trustworthiness might be undermined rather than be fostered if the user perceives that the organisation’s competence may be to the users’ disadvantage

From a data protection perspective, it is important to be able to demonstrate competence in terms of privacy protection, i.e. an enterprise in possession of users’ personal data should demonstrate it has the competence to protect it from loss or misuse or access by unauthorised persons or entities.

**Benevolence**

(Hurley, 2006), in the context of employer-employee relations, advises demonstrating real concern for others, even at some cost, in order to establish trust in a relationship. According to (Hurley, 2006) the engagement must be fair. Similarly, in times of crisis, a company that put its resources at the disposal of employees, showing benevolent concern for their well-being contributes to an enhanced perception of trustworthiness by employees (Bews and Rousseau, 2002). To demonstrate benevolence towards customers, the customers’ interests, from the customers’ point of view must be of concern to the enterprise (Ennew and Sekhon, 2007). (Van der Merwe, 2013) highlights corporate social responsibility as an element of benevolence for enterprises and points to focus on the well-being of its consumers as the distinguishing between those who destroy trust and those who can salvage trust. However, in order not to be accused of being naïve, corporate social responsibility should perhaps be scrutinised carefully. While there is undeniable potential for good to wider society through the various positive socially responsible actions an organisation may undertake, carefully selected and well publicised actions may well be calculated to sway the emotional (Van der Merwe, 2013) or affective element of trust perception, which may be designed to distract from the true context of the interaction or relationship between the enterprise and the consumer or user.

The use of privacy seals which may seem to indicate an organisation’s commitment to respecting the privacy of the customer or user may disguise the truth, as often organisations that use privacy seals are more invasive than those who do not use privacy seals (Kobsa, 2007).

As posited by (Van der Merwe, 2013), all antecedents of trustworthiness need to be present and some such as benevolence and competence perhaps share a particular tension and may need to be more tightly associated than the others in the context of data privacy and
If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane

The advanced nature of the technology and accompanying competence, and the subsequent potential risk to the user should arguably place a greater onus on the organisation to safeguard the interests of the user.

Reliability (Predictability / Consistency of behaviour / Expectation)

In an online context, the trustor has a hope or expectation that the trustee will act in a certain way. For example, there is an expectation that an online shop will deliver the goods purchased by the consumer. There is an expectation that the trustee can reasonably predict that the goods will be delivered. This characteristic of trust has been variously described as reliability (O’Neill, 2013), consistent behaviour (Brenkert, 1998), expectation (Moyano et al., 2012) as well as predictability (Hurley, 2006). (Blois, 1999) distinguishes between reliance and trust in terms of their dependency on capability that is proven in the case of the former and commitment in the form of statement in the case of the latter.

The question to be asked in relation to data privacy and data protection is what is it that the user is relying on the data based internet organisation to do? At a minimum it seems reasonable that an organisation should comply with its data privacy statement. However, an organisation’s data privacy statement can grant itself wide ranging permissions to access and process all available personal content and other data such as location, images, social connections, device details amongst others. It is perhaps, just those self-granted wide-ranging permissions, amongst other factors, that have ushered GDPR into being.

Vulnerability / Balance of Power

(Rousseau et al., 1998) identify two parts comprising trust. The first part relates to the trustor’s vulnerability being contextual and the second part relates to the trade partner’s behaviours and or intentions. In the case of data privacy and protection, the primary vulnerability lies on the side of the user. Once data is acquired, it may be transmitted and processed with very little restriction, that is until the advent of GDPR which seismically changes the data privacy and protection landscape. Trust requires the belief in the integrity of the trading partner and that they act in a responsible manner (Rousseau et al., 1998).

(Bews and Rousseau, 2002) refer to vulnerability, in the trust relationship, in terms of the potential severity of negative outcomes or loss, where behaviourally there is a conscious action of placing trust with knowledge of the potential loss. (O’Neill, 2013) describes, in a pragmatic, manner how companies can demonstrate vulnerability, in terms of trustworthiness, as the action or disposition to make oneself vulnerable to another. For example, if a consumer is not happy with their purchase, they may simply return it for another item or get their money back. The consumer, in this case, has a course of redress if they are unsatisfied.
In the context of data privacy and protection, there is an obvious connection to be made between the level of awareness of the individual to their vulnerability to highly expert data companies.

**Context**

(Moyano et al., 2012) rank context among trust concepts in the development of their conceptual trust model. Other important concepts include belief, subjective, willingness and expectation, behaviour, reliability, security, and assessment among others. While risk is not explicit in all definitions it is considered in most of them (Moyano et al., 2012).

(Rousseau et al., 1998), in a cross-disciplinary review of the meaning of trust, and with particular reference to the changing nature of organisations, hold that context has a central criticality, when considering trust. It is important to consider context with regard to voluntarily, or unwittingly providing personally identifiable information to companies, especially data driven businesses. When an internet user lands on a website that operates a data driven business model that generates revenue from advertising, the technological capability is so advanced that some companies can initiate a real-time bidding auction for advertisers to place advertisements onscreen in front of that internet user, utilising behaviourally targeting technology (Wang et al., 2017). The capability to build up behavioural profiles of individuals is substantial. Tracking technologies such as re-generating cookies and discrete browser fingerprinting, a persistent long-term tracking software identifying the user or user’s device, can be used to bypass users preference not to be tracked (Acar et al., 2014). The capability to regenerate a cookie after it has been removed by the user or cleansed from the internet cache, or inserting invisible pixel tags or browser fingerprint seems characteristic of a deliberate ploy to circumvent, secretly, the wishes of the user’s desire for privacy. Unless the internet user is quite expert, it is reasonable to conjecture that, given the enormous advances in online advertising technology (Wang et al., 2017), the individual user is at a major and almost invisible disadvantage when dealing with the internet advertising companies. The average user is probably somewhat aware of the effects of this secretive technology, i.e., irritatingly persistent advertisements based on a previous search, rather than them having a clear understanding of the context and the effect of each mouse click. The relationship between internet companies gathering data and the individual customer is asymmetric and exacerbates the privacy problem (Li and Unger, 2012).

**Risk**

(Hurley, No Date) posits that the question of trust does not arise unless there is risk. (Gellert, 2015) refers to risk as the possibility that something with harm will happen. (Das and Bing-Sheng, 2004) argue that risk and subjective trust are opposite images of the of each other.
and that both result in a probabilistic assessment of outcome, one positively portrayed and one negatively portrayed. (Das and Bing-Sheng, 2004) highlight the importance of risk in understanding the meaning of trust. (Slovic, 2016) explains how difficult it is for individuals to perceive risk accurately, sometimes depending on the probability of the threat, though large scale of threats or risks, such as climate change may result in a loss of sensitivity to the risk resulting in feelings that remain unanalysed. Certainly, the privacy issues central to this study are not at the scale of the climate change risk. However, the pervasive nature of the internet in every aspect of individual lives and business, and in particular a few extremely large and influential companies with access to enormous volumes of personal data, it may be possible to consider that the theory, often reprised, that the genie is out of the bottle in relation to privacy, may lead people accept that privacy is a thing of the past and therefore submit whatever non-sensitive (e.g. religion or sexual orientation), information as requested in order to continue to browse or continue to use internet services presented as free.

(Das and Bing-Sheng, 2004) distinguishes between subjective trust and behavioural trust, and contend that in the trustor–trustee relationship, the concept of risk is primarily associated with the trustor. Das and Bing-Sheng’s research suggests that there may be a causal relationship between behavioural trust and subjective trust as well as vice versa. This means that that having taken an action involving risk which results in success may have a positive contributory effect on the trustor’s subjective trust. In the context of online shopping or e-commerce (Yulin et al., 2014) examining the relationship of perceived effectiveness of e-commerce institutional mechanisms (PEEIM), an example of which is a credit card guarantee, trust and satisfaction found that trust in the online vendor is less influential on the intention to repurchase when PEEIM is at a higher level. (Yulin et al., 2014) recommend policy makers to commit to developing ‘effective institutional infrastructure across regions for the entire e-commerce environment’ and communicating its value. In summary, it seems that individuals positive experience of making purchases online and belief that they are somehow protected by external institutions in an e-commerce transactional sense, reduces the necessity of having to consider whether the online retailer is trustworthy or not.

Communication, Openness, and Transparency

According to (Hurley 2006) the concept of trust is relational and therefore requires that communication between parties must be good, and notes that bad communication leads to one or both parties becoming suspicious. Good communication is characterised by openness and honesty whereas bad communication is characterised by no communication or poor communication, leading to lack of trust. (Ennew and Sekhon, 2007) in their examination of the trustworthiness of financial services, as perceived by customers,
evaluate the effectiveness, responsiveness and sufficient awareness of the shared values with the customer to keep them abreast of new developments, demonstrating a certain benevolence towards the customer. Maintaining consistency with the actions and behaviours of an enterprise and how it communicates with both internal and external stakeholders is important to foster perceptions of trustworthiness (Van Der Merwe 2014). When examining communication in an online context, it is important to understand, that to a large extent it is an enterprise designed, structured and unstructured experience. While social networking sites offer the functionality to communicate in an open, unstructured way, for the most part, this communication is rich with personal information shared with other users, though the content is also collected by the platform provider. Overt communication with the service-providing enterprise is generally more structured requiring formal registration, obliging the user to input personal information, click on acceptance of terms and conditions and almost unfailingly accept the installation of cookie on the user’s device. Tracking, as outlined by (Acar et al., 2014) points to communication at device level where which is stubbornly lacking in openness and transparency.

In terms of data privacy and protection, the dimensions, openness and transparency in communication would suggests that the enterprise should make clear what personal information the company acquires, what they do with it and to whom they distribute it. (Bews and Rousseau, 2002), in an interpersonal context, highlight the negative effects on integrity and trust of withholding ‘fundamental information required to sustain the relationship’. Although the context of the relationship between an online enterprise and user is different to an interpersonal relationship it is reasonable to conjecture that communication in relation to data privacy and protection which is not open, honest and transparent, forthright, and appears somewhat obscured, vague or misleading, could plausibly have the same effect as outlined by (Bews and Rousseau, 2002).

Identification / Similarities / Shared Values

In the context of trust between individuals, an emphasis on similarities and shared values foster trust according to (Hurley, 2006). (Van der Merwe, 2013) makes reference to a study by (Pirson, 2009) and (Vanneste et al., 2013) who conclude that identification with an organisation is inclusive of, though greater than, similarity and familiarity, and posit that it is a precursor to trust. In the context of data privacy and data protection, it seems important to question the nature of the identification an individual user may have with an internet company. In an era of Web 2.0, of social media, where social connection is the foundation stone of the service offering, the social identity of the individual, i.e., the belonging to a particular group from an emotional and value perspective (Tajfel and Turner, 1979) as referenced by (Schneider and Sachs, 2017), is facilitated by the service providing platform
giving access to others in the group. The significance of the connection or identification with the platform may be somewhat conflated with the identification or connection with the user’s group or friends. (Ellis, 2010) articulates this when referring to a Facebook friend and notes that while enjoying a level of community and engagement with many Facebook friends, they are viewed as something entertaining and that the social media platform is a medium onto which is projected a range of optional identities at the whim of users, while also referring to the addictive quality of being connected.

**Calculative Trust**

Although there seems little recent academic research in relation to the calculative aspect of trust, (Sherchan et al., 2013) makes reference to work by (Tyler and Degoey, 1996) and (Scully and Preus, 1996) who examine the trustor’s calculation of what is to be gained by placing trust in the trustee. This seems central to the internet companies offering services such as apparently free browsing, email, messaging and or other productivity online services such as document creation, editing, and sharing, data storage, photograph storage and management, streaming of videos, amongst others. Therefore, the user receives something useful and apparently free of charge. However, there is an awareness that the user’s personal data is being acquired in the transaction and an element of privacy is being conceded. A calculation based on the combination of two ratios; the possibility of gaining versus the possibility of losing and the amount of the potential loss versus the amount of the potential gain, is referred to by (Coleman, 1990) and cited by (Sherchan et al., 2013), as the rational actions of a person. In the context of data protection and privacy, it may well be that individuals adopt the rational, calculating role working out the effects of each site visited or each click of the mouse although the odds seem overwhelmingly against any degree of accurate estimation of the potential costs to individual privacy.

From a data privacy and protection perspective, there seems to be the necessity for a close association between the concepts calculative trust and competence. A thorough understanding of the capabilities of big data and artificial intelligence is logically required to make a rational calculative decision to cede private information for some internet functionality or service, otherwise the basis for the rational decision is unsound. A user’s decision may have the sense or the feeling of being rational in the moment of clicking the agree button but without the clear understanding of the information ingesting machine at the other side of the interface, the calculative decision cannot be reasonably considered to be reliable. In relation to internet based personal information gathering, it would appear that on the machine side of the interface, the degree of calculation is potentially sophisticated well beyond human intelligence.
Risk Tolerance and Adjustment
(Hurley, No Date) makes reference to the peoples’ varying levels of comfort with, or tolerance of, risk. Therefore, it can be expected that people will respond differently to risk in relation to the privacy and protection of their data in an online context. (Hurley, No Date) further makes the connection between attitudes to risk and the degree of adjustment of an individual’s personality, meaning that people with high adjustment will be more optimistic and trusting, whereas individuals with low adjustment will have greater anxiety and have a greater propensity to distrust.

When considering the trustworthiness of an organisation, using customers’ or users’ perceptions as a means of evaluation is fraught with uncontrollable variables lying within the personalities of each user or customer.

Alignment of Interests
(Kim and Mauborgne, 2003) specify the need for enterprises to consider not just outcomes, but the integrity and the fairness by which the outcome was achieved, highlighting the need for engagement and taking the interests of all stakeholders into account. (Hurley, No Date) expresses the need for the alignment of interests in order to create trust and where the interests of the trustee are not clear then there is scope for mistrust. This is a central point in the discussion concerning online data privacy and protection as it focusses on the transparency surrounding the true nature of the relationship between online data driven companies and their users. Given the need for transparency to establish whether the interests of both parties are aligned or misaligned, this aspect of trust is conceptually very close to context and calculative trust.

Emotional Attraction
Emotional attraction is identified as an antecedent of trust by (Van der Merwe, 2013), concerning the affective rather than the cognitive domain and focusses on the levels of admiration or liking users have for an organisation based on how it behaves and communicates, its values and its vision. Emotional attraction is the only affective antecedent listed by (Van der Merwe, 2013), while (Wicks et al., 1999) identify two non-rational, closely related elements necessary for trust; 1) the affective element, meaning emotion and 2) the trustor’s beliefs in relation to the morality of the trustee. Ultimately, neither are in conflict with each other as it could be reasonably argued that (Van der Merwe, 2013) includes moral character and goodwill as aspects of ethical behaviour and benevolence previously identified as antecedents of trustworthiness.

The presence of emotion between organisations and individuals is never more evident than when there is an enormous betrayal of trust, for example, the cases of the Enron scandal (2001), resulting in public outrage (Van der Merwe, 2013) citing (Gillespie and Dietz, 2009).
GDPR

In order to understand the relationship between GDPR and trustworthiness, it is necessary to have a clear understanding of the regulations that constitute GDPR.

GDPR (General Data Protection Regulation) is officially:

‘REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)’

(EU-LEX, 2016)

The regulation is divided into 11 Chapters. Chapter 1 describes the general provisions concerning subject matter, objectives, scope, and definitions. Chapter 2 to 5 detail the principles, rights of the data subjects, obligations of the controller and processors of personal data, and transfers of personal data outside the EU. Chapters 6 to 11 relate primarily to the organisational infrastructure, workings, powers and obligations of the supervisory authorities of each state within the EU.

The stated objectives of GDPR concerns the protection of personal data and the specification of rules relating to the movement of personal data, and has its origin in the principles contained in the Guidelines for the protection of privacy and trans-border flows of personal data produced by the OECD (Organisation for Economic Co-operation and Development) (OECD, ND) and which was endorsed by both the US and the EU in 1980.

At a high level, it is reasonable to consider, that regulations such as GDPR, produced with the backing of the European Commission and the European Court of Justice whose origin is based on the longstanding data protection principles of the OECD, and even more so since the updates of 2013, should be adhered to as a basis for attempting to represent an organisation as trustworthy. Eschewing some or all of the regulations that have been designed for the specific purpose of safeguarding individual’s privacy and protecting trans-border data flows would seem to at least cast some doubt as to the trustworthiness of how an organisation handles personal data.

The GDPR Principles

(IAPP, 2018) summarises the seven GDPR principles as per Table (2).
If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane

<table>
<thead>
<tr>
<th>GDPR Principles</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lawfulness, fairness and transparency</td>
<td>There must be a legal basis for acquiring, processing and storing personal information and all shall be completed in a fair and transparent manner.</td>
</tr>
<tr>
<td>Purpose limitation</td>
<td>Personal information can only be collected and processed for the specific, explicit and legitimate purposes for which it was originally collected.</td>
</tr>
<tr>
<td>Data minimisation</td>
<td>Only data that is relevant, necessary and adequate for the purpose for which it was collected.</td>
</tr>
<tr>
<td>Accuracy</td>
<td>Reasonable measures must be taken to ensure that personal data is accurate and kept up-to-date.</td>
</tr>
<tr>
<td>Storage limitation</td>
<td>Personal data must not be kept for longer than is needed and then must be securely deleted.</td>
</tr>
<tr>
<td>Integrity and confidentiality</td>
<td>Personal information must be protected from unauthorised or unlawful processing, accidental loss, destruction or damage. Using inappropriate technical or organisational measures.</td>
</tr>
<tr>
<td>Accountability</td>
<td>Data controllers must be able to demonstrate compliance.</td>
</tr>
</tbody>
</table>

Table 2 Based on the principles of GDPR as outlined by (IAPP, 2018)

Mapping the GDPR principles to the trustworthiness dimensions results in fig (1) which visualises the essential connectedness of almost all the GDPR principles with each of the trustworthiness dimensions. For example, it is not reasonable to conceive of an honest organisation that does not comply with the principles of lawfulness, fairness and transparency. Likewise, if the context of the interaction or the ongoing relationship between an individual and an organisation does not adhere to the principles of lawfulness, fairness, and transparency, then it is not reasonable to consider that there are grounds for trustworthiness.

Figure 1 GDPR principles as precursors to trustworthiness dimensions
Trustworthiness dimensions that are not easily mapped to GDPR principles are 1) Calculative Trust / Assessment / Experience; 2) Risk tolerance / Subjective willingness; 3) Adjustment; 4) Similarities / Shared values; 5) Interest; and 6) Emotional attraction. While these dimensions have an effect on the trust relationship and the perceived trustworthiness of the organisation, they lie primarily in the domain of the individual customer or user of services.

Given the connection between the GDPR principles and the trustworthiness dimensions that an organisation may directly change about itself, a reasonable question to ask is, If an organisation is GDPR compliant, then is that sufficient to be considered trustworthy?

**Trustworthy versus compliant**

(Sinek, 2014) gets to the heart of the matter when it comes to distinguishing between legal compliance and companies driving profit regarding responsibility to customers, society, nation, and economy where they are permitted to operate, crystalizing the point with a reference to the complete regulatory compliance of the Titanic on its fatal maiden voyage. (Sinek, 2014) references Milton Friedman, Nobel Prize winning economist in 1976, as the articulator of this credo, in an article in the New York Times Magazine (1970) espousing the notion that businesses only responsibility to society is to increase their profits. Therefore, although Friedman’s view didn’t find universal favour, considering the critiques of his article, by (Mulligan, 1986) and (Wilcke, 2004) which unpicked Friedman’s views based on the use of a flawed paradigm that treats social responsibility outside business concerns, and the difference in understanding of policies that are pro-business as distinct from pro-market, respectively, it is clear that a distinction can be made between companies that pursue profit, compliant to governing rules, without regard for moral responsibility beyond their duty to their shareholders.

Matching of GDPR principles with trustworthiness dimensions can help to identify not only those dimensions of trustworthiness that an organisation can apply to itself but also help to uncover the differences between GDPR compliance and trustworthiness, for example, the GDPR principle of lawfulness, fairness and transparency can find equivalency with honesty and communication, openness and transparency, as elucidated earlier in this chapter.

<table>
<thead>
<tr>
<th>GDPR Principles</th>
<th>Overview</th>
<th>Applicable Trustworthiness Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lawfulness, fairness and transparency</td>
<td>There must be a legal basis for acquiring, processing and storing personal information and all shall be completed in a fair and transparent manner.</td>
<td>Honesty – contains concepts of fairness, ethical behaviour (according to codes of behaviour or laws), Communication – includes transparency</td>
</tr>
<tr>
<td>Purpose limitation</td>
<td>Personal information can only be collected and processed for the specific, explicit legitimate</td>
<td>Vulnerability / power – improves the user (data owner) control over their own data by delimiting the purpose to which it can be put and requiring consent.</td>
</tr>
</tbody>
</table>

(Sinek, 2014) references Milton Friedman, Nobel Prize winning economist in 1976, as the articulator of this credo, in an article in the New York Times Magazine (1970) espousing the notion that businesses only responsibility to society is to increase their profits. Therefore, although Friedman’s view didn’t find universal favour, considering the critiques of his article, by (Mulligan, 1986) and (Wilcke, 2004) which unpicked Friedman’s views based on the use of a flawed paradigm that treats social responsibility outside business concerns, and the difference in understanding of policies that are pro-business as distinct from pro-market, respectively, it is clear that a distinction can be made between companies that pursue profit, compliant to governing rules, without regard for moral responsibility beyond their duty to their shareholders.

Matching of GDPR principles with trustworthiness dimensions can help to identify not only those dimensions of trustworthiness that an organisation can apply to itself but also help to uncover the differences between GDPR compliance and trustworthiness, for example, the GDPR principle of lawfulness, fairness and transparency can find equivalency with honesty and communication, openness and transparency, as elucidated earlier in this chapter.
If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane

and consented purposes for which it was originally collected.

Data minimisation

Only data that is relevant, necessary and adequate to the purpose for which it was collected.

Vulnerability / power – improves the user (data owner) control over their own data by delimiting the purpose to which it can be put and requiring consent.

Accuracy

Reasonable measures must be taken to ensure that personal data is accurate and kept up-to-date.

Vulnerability / power – improves the user (data owner) control over their own data by requiring the organisation to ensure their data is accurate. Competence – is required to maintain up-to-date personal data.

Storage limitation

Personal data must not be kept for longer than is needed and then must be securely deleted.

Vulnerability / power – improves the user (data owner) control over their own data by delimiting the length of time it can be kept. Competence – is required to ensure personal data retention schedules are adhered to and secure deletion at the defined time.

Integrity and confidentiality

Personal information must be protected from ‘unauthorised or unlawful processing, accidental Loss, Destruction or damage, Using inappropriate technical or organisational measures’

Competence – is required to ensure integrity and confidentiality.

Accountability

Data controllers must be able to demonstrate compliance

Competence – in governance is required to be able to prove compliance.

Table 3 The relationship of GDPR to Trustworthiness dimensions adapted from (IAPP, 2018)

The key dimension that is not directly relatable to GDPR compliance is benevolence. An organisation may be compliant without being benevolent, that is to say looking out for the best interests of the user. However, given the closeness of the relationship at a conceptual level and also the logic of compliance with the GDPR principles being an antecedent to trustworthiness means that GDPR is inextricability linked to trustworthiness.

Summary

Analysis of the various dimension of trust and trustworthiness presents a rather tricky interconnectedness of concepts, interpretations and classification. While not being ultimately contradictory, there is a requirement for a meta construct with which to frame a useful paradigm to aid understanding and application to an investigation into the trustworthiness of data driven organisations.

The important practical and useful differences between trust and trustworthiness allow an organisation to focus on how trustworthy it is, independent of users or customers’ perceptions. Provided that appropriate, criteria-based evidence supports claims of trustworthiness, an organisation can validly self-examine, which allows it to ignore the trust/trustworthiness dimensions that lie predominantly in the domain of the user or customer.
Chapter 2. The relationship between Data Driven Businesses and GDPR

Introduction

Chapter 1 examines the relationship between trustworthiness and GDPR identifying a set of trustworthiness dimensions that are applicable in the context of data privacy and protection and concludes that the relationship between GDPR and trustworthiness is one of overlapping concepts with the exception of the trustworthiness dimension, benevolence. The purpose of chapter 2 is to gain an understanding of and evaluate the current state of data driven business’s and then to assess its likely trajectory prior to the introduction of GDPR and then assess the impact GDPR is likely to have upon that trajectory.

What are Data Driven Business Models?

DDBM types

Although there does not appear to a clear consensus as to the definition of data driven business models, several key characteristics/concepts seem to play a significant role in the acceleration of the data gathering, analysis and processing as a means to inform decision-making in business.

The rocket fuel central to the propulsion of what some are calling the 4th industrial revolution, is the proliferation of data (Schwab, 2016). Big Data is characterised by volume, variety, velocity, and veracity according to (Ittmann, 2015), referencing descriptions by (Dietrich et al., 2014), and (Sathi, 2012). Combining the volume and speed of big data with algorithms provides for “machine learning-based predictions” at dramatically reduced cost (Agrawal et al., 2017).

In an attempt to create a taxonomy of data driven business models, (Hartmann et al., 2016) focus on companies that use data as a fundamental resource for operating their company”. While limiting their sample to one hundred start-up companies, (Hartmann et al., 2016) produced a framework which categorises the elements of data based business models.

<table>
<thead>
<tr>
<th>DDBM Start-Up Types</th>
<th>Characteristics</th>
<th>Key Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free Data collector</td>
<td>Data Acquisition, Blogging Data, User generated and tracked mobile data Aggregation: Merger of multiple diverse data sets</td>
<td>Data Crawling, Visualisation</td>
</tr>
<tr>
<td>Aggregator</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analytics as a Service</td>
<td>Processing: Near real-time processing</td>
<td>Data distribution of results via portals and visualisation</td>
</tr>
<tr>
<td>Data Generation &amp; Analysis</td>
<td>Descriptive Analytics: statistical dashboard</td>
<td>Crowdsourcing, Web Analytics, Smartphone generated data or other physical sensors.</td>
</tr>
<tr>
<td>Free Data Knowledge</td>
<td>Predictive Analytics: Content and advertising recommendations</td>
<td>Use of free data and data analytics</td>
</tr>
<tr>
<td>Discovery</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane.

| Data Aggregation as a Service | Aggregating data from a customer’s multiple internal sources | Aggregation, distribution, visualisation |
| Multi-source data Mash-up and Analysis | Aggregation of external (Mostly Free) data, Data analytics | Customer metric tracking, analysis, benchmarking |

Table 4 Summarised from types of DDBM start-ups identified by (Hartmann et al., 2016)

The categories identified include the following: 1) Data sources, 2) Key Activity, 3) Offering, 4) Target customer, 5) Revenue Model, and 6) Specific Cost Advantage (Hartmann et al., 2016). Through clustering analysis, they arrived at six different types of Data Driven Business Model start-ups including the following: A) Free Data collector and Aggregator; B) Analytics as a service; C) Data Generation Analysis; D) Free Data Knowledge discovery; E) Data Aggregation as a Service; F) Multi-source data mash-up and Analysis. The very nature of start-up businesses renders them free from the encumbrance of legacy systems, processes and culture, allowing them the freedom to provide specialist products and services to the market. This freedom perhaps has the advantage of providing a purist view of categories of customer centric data driven business models.

While (Hartmann et al., 2016) provide a recent perspective on the range of activity types and their associated key characteristics, the Federal Trade Commission (FTC) in the U.S. identified the need for transparency and accountability amongst data brokers, in a quite mature yet discreet market, citing the un-consented collection of over a billion data points covering the vast majority of U.S. citizens (Ramirez et al., 2014). The data collected includes information that GDPR deems to be sensitive, and as such singles it out for special protection. The report names companies as follows: Acxiom; Corelogic; Datalogix; eBureau; ID Analytics; Intelius; PeekYou; Rapleaf; and Recorded Future, as a cross representative sample, and while none of which is a household name, it’s quite likely they have household names for most of the people living in the United States (Ramirez et al., 2014) and perhaps beyond. Their activities are consistent with activities and characteristics observed by (Hartmann et al., 2016). The purpose of gathering all this personal data is to sell it for identity verification, product marketing or fraud prevention amongst others, activities, some of which are governed in the US by the Fair Credit Reporting Act (FCRA) while others such as sale of consumer’s personal information for marketing is not regulated by FCRA and is lacking in transparency (Ramirez et al., 2014).

(CMA, 2015) provides a reasonable overview of a simplified model of the interrelationships between the consumer, and first and third party businesses in the acquisition of data in Figure (2). The first party business model may be involved in data analysis also, as in the case of Facebook and the third party business one or more of many data brokers, again, in Facebook’s case, Acxiom is an example (Delo, 2013).
Brands specialising in e-commerce and advertising including Amazon, Google, Apple, Facebook, and Amazon, known as GAFA, are potentially some of the most recognisable brands in the western world and perhaps beyond. Others perhaps not so recognisable immediately recognisable include Alibaba, Baidu, Priceline Group, are listed amongst the top ten largest internet companies in the world (Chepkemoi, 2017), some of which are more recognisable than others.

The nature of these internet businesses is such that collecting and processing individual users’ data is an essential and legitimate part of conducting their business. However, all aspects of processing, control, and distribution of user EU citizens’ data comes under the scrutiny of GDPR. Processing of data is defined by GDPR and referenced by the International Association for Privacy Professionals (IAPP) as follows:

‘Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.’

(IAPP, 2018)
Business Intelligence shares many characteristics of the data driven business model types, which use data in improving business decisions, including data gathering, storage, access and analysis identified by (Wixom and Watson, 2010). Key activities identified in DDBM innovation, similar to Hartmann et al, specify data aggregation, acquisition, analytics, generation, distribution, processing and also add visualisation (Brownlow et al., 2015).

Figure 3 Predictive Analytics vs. Prescriptive Analytics (Boire, 2016).

Figure 3 captures the broad-strokes evolution of analytics featuring descriptive analytics, followed by diagnostic analytics, then predictive analytics and finally reaching prescriptive analytics. It is perhaps the shared understanding of the potential of predictive analytics that has worried policy makers in Europe to the point where saw the necessity for regulation with the far-reaching scope of GDPR.

The macro-economic outlook for big data and data flows
(Van Der Marel, 2016) points to the connection between economic health and the investment in and use of data, and argues for the creation and use of a policy framework by countries within the EU to capitalise on the potential of the adoption of “big Data” as a source of economic growth, noting that a surprising number of countries are underperforming apparently because of the under-use of ICT in non-digital sectors (Van Der Marel, 2016). Van Der Marel relies heavily on a study of the correlation between 1) investments in research and development, computer systems, product development and
other “intangibles”, and 2) cross border data flows, as a basis for his assertion which connects big data to economic health by (Hofheinz and Mandel, 2015). Hofheinz and Mandel’s conclusions are significantly caveated due to lack of statistics for the role of data in international trade. Also, using U.S. analysis related to internet and data usage, and suggesting that those percentage increases could apply to countries within the EU without accounting for the large presence of the American digital industry titans such as Google, Facebook, Twitter and others in the EU already, is worrying but perhaps not surprising considering that Van Der Marel, and Hofheinz and Mandel’s work targets influencing EU data privacy policy. Estimations of a country’s opportunity for growth and economic health measured by correlating intangible investment in ICT and trans-border data flows, which does not take account of the rise of data intensive entertainment streaming services and data sharing from international sites due to the huge growth in personal smart devices such as smartphones (Ekholm, 2015), appears to leave the case unproven, particularly when measured by data flows.

Notwithstanding issues of academic analysis, industry seems clearly headed in the direction of a data driven enterprises for society. Credible industry analyst, (Gartner, 2017) predicts transformative growth by 2021 of key elements of analytics, artificial intelligence in enterprises, the emergence of natural language as a feature of applications, and management of information as an asset. (PwC, 2016) projected an upward trajectory for revenue generated from global internet advertising from $154 billion to $260 billion U.S. dollars between 2015 and 2020, noting the likelihood that online advertising would exceed TV advertising in 2016. (Henke et al., 2016a)’s report for McKinsey, while acknowledging predictions made for big data were not fulfilled by 2016, identified machine learning’s scope for having a high impact in the personalising of advertising.
If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane

*Figure 4 Top 10 Predictions for IT Industry (IDC, 2017)*

(IDC, 2017) captures the convergence projection of digital transformation elements towards a tipping point of completion by the year 2021 when the digital transformation becomes mainstream.

**Benefits of Business Models in General**

Business models, in and of themselves, are perceived to provide business benefit in the form of capability for competitive advantage. (Amit and Zott, 2012) in the MIT Sloan Management Review refer to a study by the Economist Intelligence Unit entitled Business 2010 Embracing the Challenge (EUI, 2005), of over 4,000 senior managers, which found that slightly over half of them highlighted business models as a source of competitive advantage. Business models can be characterised in terms of activities that are interconnected and are also interdependent, and emphasise the importance of novelty, the ability to achieve lock-in, supplementing or interdependency between elements and being efficient (Amit and Zott, 2012). However, if only slightly over half of senior managers perceived business models as a source of competitive advantage, it’s not quite a ringing endorsement. The corollary is that almost half senior managers did not perceive the same competitive advantage from business models. It seems, however, that adopting a particular type of business model may improve the likelihood of available finance. A longitudinal study of publicly traded companies on U.S. exchanges shows that there is a distinct preference amongst investors for particular types of business models, primarily highly innovative
manufacturing and intellectual property licensing (Weill et al., 2011). Financiers scouting for opportunities on the basis of particular business models is a strong endorsement for their belief in certain types of business models as differentiators of potentially successful business opportunities.

Benefits of Data Driven Business Models

In 2013, the volume of information stored in the world has been estimated at 1,200 exabytes (billion gigabytes) and companies placing themselves in the middle of the flows of this information and gather data will “thrive” according to (Mayer-Schönberger and Cuckier, 2013). The trend is set to continue with annual data growth rates of 40% annually, reaching 44 zettabytes (trillion gigabytes) by 2020, the enormous increases in computer processing power and the internet connected devices into which most ordinary people are inputting their personal information (IDC, 2014), actively or passively. Therefore, the trajectory for the raw material of data driven business models is expected to increase in abundance unless the General Data Protection Regulation chokes this seemingly free source of information by rebalancing the equation more in favour of the rights of the individual to data privacy and protection.

Some work has been done to determine the value of data driven business models. (Brynjolfsson et al., 2011) demonstrated a direct positive connection between data-driven decision-making and company market value. Similarly, It has been shown that there is a reported 5-6 per cent productivity gain in companies that are data driven as opposed to those that are not (Brownlow et al., 2015). (Ittmann, 2015) advocates adoption of big data and business analytics in logistics and supply chain management as an enhancement to business and catalogues a large array of benefits including predicting demand and tracking orders, citing world leading companies such as Amazon, IBM and others. It seems that there are undeniable gains to be made by businesses by investing in data based decision-making or perhaps by being the first to use data for competitive advantage (Winig, 2017).

(Mayer-Schönberger and Cuckier, 2013) claims that data’s greatest value lies, not necessarily in the use for which it was gathered, but in an unknown yet to be discovered use. Case studies, such as South Africa’s largest bank, Nedbank’s data practices with regard to customer relationships support the view presented by Mayer-Schönberger and Cuckier. (Winig, 2017) documents the bank’s growth strategy based in part on understanding customer behaviour. A competitive advantage and revenue growth accrued to both bank and client from packaging their client’s customer’s electronic payments data (Analytics as a service) yielding information with regard to location, timing, frequency, amount of money spent, as well as age, sex, address and all of the other data banks accumulate as a matter of course throughout their customers’ lives. Added value and
If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane

offerings appropriate to the customer profile were cited as the benefits to the customer. The Nedbank analytics team acknowledge the pilot nature of the their initial success and identified the challenge of operationally and culturally embedding analytics in the business. (Ransbotham and Kiron, 2017) also report a competitive advantage and other benefits accruing to companies investing in data analytics. Unlike Mayer-Schonberger’s assertion that the greatest value of data is lying around waiting to be discovered, perhaps the premium example of a data driven business is the online retailing giant, Amazon, whose business is guided by tracking 500 metrics, most of which are customer related (Anders, 2012), though GDPR may impact on Amazon’s capability to use personal data as they currently do. In support of this strategic approach, (Short and Todd, 2017) advocate a needs based approach by senior management towards monetizing digital assets.

If Mayer-Schönberger’s assertion is true, and it is certainly supported by evidence from the Nedbank case-study, then data driven business models that rely on gathering and processing personal data may hit a significant but probably not insurmountable, road-block once GDPR comes into effect. Chapter II, Article 5(b) of the regulations specifically prohibits further processing of personal data beyond the initial specified and legitimate purpose for which it was gathered. While the win-win-win (for bank, client, and customers) is reported in the case study, the GDPR limitation seems to be included to specifically address what (Mayer-Schönberger and Cuckier, 2013) refers to as the potential to skirt the ethical, moral and legal aspects of personal data gathering.

Amazon’s success lies to a large extent in its goal of truly placing the customer first, the symbolism of the empty customer chair at senior executive meetings (Anders, 2012), captures the strategy aptly. In contrast to Amazon’s approach, the capability of companies to track online activity such as chat and blogging communities sets quite a different tone, though can yield beneficial feedback for companies. For example, analysis of the patterns of interactions of online blogging communities was shown to provide useful product related feedback which can then inform management decisions related to their product offering thus improving the offering for the customers. A limited study of the interactions of blogging communities writing in relation to IPODs and Starbucks on the blog site Xanga, revealed patterns of communications that address business Intelligence questions (Chau and Xu, 2012). On a larger scale, it has been shown that access data from the Web 2.0 environment can provide useful socio-cultural perspectives on potential merger and acquisition targets thus improving the opportunity for success in this business expansion activity (Lau et al., 2012).

An example of marrying operational data with customer information in real-time, enables changes that can have a positive operational impact or a customer experience impact. For
example, optimal coordination of flights by an airline based on data received and analysed in real-time or identifying high value customers and managing their experience during disruption to ensure their experience of using the airline is a good one (Wixom and Watson, 2010). The customer data, in this, case is legitimately held by the airline and therefore unlikely to be in conflict with GDPR.

Porter's value chain model as elaborated by recreated by (Butler, 2011) is representative of the nature of activities of a modern company, perhaps leaning more towards the creation of physical products than virtual or software products or services. It is still a useful framework to consider when attempting to analyse data driven business models in relation to the various activities of a company.

![Figure 5 Porter’s value chain model – recreated by (Butler, 2011)](image)

Much of the big data and analytics literature focusses upon collecting and processing customer data. Within Porter’s Value Chain Model, the primary activities concerned with customer data is marketing and sales, and customer services and in cases where there is direct delivery to the customer such as with Amazon, outbound logistics would also be customer data centric.

Benefits accruing to companies from data driven business models that are applied to inbound logistics and operations are less likely to be less impacted by GDPR restrictions unless the “raw materials” are personal data. Companies like General Electric feature prominently as increasingly digital, data driven, and are at the forefront of digital operational technology, focussing on generating data from industrial monitoring sensors in jet engines
and gas turbines amongst other machines, and feeding this into cloud based platforms and analytics systems which predict failures and help avoid disasters as well as lower cost and improve efficiency (Winnig, 2016). The likes of General Electric’s, Predict analytics software used to analyse GE’s sensors represents an investment of over a billion dollars (Winnig, 2016), and is immune from the effects of GDPR.

**Weaknesses of Data Driven Business Models**

*Modest gains*

Highlighting some obvious successes in the sphere of data analytics such as Google, Amazon, Netflix, Facebook, and Uber, (Henke et al., 2016b) observe that many companies have failed to achieve substantial gains from their investments in advanced data analytics and artificial intelligence. Despite 85% of executives believing that artificial intelligence would improve competitive advantage for their company; only 19% (Pioneers) have widely integrated AI into their business processes; 32% (Investigators) are at the piloting stage with AI; 13% lack deep understanding of AI but are experimenting; and 36% with little understanding of AI and not even experimenting (Ransbotham et al., 2017). Other than the star performers, there appears to be a mismatch between the hype and the reality. It may be an indication of the maturity of the market in relation to adoption of data driven technologies.

*Reliance on abundance of data*

With a doubling of the volume of stored data rising to 44 trillion gigabytes by 2020 (IDC, 2014), as a central plank for the growth of data driven business’, there is a question as to how much of this growth relies on consumers allowing their data to be acquired, processed and distributed. Every hour 2.5 petabytes (million gigabytes) of customer data is created by one of the largest retail giants in the world, Walmart (McAfee and Brynjolfsson, 2012). However, with this immense growth in data acquisition, there are growing concerns with regard to data privacy (Belanger et al., 2002). The continued harvesting of consumer data is subject to being permitted to do so in an increasingly regulated environment.

*Lack of data scientists and analytics tools*

(Erevelles et al., 2016) conclude that challenges to marketers capitalising on big data include an inadequate supply of data scientists, a lack of appropriate database management tools to support strategic data based decision making and the lack of strategic business decisions based on data analysis. The conclusions drawn by Erevelles et al are perhaps an indication of the early phase of the growth of data science which are likely to self-correct towards meeting market demand.
Environmental cost of data storage
The rate at which data is being collected and stored is increasing and it is estimated that it will amount to 44 zettabytes (44 trillion gigabytes) by 2020 (IDC, 2014). Though one of data centre players, Google, is using its AI to optimise its data centre energy consumption, the power required is similar to that required for a city, and the greenhouse gas emissions produced globally by data centres are calculated to be approximately 2%, which is the same as the aviation industry (Shead, 2016).

Threats
Regulation
There is a sense that the long run of light touch or out of reach regulation enjoyed by highly successful internet companies such as, Google, Apple, Facebook and Amazon, GAFA as they have become known widely in the press particularly in the EU, may be drawing to a close. If the extensive range of data privacy and data protection regulations and the supporting regulatory infrastructure alone were insufficient for large and hugely successful internet companies to sit up and take notice, the appetite in the EU for taking on American technology titans is large, as evidenced by the imposition by the EU competition commissioner, Margrethe Vestager of a €13 billion euro penalty for tax irregularities on the Apple Group companies, Apple Operations Ireland and Apple Sales International (Vestager, 2017). The evidence suggests that the internet titans are acutely aware of the regulatory threats they potentially face, for example, Alphabet Inc. specified risks arising from changes to the regulatory environment amongst its 10 pages of risks in its 2017 annual report (Alphabet, 2017), made all the more real by the 2.4 billion euro antitrust fine and forced changes imposed by the EU competition Commissioner. The reality of regulatory threats could intensify for Google as the EU Competition Commissioner has not ruled out breaking up the company amidst worries over the company’s dominance (Crisp, 2018). In the United States the traditional reluctance to impose effective regulation on technology giants, as evidenced by the difficulty encountered with the introduction of the self-regulating Do not track rule and the respective roles of Regulator and Congress (Tsukayama, 2012), seems to be changing, though not as quickly as in the EU.

The Federal Trade Commission in the United States required Google to change its anti-competitive practice of seeking injunctions to block rivals’ use of patents it acquired as part of the acquisition of the company, Motor Mobility (MMI) that was obligated as an industry standard setter enabling interoperability of devices to fairly, reasonably and non-discriminatorily licence the patents (FTC, 2013). Findings by the FTC that Google’s contractual terms hampered advertisers use of competitor platforms, potentially negatively impacting competition, required Google to make changes to assuage the concerns of the
FTC, while the investigation into search bias was closed on the basis that the practice was justified on the grounds of innovation and better user experience (FTC, 2013).

Regulators in the United States have become more active in enforcing data related regulations also. Data brokers in the United States, in the business of acquiring, processing and distributing billions of personal data items, have come under the scrutiny of the Federal Trade Commission (Ramirez et al., 2014). The FTC report calls for the American Congress to legislate for an increase the data and privacy protection for individuals (Ramirez et al., 2014) to that which is broadly in-line with the EU’s GDPR.

In 2015 another US agency, the Federal Communications Commission (FCC) effectively broadened its definition of personal information when it fined AT&T $25 million dollars due to a data breach but crucially also included the breach of personal information including social security numbers (Ruckman and Dhaliwal, 2015).

GDPR, the general data privacy regulation (enforcement date May 25th, 2018), introduces is the latest in a range of data privacy initiatives (Finn and Wadhwa, 2014). While GDPR has been the subject of much industry and academic interest and debate in advance of its commencement, the essential principles of GDPR are rooted in the Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data, produced by the OECD and endorsed by both the US and the EU in 1980 (OECD, ND).

GDPR potentially comes into conflict with some of the data driven business practises and activities where personally identifiable information, be it user or customer data, employee data or the personally identifiable information of any person such as suppliers or distributors or any natural person in the EU for whom they collect, process or distribute that information. While GDPR embodies many of the principles of the preceding data privacy and data protection initiatives, it is perhaps the most far reaching of any of its predecessors.

GDPR operates with the backing of the ECJ (European Court of Justice) (IAPP, 2018) and provides for penalties of up a maximum of 20 million Euros or 4% of global turnover, whichever is the greater (EUGDPR.ORG, ND). Organisations operating inside or outside of the EU that offer goods and services or track the behaviour of persons residing in the EU are subject to GDPR (EUGDPR.ORG, ND). This makes many if not all the major internet companies liable if they do not comply with the EU regulations. GDPR is impressive in its breadth and equally in its supporting regulatory infrastructure, which compares in scale to the regulatory structures for other markets including telecommunications, energy and finance (Hofheinz and Mandel, 2015).
Negative Media Exposure

Cambridge Analytica, a London based data analytics company became the centre of a media storm in March of 2018, involving the unauthorised usage of 78 million Facebook users’ accounts in the alleged manipulation of voters in the 2016 US presidential elections and potentially the BREXIT referendum. Cambridge Analytica was hired by Donald Trump’s campaign team which used Facebook’s algorithm to target voters with propaganda favouring Trump (Economist, 2016). It is also reported by the Guardian newspaper that Facebook has been aware of this data breach since 2015, taking action to suspend Cambridge Analytica only in March 2018, and that the fallout of the scandal has resulted in Facebook’s stock plummeting by billions of dollars (Greenfield, 2018), albeit temporarily. The New York Times reported on a twitter campaign to delete Facebook, supported by long time Facebook critics and promoters of privacy protection, though noting the muted responses from other technology internet giants whose data driven business models are not so different from Facebook’s (Wingfield, 2018).

Cyber-attack threats

CSO, the security information arm of the Chinese owned Technology Media company IDG, lists the 17 largest data breaches so far in the 21st century up to January 2018, the size of the breaches ranging from 22 million to 3 billion users’ data being exposed to cyber criminals (Armerding, 2018). The World Economic Forum (WEF), in 2018 highlighted that the chief risk to global stability is cyberattacks from criminals or rogue states citing thousands of attacks every month on critical infrastructure in the EU and US (Morris, 2018). The cost of cybercrime is expected to double from 3 trillion dollars in 2015 to 6 trillion dollars in 2021 (Daughters, 2017).

<table>
<thead>
<tr>
<th>No. of users’ data stolen/other impacts</th>
<th>Company</th>
<th>Attack type</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>3,000,000,000</td>
<td>Yahoo</td>
<td>Hacked user accounts</td>
<td>2013-2014</td>
</tr>
<tr>
<td>412,200,000</td>
<td>Adult Friend Finder</td>
<td>Weak password protection algorithm hacked</td>
<td>2016</td>
</tr>
<tr>
<td>145,000,000</td>
<td>eBay</td>
<td>Use of employee credentials</td>
<td>2014</td>
</tr>
<tr>
<td>134,000,000</td>
<td>Heartland Payments</td>
<td>SQL injection</td>
<td>2008</td>
</tr>
<tr>
<td>110,000,000</td>
<td>Target Stores</td>
<td>Access gained through 3rd party contractor</td>
<td>2013</td>
</tr>
<tr>
<td>94,000,000</td>
<td>TJX Companies, Inc.</td>
<td>Weak data encryption targeted</td>
<td>2006</td>
</tr>
<tr>
<td>78,800,000</td>
<td>Anthem</td>
<td>Phishing mail</td>
<td>2015</td>
</tr>
<tr>
<td>77,000,000</td>
<td>Sony PlayStation’s Network</td>
<td>Hacked</td>
<td>2011</td>
</tr>
<tr>
<td>76,000,000 Plus 7,000,000 small businesses</td>
<td>JP Morgan Chase</td>
<td>Servers hacked</td>
<td>2014</td>
</tr>
<tr>
<td>57,600,000</td>
<td>Uber</td>
<td>Accessed Uber’s AWS account</td>
<td>2016</td>
</tr>
</tbody>
</table>
If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane

<table>
<thead>
<tr>
<th>Date</th>
<th>Company</th>
<th>Description</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>56,000,000</td>
<td>Home Depot</td>
<td>Malware posing as anti-virus software</td>
<td>2014</td>
</tr>
<tr>
<td>40,000,000</td>
<td>RSA Security</td>
<td>Phishing attack</td>
<td>2011</td>
</tr>
<tr>
<td>38,000,000</td>
<td>ADOBE</td>
<td>Hacked</td>
<td>2013</td>
</tr>
<tr>
<td>22,000,000</td>
<td>US Office of Personnel Management (OPM)</td>
<td>Chinese Hacker</td>
<td>2012-2014</td>
</tr>
<tr>
<td>209,000</td>
<td>Equifax</td>
<td>3rd party Vendor hack</td>
<td>2017</td>
</tr>
<tr>
<td>Undisclosed data stolen</td>
<td>Verisign</td>
<td>Unauthorised access to systems</td>
<td>2010</td>
</tr>
<tr>
<td>Destroyed 984 uranium enriched centrifuges</td>
<td>Stuxnet</td>
<td>Computer virus (Worm) attack by US and Israel on Iran’s Nuclear programme</td>
<td>2005-2010</td>
</tr>
</tbody>
</table>

Table 5 Adapted from (Armerding, 2018) – 17 largest data breaches 2000-January 2018.

It is clear that cyber-attacks are very real and have the capability to deliver widespread financial damage to millions of users of online services. The indications are that reputational damage to online companies comes at a very steep price too. In Yahoo’s case it is estimated that in the region of €350 million dollars was wiped off the price when being sold to Verizon (Armerding, 2018), though it’s not possible to fully attribute this valuation adjustment to the enormous data breach, it is consistent with the timescale. In the era of GDPR, had there been data breach with victims based in the EU, there would be potentially be an additional fine of 4% of global revenue or 20 million euro.

The financial crisis of 2007-8 is instructive when considering the views expressed by the Davos delegates at the World Economic Forum regarding the threat of cyberattacks on global stability. (Gillespie et al., 2012) refer to the destruction of 4.1 trillion dollars in global wealth, according to the International Monetary Fund’s (IMF) estimate, and the failure of hundreds of companies, large and small, loss of jobs, homes and financial security, as a result of a huge organisational systems level trust failure. It could be argued that the global financial system is a subset of the data systems and networks (including defence, energy, commerce, transport and others) which may become vulnerable to the constant and increasingly complex cyberattacks, with even more devastating consequences.

The Effects of GDPR on data driven business

Effect of GDPR on the Benefits of Data Driven Business

The obligation placed on all organisations to meet the regulation with regard to 1) Lawfulness of processing; 2) meeting conditions for consent; 3) Processing special categories; 4) Transparency; 5) Providing privacy information and access to the data owner; 6) Capabilities for rectification and erasure; 7) Right to object and restrict data processing 8) Restrictions around automated decision making; 9) Organisational structures, such as appointing a Data Protection Officer, and establishing processes and procedures to ensure accountability, has the potential to have a greater impact on data driven businesses.
An industry commissioned report, produced by (Deloitte, 2013), representing the potential economic impacts of GDPR on the data analytics industry, particularly 1) Data marketing; 2) Online Behavioural Advertising; 3) Web Analytics and; 4) Credit Information, identified a number of negative impacts including:

- 85% reduction in users allowing behavioural analytics
- 69% reduction in users allowing web analysis
- 34% reduction in users allowing direct marketing
- €173 billion reduction in GDP
- 2.8 million jobs lost

While the full effects of GDPR remain to be seen, and those presented by (Deloitte, 2013) appear dramatic, their report captures explicit concerns and potential economic impacts of the implementation of GDPR.

Figure 6 Share of the digital advertising market (Desjardins, 2016)
If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane

Figure 11 illustrates the competitive landscape for digital advertising, identifying Google and Facebook as the largest players in 2015 (Desjardins, 2016) and market growth in the region of $228 billion in 2017.

**Effects of GDPR on the Weaknesses of Data Driven Business**

The fact that data analytics is failing to meet the expected growth targets generally, due potentially to the complexity and lack of expertise (Henke et al., 2016a), may be further encumbered by the additional risk of regulatory penalties and reputation damage as well as the additional cost to an already potentially considerable cost of embedding data analytics in an organisation and transforming the organisation to take full advantage of data driven decisions. While (Henke et al., 2016a) and (Erevelles et al., 2016) present a 4th industrial revolution that is a tad tardy, in part due to lack of tools and data scientists, it may not be fully reflective of the data driven business of analytics premium exponents such as those referred to as GAFA, Google, Apple, Facebook and Amazon.

The rebalancing of the privacy equation in favour of the user as put into effect by GDPR has the potential to affect the volume and richness of personal data on which data driven business thrives.

**The Effects of GDPR on the Threats to Data Driven Business**

GDPR is concerned with data privacy and protection, and it clearly places obligations on organisations to better protect personal data. Table (5) lists the most serious data breaches in the 21st century up to January, (Armerding, 2018), and identifies a degree of laxity in the protection of personal data. The largest breach recorded, compromising 3 billion users’ names, dates of birth, email addresses and passwords, that by the company’s own admission were protected less well than those of earlier breaches (Armerding, 2018). The Equifax data breach affecting 143 million consumers included such important personal information such as social security numbers and credit card numbers, and the Heartland payment systems breach also including credit card numbers were blamed on an application vulnerability, and widely forewarned vulnerability called SQL injection (Armerding, 2018).

Improving data protection to point of acceptability by GDPR is not without its costs but it is an even playing field in that it applies equally to every organisation handling personal data. Therefore, the costs of information security will go up and those that are better at securing personal data may find that consumers have increased confidence in them with regard to handling their personal data.

The impact of GDPR on the potential negative media exposure that might be experienced by data driven companies may potentially increase as the acceptable standard of behaviour in relation to data privacy and protection has dramatically increased, and may be difficult to achieve.
Conclusion

Chapter 2 explains the nature of data driven business and identifies opportunities, weakness and threats to the burgeoning information age, data analytics and data driven business, and identifies the potential impacts of GDPR in terms of stemming the flow of data, mass adoption of opting out of online behavioural and web analytics, large GDP and job losses and damaging negative media exposure due to difficult to meet standards.
Chapter 3: A Trustworthiness Model for data Privacy and protection

Introduction
The conclusion in Chapter 2 exposed the potential for large scale job losses in key areas of analytics and therefore in data driven business, resulting in €170 billion in losses to GDP due to the entitlement of users to opt out of online behavioural analytics, web analytics and direct marketing, reducing the flow of data and damaging media exposure due to inability to meet new standards. The purpose of this chapter is to construct a framework which aids the understanding of how the concepts central to trustworthiness applies in the context of data privacy and protection. The creation of this model draws on previous work on the construction of trust or trustworthiness frameworks by (Ennew and Sekhon, 2007), (Hurley, 2006), and model by (Van der Merwe, 2013), and taking direction from the measurement methods of (Roy and Shekhar, 2010).

Investigation of trust and trustworthiness models
This study seeks to simplify the approach to trustworthiness by using the ample research on dimensions, elements and antecedents of trust and building these into a model which enables companies to demonstrate their trustworthiness. In essence, this study proposes to acknowledge and detail the characteristics and factors influencing the trustor aspects of the trustworthiness relationship but ultimately de-emphasise the variable of trustors’ perception and instead proposes an evidence based approach to trustworthiness which focuses on the organisation and is independent of the perceptions of the trustor or user. This is consistent with the approach proposed by (O’Neill, 2013), seeking the provision of evidence as a critical element in proving trustworthiness and the assertion by (Van der Merwe, 2013) that trustworthiness is demonstrable, and points in the direction of focusing on factors or dimensions that lie in the organisation domain rather than in the users domain.

Organisational and User domains
A framework for measuring trust in financial services as depicted in figure (7), constructed by (Ennew and Sekhon, 2007) is organised along similar lines to the framework proposed for this study. Dimensions of trustworthiness are clearly in the domain of the organisation and distinct from the factors contributing to the trust the consumer has in the organisation. Therefore, separating the dimensions of trust / trustworthiness into organisational and user domains can be particularly useful in terms of examining and evaluating the level of trustworthiness of an organisation.
If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane

(Van der Merwe, 2013) propose a conceptual model of trustworthiness leading to corporate trust which is represented in Figure (8), portraying the interrelationship between the characteristics of trustworthiness and key antecedents which are inclusive of some of those proposed by (Ennew and Sekhon, 2007). All the characteristics and antecedents are in the organisational realm and under the influence of the organisation. That is to say that vision and values of the organisation leading to communication and behaviours based on the characteristics and antecedents of trustworthiness as listed by (Van der Merwe, 2013) can be put into effect to a greater or lesser degree by the actions of the organisation. As (O'Neill, 2013) makes clear, it is up to the trustee to prove their trustworthiness. While influence may be brought to bear on the organisation by user feedback or media endorsement of good practise and outrage at poor practise, trustworthiness lies in the domain of the organisation.
Constructing a data privacy and protection model

Model, Concept or Theory

(Ngulube et al., 2015), investigating the use of conceptual and theoretical models and frameworks, argue that a model is constructed based on experience of the world, which may be used to derive a concept and that a collection of concepts may be used in the definition or explanation of a phenomenon, and this is referred to as a theory.

As a basis for creating a useful model from which to examine data privacy and protection of data driven businesses in the context of GDPR, it is important perhaps to give some consideration to understanding the plane on which to situate that model.

The primary organising focus of this study centres around increasing understanding of the concept of trustworthiness and its relationship to newly introduced principles for regulating data privacy and protection of people residing within the EU. (Ngulube et al., 2015), reviewing literature concerning theoretical and conceptual frameworks, present the confusion of contradictory views, but manage to define concepts as ‘labels that we assign to dimensions or elements in the real world’ and conclude that the key distinction between conceptual and theoretical frameworks is that the focus of the former is mainly concerned with qualitative research and the latter is more concerned with quantitative research, while both are concerned with mixed methods research. (Lester, 2005) distinguishes between conceptual and theoretical frameworks in terms of their purpose, clarifying that the intention of conceptual frameworks is explanation and the intention of theoretical frameworks is justification.

Not many theorists attempt to disentangle the nature of frameworks versus models. However, (Jabareen, 2009) proposes to reserve for frameworks, the exclusivity of dealing solely with concepts, whereas models are permitted to include the use of variables and factors. The structure used in this study to help describe the relationship between trustworthiness, data driven business models and GDPR, includes concepts, factors, variables and principles of regulation as well as an external organisational entity which places it more in the realm of model rather than framework.

The nature of this study is the provide an explanation of trustworthiness in the specific online context of data privacy and protection as it pertains to data driven businesses.

Data Privacy and protection Trustworthiness Model

When considering the construction of a conceptual model to apply to data privacy and protection, (Hurley, 2006) provides a clue to a central concept when he makes a distinction between situational factors and decision-maker factors, though it needs to be adapted for a data privacy and protection model. In Hurley’s framework, there is a split between
If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane

exclusively trustor factors and a combination of trustor and trustee factors. From the data privacy and protection perspective, the notion of situational factors or context, as central to the concept of trust, according to (Rousseau et al., 1998), is particularly important given the capacity for devices such as smart devices to gather personal data, will form a foundational construct of the model.

As part of the literature research in Chapter 1, the work of various authors characterise as dimensions, factors, concepts, antecedents, characteristics and elements, the aspects of trust and trustworthiness they have chosen to examine, some of which are represented graphically as models and frameworks. Also, consideration was given to the principles of GDPR being foundational antecedents to trustworthiness. It is perhaps even more useful to consider that the principles of GDPR provide a data privacy and protection lens through which to examine the difficult area of the context of trustworthiness in the area of online data driven businesses.

(Van der Merwe, 2013) features the concept of trustworthiness in their model and (Ennew and Sekhon, 2007) feature centrally, the concepts of trust and trustworthiness while acknowledging the cognitive and affective factors of the customer as distinct and visually separate from trustworthiness. (Van der Merwe, 2013) identifies an array of characteristics and key antecedents to trustworthiness in their conceptual model, progressing to corporate reputation but exclude the user perspective.

The model proposed in this research seeks to provide a representation to aid understanding of trustworthiness of data driven organisations in light of GDPR. The model identifies key trustworthiness concepts evaluated in the literature review in Chapter 1, placed in the organisation domain. The central position of context, containing the principles of GDPR, and its connection to both trustworthiness concepts and user trust factors, is therefore in the organisation domain. For completeness, the user factors, also evaluated in the literature review in Chapter 1 are specified but are not the main focus of this research.
If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane.

Table (9) compiles the justifications for teasing apart the aggregation of the aspects of trustworthiness and assigning them positions/domains in the trustworthiness model. Without any difficulty, the elements identified by (O'Neill, 2013) amongst others: honesty, competence, benevolence, and reliability can be readily situated in the organisation domain as they are directly under the sphere of influence of the organisation.

Pre-GDPR, Power/vulnerability, context, and risk would be under the control of the organisation. However, GDPR has re-defined the data privacy, and protection context embodied in its principles and therefore holds a central, pivotal position in the model albeit still within the control of the organisation but also under the watchful eye of the Data Protection Commissioner.

The data privacy and protection obligations placed on the organisation and the rights granted to the user by GDPR, not only alter the context, they also have the potential to change the power/vulnerability relationship and influence the risks faced by the user. Vulnerability, as presented by (O'Neill, 2013) is proactive. As discussed previously, compliance with GDPR may be reasonably considered to be an antecedent of trustworthiness, but the question arises as to whether mere compliance is sufficient or whether a further degree of vulnerability beyond the requirements of GDPR is necessary in order to fulfil the power/vulnerability aspect of trustworthiness. Therefore, the power/vulnerability aspect of trustworthiness lies within the organisation domain though is heavily moderated by the GDPR principles' influence on the context of the data privacy and protection relationship between the organisation and the user.
Compliance with GDPR may serve a similar function to the Perceived Effectiveness of E-commerce Institutional Mechanisms (PEEIM) examined by (Yulin et al., 2014), reducing perceived risk and thus reducing the need to question the trustworthiness of the organisation. Also, grey or less explicit areas within the regulation may allow for legal challenges.

<table>
<thead>
<tr>
<th>Trustworthiness</th>
<th>Trustworthiness model consideration</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Honesty</td>
<td>Includes ethics, fairness in the control of the organisation.</td>
<td>Organisation</td>
</tr>
<tr>
<td>Competence</td>
<td>The competence of the organisation is fundamental to being worthy of managing personal data of the user.</td>
<td>Organisation</td>
</tr>
<tr>
<td>Benevolence</td>
<td>Central to how an organisation perceives, respects and protects the customer’s interests regarding their personal and data</td>
<td>Organisation</td>
</tr>
<tr>
<td>Reliability</td>
<td>The organisation must be consistently trustworthy regarding its behaviour towards personal data enabling the user to have a reasonable expectation that the trustworthy behaviour will continue into the future.</td>
<td>Organisation</td>
</tr>
<tr>
<td>Power/Vulnerability</td>
<td>Compliance with GDPR rebalances the personal data power/vulnerability relationship to the extent that new obligations are placed on the organisation, and new rights are granted to the user. Vulnerability, in the realm of trustworthiness, as presented by (O’Neill, 2013) is more proactive than simply compliance with GDPR. Also, grey areas may allow for legal challenges.</td>
<td>Organisation</td>
</tr>
<tr>
<td>Context</td>
<td>The data privacy and protection context is created by organisations but GDPR defines and regulates it. Context is therefore pivotal to a data privacy and protection model examining trustworthiness, in light of GDPR. Context is layered in hardware, software, internationally agreed telecommunications standards and protocols and also the service or product offering. While some aspects of context are rapidly changeable, service terms and conditions for example, others such as internationally agreed standards and regulations are less so.</td>
<td>Organisation and a central pivotal element defined by GDPR</td>
</tr>
<tr>
<td>Risk</td>
<td>Without risk, there is no need for trust according to (Hurley, No Date). With the pervasiveness of data acquisition, analytics and emergence of AI, risk to data privacy and protection can only be considered high, though moderated by GDPR. In the context of data privacy and protection risk is almost synonymous with trust. The greater the risk, the greater the need for trust and therefore the greater need to be trustworthy. Therefore, the risk to the user is determined by the action or inaction of the organisation. A question arises as to whether risk is implicit or whether adding ‘risk to the model serves to enhance clarity.</td>
<td>As risk is implicit in to the concept of trust and inclusion does not enhance the clarity or validity of the model, it has been omitted from the model.</td>
</tr>
<tr>
<td>Communication/ Openness</td>
<td>Similar to context, communication in relation to data privacy and protection is within the control of the organisation though more determining how open, clear, forthright the organisation is with the user. It conveys or obscures the trustworthiness characteristics of the organisation to the customer.</td>
<td>Organisation</td>
</tr>
<tr>
<td>Identification</td>
<td>Identification, being an antecedent to trustworthiness whereby stakeholders positively share the values espoused by the organisation to the point where they identify with it (Van der Merwe, 2013) places it as a user response to the organisation, therefore belonging in the user domain.</td>
<td>User</td>
</tr>
</tbody>
</table>
Calculative trust is a potential approach to a data privacy and protection risk situation by a user or customer. Risk tolerance is a disposition of the user towards risk generally which is multi-factorially based. Alignment of interests centres around the transparency of true nature of the relationship between the trustor and the trustee (Hurley, No Date) and as such is bound up with honesty and communication and it is questionable as to whether its inclusion adds to the model. Emotional attraction refers to how much the users like what the organisation stands for; its values; its vision; how it behaves; and the way it communicates (Van der Merwe, 2013). Therefore, in terms of data privacy and protection, it is a user reaction to the organisation’s trustworthiness.

Identification, calculative trust, risk tolerance, and emotional attraction belong in the user domain as they are user approaches, dispositions, or responses to the organisation.

Alignment of interests centres around the transparency of the true nature of the relationship between the trustor and the trustee (Hurley, ND) and as such is bound up with honesty and communication and it is questionable as to whether its inclusion adds to the model, therefore it has been excluded.

(O’Neill, 2013) values evidence as a key aspect of trustworthiness. Similarly, (Van der Merwe, 2013) argue for antecedents of trustworthiness that are demonstrable. Without evidence, there is scope for misalignment between intention and reality. Policies and processes to implement trustworthiness may be circumvented or abandoned without monitoring and enforcement. Therefore, the model features a linkage between evidence and the GDPR principle of accountability.

**Evaluation of the Data Privacy and Protection Trustworthiness Model**
(Mayer, 1989) identified seven criteria for evaluating models which are applied to the data privacy and protection trustworthiness model in Table (7).

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Description</th>
<th>Trustworthiness Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete</td>
<td>All the essential elements must be included and important relationships identified.</td>
<td>The data privacy and protection trustworthiness model includes all the characteristics of trustworthiness, variously described as factors, antecedents, characteristics, dimensions, and elements, while allowing for synonyms and similar concepts, all of which is based on a representative literature review of trust and</td>
</tr>
</tbody>
</table>
If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concise</td>
<td>The appropriate level of detail to explain the key characteristics is required.</td>
<td>The model represents the domains of the relationship between user and organisation or enterprise and organises at a conceptual level the constituent characteristics or factors in each domain avoiding the detail of, for example, the articles of GDPR, which enables a simpler accessible structure.</td>
</tr>
<tr>
<td>Coherent</td>
<td>The elements, and the rules of how they interact must be logical, intuitive and transparent.</td>
<td>The coherence of the model lies in representing the GDPR principles as the defining context of the relationship between the user domain and the enterprise or organisation’s domain.</td>
</tr>
<tr>
<td>Concrete</td>
<td>Models, including physical and visual must be represented at a level that is appropriate to the user.</td>
<td>The data privacy and protection trustworthiness model is based on existing more general trust and trustworthiness models identifying the characteristics or elements of the central concepts at a level that is readily accessible and understandable. The context of the relationship, the definition of which is aided by GDPR is the central feature of the model.</td>
</tr>
<tr>
<td>Conceptual</td>
<td>Good models should have a meaningful basis, i.e., providing an explanation of a system.</td>
<td>The value of the model is that it has a specific relevance for the data privacy and protection domain and the representation of the model facilitates better understanding of and the locus of the issues central to trust and trustworthiness in this particular domain.</td>
</tr>
<tr>
<td>Correct</td>
<td>There should be a good correspondence between actual real-world phenomena or events and their representation in the model.</td>
<td>The real-world context for trustworthiness of data privacy and protection for data driven business in the online environment is the smart device, now regulated by GDPR, has a central position in the model which connects each but also separates organisational elements of trustworthiness from the user centric factors in the relationship.</td>
</tr>
<tr>
<td>Considerate</td>
<td>A good model should represent the system or objects and their relationship at a level that is appropriate to the user.</td>
<td>The model is representative at a conceptual level of the interplay of sets of characteristics, concepts and factors and where they reside in the relationship between users and organisations or enterprises. The sets of characteristics, concepts, and factors can be further decomposed to policies, processes, behaviours, values or biases particular to an audience wishing to apply the model with a view to evaluating the trustworthiness or an organisation or enterprise.</td>
</tr>
</tbody>
</table>

Table 7 seven criteria for evaluating models (Mayer, 1989) applied to the data privacy and protection trustworthiness model.

(Whetton, 1989), when judging conceptual research expects that the research should contribute something new. The data privacy and protection trustworthiness model extends the existing models for trustworthiness by extending the tailored sets of trustworthiness characteristics of organisations in a separate domain from user factors relating to trust, and centrally places context as defined by the principles of GDPR between the two domains. The model also shows the interrelationship of the key elements of the model. While the focus of this research is not primarily concerned with them, user factors are included in the model to complete the picture.
An approach to measuring Trustworthiness

Leaving assessment or measurement of compliance with GDPR to the eager service of the consultancy firms, this research proposes to examine an approach for capturing a view of the level of trustworthiness of an organisation. (Hurley, 2006) and (Ennew and Sekhon, 2007) provide some guidance as to the method for gaining insight into trustworthiness using the interrogative method.

(Hurley, 2006) proposes a model as presented in Figure (10), for identifying the trust between individuals based on questioning the level of trust factors relating to the trustor; whether their risk tolerance is low or high; whether the well-adjustedness of the trustor could be described as low or high; and whether the power of the trustor is low or high relative to the trustee. Similarly, using a simple scale from low to high (Hurley, 2006)’s model provides the opportunity to examine the situational factors such as feelings of security between the two parties, similarities, alignment of interests and communication. Hurley’s model for evaluating trust relationships and takes both sides of the relationship into account.

(Ennew and Sekhon, 2007), rather than providing a simple scale as in Hurley’s model, ask a sample population of customers the strength with which they agree or disagree with trust and trustworthiness statements, and statements regarding drivers of trustworthiness of their main bank, as per Table 8, and Table 9 respectively.
Measures of trust and trustworthiness

<table>
<thead>
<tr>
<th>My main bank….</th>
<th>Strongly Disagree</th>
<th>Neutral</th>
<th>Strongly Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>I trust my bank to do what is says it will do</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>I trust my bank to have my best interests at heart</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>My bank is very reliable</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>My bank is always honest with me</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>My bank is concerned about my best interests</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Overall, I feel I can trust my bank</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>My bank makes every effort to address my needs</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>My bank has a reputation for being reliable</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>My bank has a reputation for being honest</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>My bank has a reputation for being dependable</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>My bank has a reputation for looking after its customer</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>My bank has a reputation for having its customers interests at heart</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Overall, I feel my bank is trustworthy</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

Table 8 Measures of trust and trustworthiness of banks (Ennew and Sekhon, 2007)

<table>
<thead>
<tr>
<th>My main bank …</th>
<th>Strongly Disagree</th>
<th>Neutral</th>
<th>Strongly Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>My bank does whatever it takes to make me happy</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Keeps its word</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Acts in the best interest of its customers</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Shows high integrity</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Is honest</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Conducts transactions fairly.</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Has the information it needs to conduct its business.</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Is consistent in what it does.</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Can be relied upon to give honest advice.</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Shows respect for the customers.</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Treats its customers fairly.</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Has the same concerns as me.</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Is receptive to my needs.</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Competently handles all my requests.</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Is efficient.</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Communicates clearly.</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Is responsive when contacted.</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Informs me immediately of any problems.</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Has the same values as mine.</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Informs me immediately of new developments.</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>
If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane.

<table>
<thead>
<tr>
<th>Act as I would.</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is knowledgeable.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Communicates regularly.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

Table 9 Measures of the drivers of trustworthiness of banks (Ennew and Sekhon, 2007)

The evidence in the approach taken by (Ennew and Sekhon, 2007) is provided by the opinion or the perception of the customer, i.e., the trustor. (Van der Merwe, 2013) and (O'Neill, 2013) take an approach that is different. They present a view that trustworthiness is demonstrable (Van der Merwe, 2013) and requires evidence (O'Neill, 2013).

In order to translate the combination of (Hurley, No Date), (Ennew and Sekhon, 2007), (Van der Merwe, 2013) and (O'Neill, 2013)'s work into an approach that is practical and can usefully be applied by an organisation to itself, it is necessary to exclude statements regarding factors relating to trustworthiness that are based in the user domain, i.e. sharing the same values, concerns and acting in the same way the customer would. Also, the 1 – 5 scale used by (Ennew and Sekhon, 2007) based on the degree to which the customer agrees or disagrees with the statement relating to the trustworthiness of the bank is based on the strength of customer perception. It is potentially more useful to the organisation to be more specific when asking the questions of itself. After all, the organisation or an auditor would have greater access to internal policies and processes and resulting documents, communications and behaviours, to find evidence to give a better view of the trustworthiness of the organisation to itself.

While there is a degree of overlap amongst the concepts of trustworthiness, and though all need to be present in order to be deemed to be trustworthy (Van der Merwe, 2013), it is useful, if an organisation is striving to be trustworthy, to be able to drill down to the points of failure in order to focus on fixing them. Therefore, it is perhaps useful to gather together statements elucidated in the literature review in chapter 1 that are used to explain the constituent concepts that make up trustworthiness and make a declaration that can be associated with a status, such as very honest; quite honest; unproven honesty; quite dishonest; or very dishonest., for example, as illustrated in Table 10. Using a scale of -2 to +2 is also more immediately informative and captures not just a poor score but the active nature of the status, in this example, to be proven to be actively dishonest in this aspect of honesty, i.e., the organisation does not do what it says most of the time. Choosing a scale of -2 to +2 links to reasonable semantic understanding of how honest an organisation may be. It would be difficult to readily understand or elicit value from a score of -8 from a larger scale of -9 to +9, for example.

<table>
<thead>
<tr>
<th>Very Dishonest</th>
<th>Quite Dishonest</th>
<th>Unproven Honesty</th>
<th>Quite Honest</th>
<th>Very Honest</th>
</tr>
</thead>
<tbody>
<tr>
<td>-2</td>
<td>-1</td>
<td>0</td>
<td>+1</td>
<td>+2</td>
</tr>
</tbody>
</table>
If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane

<table>
<thead>
<tr>
<th>Proven that words and actions are NOT congruent most of the time</th>
<th>Proven that words and actions are Not congruent at times</th>
<th>Not Proven that words and actions are congruent</th>
<th>Proven that words and actions ARE congruent most of the time</th>
<th>Proven that words and actions ARE always congruent</th>
</tr>
</thead>
</table>

Table 10 Sample Honesty status statements

See Appendix (1) for further proposed trustworthiness sample statements related to the trustworthiness concepts.

Evidence of trustworthiness or untrustworthiness

Regulatory Sources

It is possible to find evidence of whether an organisation should be considered trustworthy or not. Regulatory enforcement organisations, whose job it is to police corporate compliance, such as the Federal Trade Commission (FTC) and the EU Competition Commission, publish reports regarding their investigations and findings, which can provide evidence to be used in determining whether an organisation is trustworthy or not.

The FTC found against Facebook on eight complaints in relation to the use of deception or false or misleading statements in regarding data privacy. These findings traverse all of the dimensions of trustworthiness as presented in Table 11 (Leibowitz et al., 2012). The FTC found that Google misrepresented privacy assurances made to users resulting in a penalty of $22.5 million (FTC, 2012). Other findings of abuse of market dominance by Google are examples of dishonesty even if not specifically related to data privacy and protection (Chee, 2017).

<table>
<thead>
<tr>
<th>Honesty</th>
<th>Examples of evidence – Facebook (Leibowitz et al., 2012)</th>
<th>Examples of evidence – Google</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proven that words and actions are always congruent</td>
<td>The United Stated Federal Trade Commission’s 8 complaints traverse all central dimensions of trustworthiness: 1) Facebook found to have deceptive privacy settings. 2) Facebook’s unfair December 2009 privacy changes. 3) Facebook’s deceptive December 2009 privacy changes. 4) False and misleading statements with regard to platform applications having access to user profile information beyond what was needed to operate. 5) Facebook was false and misleading regarding the sharing about its users. User IDs were shared with the platform advertiser despite statements by Facebook that they shared only combined data that was anonymous.</td>
<td>Google pays a $22.5 million settlement to the FTC due to charges that it misrepresented privacy assurances to users of Apple’s Safari internet browser. (FTC, 2012) In 2017 Google is fined €2.4 billion by the European Commission for abusing its dominance in the search market. (Chee, 2017)</td>
</tr>
<tr>
<td>Proven to always adhere to facts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proven to be always open and honest in communication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proven to conduct itself fairly and in a straightforward manner at all times</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proven to respect the consumer’s privacy at all times and all circumstances</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proven to have benevolent concern for the well-being of the consumer at all times and in all circumstances</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proven to be able to provide the highest level of protection for consumers</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane.

Table 11 Examples of sources of evidence of trustworthiness

<table>
<thead>
<tr>
<th>Source of Evidence</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Statements</td>
<td>Facebook’s false or misleading representation of platform application’s security.</td>
</tr>
<tr>
<td></td>
<td>Contrary to their claims, Facebook continues to display users’ photos via Facebook’s Content URLs for them even after user accounts have been deleted.</td>
</tr>
<tr>
<td></td>
<td>Facebook engaged in unfair or deceptive acts or practices, in or affecting commerce, in violation of Section 5(a) of the Federal Trade Commission and contravening the U.S. Safe Harbour principles. (Leibowitz et al., 2012)</td>
</tr>
</tbody>
</table>

Privacy Statements

One of the changes made by Facebook, a high profile and globally widely used data driven business, in advance of the GDPR deadline, May 25th, was to offer face recognition as a means to enhance security as per the following press release.

‘Allowing face recognition technology. Our face recognition features help protect our privacy and improve your experiences, like detecting when others might be attempting to use your image as their profile picture and allowing us to suggest friends you may want to tag in photos or videos. We’ve offered products using face recognition in most of the world for more than six years. As part of this update, we’re now giving people in the EU and Canada the choice to turn on face recognition. Using face recognition is entirely optional for anyone on Facebook.’

(Egan and Beringer, 2018) Facebook

On the face of it and typical of the language used in online privacy statements, functionality is presented as a service in the above statement by Facebook. A casual reader might be
inclined to accept Facebook’s bona fides and agree to opt in to face recognition. However, if it were made explicit that an artificial intelligence algorithm, can be used to determine sexual orientation with 91% and 83% accuracy in men and women respectively (Wang and Kosinski, 2018), the reader would have more complete information with which to decide whether to opt in or not. Is it dishonest of Facebook not to disclose the potential use for facial photographs? If they had no knowledge of the current or future potential capability, then perhaps it displays incompetence rather than dishonesty. Is it reasonable to presume that Facebook is unaware of the work of Professor Kosinski, considering he is one of the academic figures associated with the Cambridge Analytica scandal (Lewis et al., 2018), about which the CEO was required to answer questions regarding privacy at a congressional hearing (Vanian, 2018), and EU Parliament (Rankin, 2018)?

Research contributing to the Cambridge Analytica by (Kosinski et al., 2013) found that Facebook’s ‘Likes’ functionality enables analysts to create a model which can predict to a high degree of accuracy, sexual orientation, ethnicity, and political preferences, i.e., whether Republican or Democrat. Further to the 2013 research, (Youyou et al., 2015) proved that that analysis of Facebook’s ‘Likes’ functionality is better at predicting personality than close friends and relations. Therefore, presenting face recognition technology simply as a data protection mechanism is not the whole story, based on the technical capability available to the organisation receiving this additional rich source of personal information and cannot be considered proven to be honest in terms of openness, clarity, and transparency.

Table 14 in Appendix (2) provides an overview of what types of data Facebook collects and how it processes that data based on Facebook’s Data Policy of February 2018 (Facebook, 2018). Facebook’s partnering with data brokers, Epsilon, Acxiom, and Datalogix adds shopper loyalty information to further enrich the personal data it already has (Delo, 2013). In an FTC report into transparency and accountability of data brokers, (Ramirez et al., 2014) found that Acxiom possesses ‘personal data on approximately 700 million people globally they store over 3000 data elements for almost every American consumer. This gives an insight into Facebook’s approach to personal data collection which could reasonably be characterised as gathering every possible piece of personal data it is possible to collect. With 2.19 billion active monthly users (Statista, 2018), the evidence prominently points to Facebook being a world class personal information collector. It is in this light that existing and newly offered functionality needs to be evaluated.

Google, similar to Facebook, gathers seemingly as much personal information as is possible, including device information, server log information, location information, system, and application information, and include the use of tracking technologies, according to its privacy policy as of February 2018 (Google, 2018). There is strong marketing feel to
Google’s privacy policy which in stark contrast to British Telecom for example. British Telecom’s (BT) privacy policy is clear and forthright and provides all information and options to make an informed decision about whether a user should provide personal information by segregating cookies into 1) Strictly necessary; 2) Performance; 3) Functionality; and 4) Targeting. Even from the high level list provided by BT it is possible to discern that 4) Targeting is related to direct advertising. BT further explain specifically what the cookies do and what they don’t and provides a list of all of the cookies. Google’s privacy policy obscures the doubtless similar categories of cookie which would render BT close to very honest but based on this comparison, the same could not be said for Google.

*Visibility of Trustworthiness*

From a trustworthiness perspective, perhaps not all companies will meet the criteria to be able to meet all the criteria to claim complete trustworthiness immediately. Having assessed the company’s trustworthiness, it may be useful it to represent organisation’s status at a point in time with a view to improving.

*Figure 11 Trustworthiness Tree*

Figure 14 offers a visual representation of the overall trustworthiness of a company that is doing poorly in relation to honesty and vulnerability and very poorly in relation to
benevolence, while doing moderately well in relation to reliability and communication and very well in relation to competence. At a glance, it is possible to see the overall status and identify where work needs to be done.

Conclusion

Chapter 3 presents a data privacy and protection trustworthiness model which identifies the central importance of context, particularly in the new era of GDPR and aids understanding of the new aspects of the relationship between the organisation and the user in terms of data privacy and data protection. An approach to measurement of the trustworthiness dimensions is proposed, identifying the usefulness of matching a scale of -2 to +2 to stated standards of behaviour. Evidence can be found to determine the level of trustworthiness of an organisation through published finding of the regulatory enforcement institutions and though close examination of the organisation’s privacy statements and public corporate actions. An organisation interested in improving its trustworthiness will have internal values, policies, procedures, and behaviours available to them as a source of evidence.
Chapter 4 Discussion

The aim of this research is to determine whether the concerns raised by GDPR for data driven business could be resolved by trustworthiness. The concerns identified, include impacts on the expected benefits that accrue due to data driven business, the weaknesses and the threats to data driven businesses.

Research Question Answered

This research addressed the question ‘Does trustworthiness resolve the concerns raised by GDPR for data driven businesses?’

In examining the potential impacts of GDPR on data driven businesses, the empowerment of the user, through the new rights granted by GDPR, requires an organisation to become trustworthy in order to appeal to the factors that influence whether a user or customer will place their trust in the organisation and continue to supply them with the raw material necessary for the organisation to survive and thrive. The analysis indicates that trustworthiness can be used as a source of competitive advantage.

Trustworthiness – and the benefits of data driven business

Analysis of the effects of GDPR on data driven business identified potentially serious negative economic impacts at the level of loss of billions of euro in GDP and large scale job loss based on the majority of users refusing permission for data analytics to be applied to personal information (Deloitte, 2013).

While there has been a 5% decline in the amount of time spent daily on Facebook in late 2017 and a fall in the number of Americans on the platform, which may reflect a maturing attitude among the public to the other pervasive negative aspects of social media such as trolling, hate speech, time-wasting and mental health issues (Sloane, 2018), marketers spent 47% more in 2017 than in 2016, totalling $40 billion revenues for Facebook in 2017. This makes it very clear who Facebook’s customers are.
If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane

However, while Porter’s value chain model, referred to in Chapter 2, excluding support activities, presents a linear process, the feedback loop of user analysis in data driven businesses potentially contributes not just targeted advertising but also to targeted product development, not to mention individualised pricing. Therefore, the data driven business value chain has a more complex relationship with their users as both a source of raw material, i.e., detailed personal information leading to design input and marketing, and user of internet services, be it social media or search functionality or productivity functionality such as e-mail. Though a form of this relationship already exists at a distance, it could be argued that the immediacy and the intimacy of the personal information delivered to the marketers and producers of products and services, alters the value chain and places the user or customer in a unique position. This is why there is an opportunity, referred to in the conclusions Competition & Markets Authority (CMA) in the United Kingdom, in their report on the Commercial use of consumer data, regarding empowerment of consumers and encouragement of competition to offer better services (CMA, 2015). Trustworthiness is an obvious basis on which organisations can compete for users and customers and this is at the forefront of research related to corporations and their responsibilities to society.

Trustworthiness in general, and in a data privacy and protection context in particular, is built on a highly attractive set of characteristics for a company to possess (Van der Merwe, 2013) and prove that it possesses. The importance of proof is supported by evidence provided by (DeSteno, 2014) who found that 90% of people, who consider themselves to be trustworthy will behave dishonestly if it is to their benefit and that those with more relative power and status will be more dishonest than those with less relative power and status. Also, how honest a person is, depends on who else is being honest or dishonest (Ariely, 2012). Therefore, given the human propensity for dishonesty in certain situations then it is rational to require proof.

To be considered trustworthy there are not insignificant choices to be made:

- Honest versus dishonest
- Benevolent towards your stakeholders including wider society concerns regarding sustainability as opposed to seek only profits
- Competent to deal with existing and future threats to personal data versus incompetent
- Reliable and consistent regarding to trustworthiness, versus changeable calculating and strategic
- Vulnerable to customers so they will feel empowered
- Communicate clearly, transparently, and openly rather than concealing real interests, beliefs and behaviours.
Fortunately, some insightful work has been done to evolve a framework for exploring this concept further.

**Strategy and Ethics**

(Porter and Kramer, 2011)’s work espouses a new form of capitalism, of a higher order that seeks competitive advantage through ‘Creating Shared Value’ (CSV), which is tightly entwined with reimagining and improving an organisation’s central and peripheral processes based on an integration with the societies with whom they interact, while identifying some of the flaws related to Corporate Social Responsibility (CSR). (Moon et al., 2011) build on Porter and Kramer’s work in CSV by providing a typology framework, differentiating between the ideal, smart corporations, good corporations, selfish corporations and stupid corporations, on the axes of strategy and ethics. Good corporations don’t achieve the corporate benefit; selfish corporations achieve corporate benefit while smart corporations achieve both social and corporate benefit.

![Figure 13 Types of Corporations (Moon et al., 2011)](image)

Applying (Moon et al., 2011)’s typology in the data privacy and protection context, the smart corporation is likely the one which recognises the human need, and the foundation of democracy requires, personal privacy and the avoidance of further Cambridge Analytica like scenarios. Rather than acquiring every possible piece of personal data from users to be put to use for the benefit of marketers and platform providers, the new smart skill for a trustworthy organisation is to prove that it is to the genuine benefit of the user to provide the information that they are comfortable revealing and that their data is safe.
If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane

In an unpublished work (due for publication 2018/19), (Moon and Parc, 2017) further extend the work of (Porter and Kramer, 2011) by introducing the concept of corporate social opportunity (CSO), captured effectively in Figure 13, indicating CSO for competitiveness is underpinned by a sophisticated strategy and high corporate efforts leading to high corporate benefits.

Figure 13 reflects effort and benefit on the one axis and a range of simple to strategy complexity on the other. This creates the impression that CSO is less susceptible to being reduced, modularised, simplified and outsourced but rather it needs to be more native to the values and principles integral to the processes of the organisation in order to be successful. In effect, the indication is that CSO needs to be as much cultural as strategic.

Figure 14 Shifting corporate social responsibility to corporate social opportunity through creating shared value (Moon and Parc, 2017).

The advent of GDPR has reversed the privacy equation to an extent. No longer can organisations keep private about what personal data they acquire and how the process it and the eventual purpose to which it is put. Shining the GDPR light on the specific personal data, the storage and the purpose of the data processing activities carried out on users’ data requires an organisational response. The only reasonable minimum response is to engage and be as compliant as possible. The raised awareness amongst users of their data rights may tilt the user inclination against providing more access and processing of personal data if organisation’s behaviour remains unchanged. However, treating users with greater respect has benefits as (Dean et al., 2013) found that enabling the effective management of privacy settings led to a 51% greater willingness to allow their data to be shared than
those not in control of their privacy. (Bower, 2003) identifies that a high standard of ethics in a company has the following advantages:

- Everyone knows the right thing to do and does it decisively
- High calibre people are attracted to work in highly ethical companies
- Is more profitable
- Has better relationships with customers
- Has better relationships with competitors
- Has better relationships with the general public
- Has a favourable ethical image, is trusted more by customers

(Bower, 2003)’s recommendation is that a company’s philosophy is made explicit and that the values of honesty and trustworthiness are clearly articulated so that everyone understands the high ethical standards that they should expect and are expected of them.

The conclusion that can be drawn from the analysis and discussion regarding trustworthiness resolving the concerns GDPR raises for the opportunities and benefits of data driven business models, is that focussing on trustworthiness presents itself as the opportunity for competitive advantage in an increasingly complex regulatory environment. Anonymising personal data, engaging with the user and sharing fully the activities carried out and uses to which user data is put, is empowering for the user. If there is, in fact, an advantage conveyed to the user from; the much ventilated, justification for, personalisation of advertising tailored to the individual, an empowered user could give honest feedback very quickly.

Data driven businesses may have a choice to move to a subscription model for providing e-mail, or social networking services. Spotify and Amazon already have subscriptions built into their business model as does Microsoft with its cloud offering Office 365. A recognition of the value of personal information by data driven businesses paying users for their data is an option, or a hybrid option could be considered. Being a trustworthy organisation is ultimately about being respectful to your customer. GDPR has changed the risk landscape considerably for data driven businesses and the factors that determine whether a customer or user will continue to place their trust is based on multifarious cognitive and affective factors, as per the data privacy and protection conceptual model. GDPR has given users and customers the ability to switch off data, the source of raw material for data driven businesses. A trustworthy organisation known for its high ethical standards has the best opportunity assuage the doubts of customers (Bower, 2003).
Trustworthiness – GDPR and the weaknesses of data driven business

Moderate Gains

GDPR could be seen as an additional obstacle and cost to the already difficult task of evolving into a data driven business or it could alternatively require organisations to narrow their focus and put their efforts into defining where there is specific business advantage to be gained and ensuring that building a trustworthiness into their approach to data privacy and protection may improve organisation’s chances for success.

Reliance on an abundance of data

GDPR has made clear who owns the personal data and the rights of the data owners and obligations of the key stewards of the information. Without putting the effort into becoming a trustworthy steward of users’ personal data, the likelihood is that a more trustworthy competitor will receive the commercial benefit of the data users are willing to share.

Lack of Data Scientists

In a general sense, a more trustworthy industry will thrive and therefore continue to attract students to data science in pursuit of high end careers which will have the effect of enabling the competence gap to continue to resolve itself as the industry matures.

Environmental cost of data storage

GDPR requires organisations to protect personal information. Therefore storage of that data is of critical importance. An organisation striving to be trustworthy would need to consider how to tackle this as a problem rather than merely maintaining compliance to the regulation. In order to prove itself trustworthy in this regard, an organisation would need to take the trouble put in place a plan to leading to a more sustainable storage solution.

Trustworthiness - GDPR and the threats to data driven business

The impact of GDPR on threats to data driven business include regulatory impacts, negative media coverage, and cyberattacks. Compliancy with GDPR will reduce the threat of successful cyberattack exposing personal data and improve the immediacy of the disclosure of breaches. However, as the sophistication of attacks increase (Biscoe, 2018) more and more innovative security solutions may be required. IBM identified that of all security breaches, 95% are caused by human error (Howarth, 2014). This implies that a culture of vigilance is around cyber required. A convincingly trustworthy organisation would not only be compliant but also innovating to prevent future cyberattacks rather than remaining compliant with security patches and processes for dealing with current threats.

The regulation impacts have already been discussed in this chapter, and there is a strong likelihood that negative media exposure is going to continue given that there is now a high standard of data privacy and protection to be achieved with which many struggle.
Chapter 5 Recommendations, Limitations and Future Research

Recommendations
Based on the analysis and discussion of trustworthiness, GDPR and data driven businesses, the following recommendations may guide organisations in the new more highly regulated business world.

- Define core values for the organisation regarding data privacy and protection
- Create a culture of living up to and expecting high ethical standards in relation to data privacy and data protection
- Define Trustworthiness Key Performance Indicators in relation to data privacy and data protection
- Assess your organisations trustworthiness
- Use an infographic to represent the assessed status and the trustworthiness standards expected of the organisation

While it is possible that trustworthiness may be domain specific, that is located within the realm of data privacy and protection, being trustworthy in all areas of business is likely to bolster the specific trustworthiness related to data privacy and protection.

Limitations
This research established a basis for assessing whether trustworthiness could resolve the concerns raised by GDPR for data driven businesses. It was necessary to remain at a conceptual and theoretical level due to the allowable length of the dissertation and the time available to complete it. The study is limited in that the dimensions of trustworthiness were related to the principles of GDPR and not the detailed articles of the regulation which would yield a far richer analysis. The proposed approach to the measurement of trustworthiness evolved from the approach of previous researchers but was limited to specifying statements, linked to points on a scale, which were high level and untested by detailed application to and with the support of one or more data driven companies. The evidence available to validate the approach to measurement was limited to samples of published information from US and EU regulatory enforcement commissions, and analysis of samples of data privacy policies. Partnering with a data driven company to assess the trustworthiness provide a richer source of evidence.

Future research
An area of future research lies in examining trustworthiness as it relates to GDPR at the deeper level of the articles of the regulation. The model for measurement of trustworthiness could be applied and further evolved or validated by partnering with one or more data driven companies and utilising a richer source of data and evidence. An analysis of the before and
If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane after GDPR data privacy policies would yield an interesting perspective on the level of and approaches to compliance. A case study following the implementation of a trustworthiness model and culture to gain a competitive advantage in a data driven business provide insight and value.
If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane.

References


ALPHABET 2017. ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934 For the fiscal year ended December 31, 2017.


II GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane


CRISP, J. 2018. EU Competition chief holds the threat of breaking up Google. The Telegraph, Technology Intelligence, 25/03/2018.


FTC, F. T. C. 2013. Google Agrees to Change Its Business Practices to Resolve FTC Competition Concerns In the Markets for Devices Like Smart Phones, Games and Tablets, and in Online Search. Washington , DC 20580.


II GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane


MERRIAN-WEBSTER ND.


O’NEILL, O. 2013. What we don’t understand about trust. TEDx Houses Of Parliament: TEDx.

If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane.


SINEK, S. 2014. Leaders eat last : why some teams pull together and others don't / Simon Sinek.


TSUKAYAMA, H. 2012. FTC releases final privacy report, says 'Do Not Track' mechanism mas be available by end of year. Washington Post, 26/03/2012.

If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane.


If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane

Appendices

Appendix 1. Sample Trustworthiness dimension standards matching proposed scale

<table>
<thead>
<tr>
<th>Very Dishonest</th>
<th>Quite Dishonest</th>
<th>Unproven Honesty</th>
<th>Quite Honest</th>
<th>Very Honest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proven that words and actions are congruent most of the time</td>
<td>Proven that words and actions are not congruent at times</td>
<td>Not Proven that words and actions are congruent at times</td>
<td>Proven that words and actions are congruent most of the time</td>
<td>Proven that words and actions are always congruent</td>
</tr>
<tr>
<td>Proven not to adhere to the facts much of the time</td>
<td>Proven not to adhere to the facts at times</td>
<td>Not proven to always adhere to facts</td>
<td>Proven to adhere to the facts most of the time</td>
<td>Proven to always adhere to facts</td>
</tr>
<tr>
<td>Proven not to be always open and honest in communication much of the time</td>
<td>Proven not to be open and honest in communication at times</td>
<td>Not proven to be always open and honest in communication</td>
<td>Proven to be open and honest in communication most of the time</td>
<td>Proven to be always open and honest in communication</td>
</tr>
<tr>
<td>Proven to not conduct itself fairly and in a straightforward manner much of the time</td>
<td>Proven to not conduct itself fairly and in a straightforward manner at times</td>
<td>Not proven to conduct itself fairly and in a straightforward manner</td>
<td>Proven to conduct itself fairly and in a straightforward manner most of the time</td>
<td>Proven to conduct itself fairly and in a straightforward manner at all times</td>
</tr>
<tr>
<td>Not at all benevolent</td>
<td>Not very Benevolent</td>
<td>Unproven Benevolence</td>
<td>Quite Benevolent</td>
<td>Very Benevolent</td>
</tr>
<tr>
<td>Proven not to have any respect the consumers privacy</td>
<td>Proven not to have much respect the consumers privacy</td>
<td>Not proven respect the consumer’s privacy</td>
<td>Proven to have some respect for consumers privacy</td>
<td>Proven to respect the consumer’s privacy at all times and all circumstances</td>
</tr>
<tr>
<td>Proven not to have benevolent concern for the well-being of the consumer at any time or any circumstances</td>
<td>Proven not to have benevolent concern for the well-being of the consumer at times and in some circumstances</td>
<td>Not proven to have benevolent concern for the well-being of the consumer at times and in some circumstances</td>
<td>Proven to have benevolent concern for the well-being of the consumer some of the time and in some circumstances</td>
<td>Proven to have benevolent concern for the well-being of the consumer at all times and in all circumstances</td>
</tr>
<tr>
<td>Very incompetent</td>
<td>Quite incompetent</td>
<td>Unproven competence</td>
<td>Quite Competent</td>
<td>Very Competent</td>
</tr>
<tr>
<td>Proven to be unable to provide protection for consumers data at on multiple occasions and circumstances</td>
<td>Proven to be unable to provide a reasonable level of protection for consumers data at times and in some circumstances</td>
<td>Un-Proven to be able to provide protection for consumers data at all times and in all circumstances</td>
<td>Proven to be able to provide a reasonable level of protection for consumers data most of the time and in most circumstances</td>
<td>Proven to be able to provide the highest level of protection for consumers data at all times and in all circumstances</td>
</tr>
</tbody>
</table>
If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane.

<table>
<thead>
<tr>
<th>Proven to be unable to provide protection for consumers privacy on multiple occasions and circumstances</th>
<th>Proven to be unable to provide a reasonable protection for consumers privacy at times and in some circumstances</th>
<th>Un-Proven to be able to provide the protection for consumers privacy</th>
<th>Proven to be able to provide a reasonable level of protection for consumers privacy most of the time and in most circumstances</th>
<th>Proven to be able to provide the highest level of protection for consumers privacy at all times and in all circumstances</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not at all Vulnerable</td>
<td>Not very Vulnerable</td>
<td>Unproven Vulnerability</td>
<td>Quite Vulnerable</td>
<td>Very Vulnerable</td>
</tr>
<tr>
<td>Proven not to adhere to even a basic level of consumers’ privacy and data protection at any time and in any circumstances and not assure that any costs of damage or loss caused to customers due to the organisation’s failings will be rectified.</td>
<td>Proven not to adhere to the highest level of consumers’ privacy and data protection at all times and in all circumstances and assure that any and all costs of damage or loss caused to customers due to the organisation’s failings will be rectified.</td>
<td>Un-Proven that the organisation adheres to a high level of consumers’ privacy and data protection and in any circumstances and no evidence of assurance that most costs of damage or loss caused to customers due to the organisation’s failings will be rectified.</td>
<td>Proven to adhere to a reasonably high level of consumers’ privacy and data protection most of the time and in most circumstances and assure that most costs of damage or loss caused to customers due to the organisation’s failings will be rectified.</td>
<td>Proven to adhere to the highest level of consumers’ privacy and data protection at all times and in all circumstances and assure that any and all costs of damage or loss caused to customers due to the organisation’s failings will be rectified.</td>
</tr>
<tr>
<td>Very Unreliable</td>
<td>Quite Unreliable</td>
<td>Unproven Reliability</td>
<td>Quite Reliable</td>
<td>Very Reliable</td>
</tr>
<tr>
<td>Does not do what is says</td>
<td>Does what is says some of the time and in all circumstances</td>
<td>Unproven that it does what is says</td>
<td>Does what is says most of the time and in most circumstances</td>
<td>Does what is says at all times and in all circumstances</td>
</tr>
<tr>
<td>Proven to be unable to provide protection for consumers data at any times or any circumstances</td>
<td>Proven to be unable to provide the protection for consumers data at times and in some circumstances</td>
<td>Un-Proven to be able to provide the highest level of protection for consumers data at all times and in all circumstances</td>
<td>Proven to be able to provide the highest level of protection for consumers data most of the time and in most circumstances</td>
<td>Proven to be reliable to provide the highest level of protection for consumers data at all times and in all circumstances</td>
</tr>
<tr>
<td>Proven to be unable to provide protection for consumers privacy at any times or any circumstances</td>
<td>Proven to be unable to provide the protection for consumers privacy at times and in some circumstances</td>
<td>Un-Proven to be able to provide the protection for consumers privacy</td>
<td>Proven to be able to provide the highest level of protection for consumers privacy most of the time and in</td>
<td>Proven to be able to provide the highest level of protection for consumers privacy at all</td>
</tr>
</tbody>
</table>
If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane.

<table>
<thead>
<tr>
<th>Communicates very badly</th>
<th>Communicates quite badly</th>
<th>Unproven to communicate well</th>
<th>Communicates quite well</th>
<th>Communicates very well</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proven to be unclear in communication all of the time in relation to data privacy and protection</td>
<td>Proven to be unclear in communication a lot of the time in relation to data privacy and protection</td>
<td>Unproven to communicate clearly in relation to data privacy and protection</td>
<td>Proven to communicate clearly most of the time in relation to data privacy and protection</td>
<td>Proven to always communicate clearly in relation to data privacy and protection</td>
</tr>
</tbody>
</table>

Table 12 Sample Trustworthiness dimension standards matching proposed scale.
### Appendix 2. Sample of Facebook’s Privacy Policy 7th February 2018

<table>
<thead>
<tr>
<th>Data Collection</th>
<th>Content</th>
<th>What</th>
<th>When</th>
<th>How</th>
</tr>
</thead>
</table>
|                 | Things you do and information you provide.                             | Content of your message  
Content of your communications                                          | sign-up  
create, share, message, or communicate  
Information about the content including location and date of content creation |                                          |
|                 | Things others do and information they provide.                         | Information on how you use the service types of content you view  
type of content you engage with  
frequency of your activities  
duration of your activities  
Content and information others provide about you, share a photo or message  
contact information if they upload your details sync or import this information |                                          |                                          |
|                 | Your networks and connections.                                          | People you communicate with  
the most  
Groups you like to share with  
information about purchase transactions, Payment Information: (Credit/Debit card number and other card information, authentication information, billing information, shipping and contact details) | Make a purchase on Facebook  
On devices where you install or access our services |                                          |
|                 | Information about payments                                              | Make a purchase on Facebook  
On devices where you install or access our services | Make a purchase on Facebook  
On devices where you install or access our services |                                          |
|                 | Device Information                                                      | Operating system  
Hardware Version  
device settings  
file and software names and types  
battery and signal strength  
device identifiers  
Device locations (Including specific geographic locations (through | Make a purchase on Facebook  
On devices where you install or access our services | Make a purchase on Facebook  
On devices where you install or access our services |                                          |
If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane.

<table>
<thead>
<tr>
<th>Data Use</th>
<th>Information from websites that use Facebook Services</th>
<th>Information from third-party partners.</th>
<th>Facebook companies</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>GPS, bluetooth or wifi signals)</td>
<td>Connection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information name of mobile operator or ISP</td>
<td>Information about websites you visit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>browser type</td>
<td>Information about the Apps you visit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Language</td>
<td>Your use of services on those websites and apps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Time zone</td>
<td>Information on the developer or publisher of the app or website provides to you or Facebook</td>
<td></td>
</tr>
<tr>
<td></td>
<td>mobile number</td>
<td>Information about you and your activities on and off facebook from 3rd parties about your experiences with them</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP Address</td>
<td>Information from companies that are owned or operated by Facebook</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When you visit or use 3rd party websites and apps that use Facebook services</td>
<td>When you use the like button</td>
<td>Use measurement services and advertising Services</td>
</tr>
<tr>
<td></td>
<td>When you Facebook login</td>
<td>When Facebook jointly offers services with 3rd parties</td>
<td>In accordance with companies terms and policies</td>
</tr>
</tbody>
</table>

**Data Use**

- All information
- Location information
- Communicate with user

- To provide and Support support for Facebook Services
- Provide services
- Improve services
- Develop services
- Personalise content
- Make suggestions for user
- To provide shortcuts for users
- Analyse informaiton to evaluate and improve products and services
- To tailor services for user and others
- To conduct audits
- troubleshooting
- Send user marketing communications
- Communicate with user about policies and terms
If GDPR embodies the rules of the road for Data Privacy and Protection then Trustworthiness is the fast lane

<table>
<thead>
<tr>
<th>To respond to user contacts</th>
<th>Use infomation Facebook has for advertising and measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>To improve Facebook advertising - i.e. relevant ads on and off Facebook and measure the effectiveness and reach of ads and services.</td>
<td>Promote Safety and Security</td>
</tr>
<tr>
<td>To improve measurement systems</td>
<td>To improve measurement systems</td>
</tr>
<tr>
<td>Verify accounts and activity</td>
<td>Verify accounts and activity</td>
</tr>
<tr>
<td>Promote safety and Security on and off Facebook services e.g. investigating suspicious activity or policy violations</td>
<td>Promote safety and Security on and off Facebook services e.g. investigating suspicious activity or policy violations</td>
</tr>
<tr>
<td>Use engineers to Protect Users’ accounts</td>
<td>Use engineers to Protect Users’ accounts</td>
</tr>
<tr>
<td>Use automated systems to protect users’ accounts</td>
<td>Use automated systems to protect users’ accounts</td>
</tr>
<tr>
<td>Use Encryption to protect users’ accounts</td>
<td>Use Encryption to protect users’ accounts</td>
</tr>
<tr>
<td>Use Machine learning to protect users’ accounts</td>
<td>Use Machine learning to protect users’ accounts</td>
</tr>
</tbody>
</table>

Table 13 Sample of Facebook’s Privacy Policy 7th February 2018 (Facebook, 2018)