Everything is Outcomes

Reframing Information Quality, Data Protection, and Data Governance for a Big Data World

Daragh O Brien – Castlebridge Associates

About the Author

Daragh O Brien is the Managing Director of Castlebridge Associates.

He has a Bachelor Degree in Business and Legal Studies, holds the IQCP certification, is a Fellow of the Irish Computer Society. He is an experienced Data Governance, Information Quality, and Data Protection consultant and trainer with experience across a wide range of industries in a number of countries.

In addition to consulting, he advises on academic research projects in these areas and in the fields of Life Logging and Big Data.

Daragh is an Advisor to DAMA International, a former Director of the IAIDQ, a contributor to the Innovation Value Institute, and is associated with the Data Governance Institute.

email: daragh@castlebridge.ie

twitter: @daraghobrien

web: www.castlebridge.ie

Table of Contents

Introduction

It is often stated that "quality is in the eye of the beholder". This statement is sometimes seen as being glib and unhelpful but it actually neatly sums up what quality is. Quality is a measure of how well a product or service meets or exceeds the expectations of the people are availing of the product or service and how well their use of the product or service brings about desirable outcomes.

Outcomes. Ultimately, in every field of human endeavour, it comes down to outcomes. The outcome is often subjective and personal, tied ultimately to our fundamental hierarchy of needs. It might be warm dry feet delivered by a pair of shoes on cold damp winter's day, or a commute to the office on a quiet train with enough table space for you to write that paper you've been putting off for weeks. A meal from a fast food chain restaurant might address the outcome of sating hunger, but a meal from a Michelin-starred restaurant will satisfy a different set of outcomes.

When the outcome you are focusing on represents a "Big Hairy Audacious Goal", very often the outputs of the capabilities you develop can, in themselves, be seen as valuable outcomes in their own right, albeit serving new and different needs. One thinks of the many outcomes of JFK's stated outcome of "putting a man on the moon and returning him safely to earth": Velcro, scratch-resistant lenses, freeze dried food, athletic shoes, cordless power tools, and CAT and MRI machines.

W. Edwards Deming famously advised that we needed to work on our processes, not the outcome of our processes. However that needs to be considered in the context of Deming's advice to adopt a constancy of purpose. Developing processes that more efficiently deliver sub-optimal or just plain wrong outcomes is not the same as delivering quality improvement. Deming himself recognized this when he advised that:

> *"It is important that an aim never be defined in terms of activity or methods. It must always relate directly to how life is better for everyone... The aim of the system must be clear to everyone in the system. The aim must include plans for the future. The aim is a value judgment"*

Today, we are faced with an incredible range of potential outcomes from the use of and exploitation of data and information. Examples include improved environmental management through analysis of water consumption or traffic flow data in cities or improved healthcare outcomes through the use of treatment data. However, in pursuing these outcomes we need to consider the potential secondary outcomes from the development of these technologies and uses of data.

As the potential for different outcomes becomes better understood by consumers the priority given to these outcomes can change. Recent research by Pew Research suggest a growing awareness of the risks to personal data privacy in the United States, with 50% of respondents to a recent study reporting this as a concern, up 17% since a comparable study in 2009[i].

Studies have consistently highlighted consumer concern about and resistance to the excessive capture of, sharing of, and analysis of personal information. For example a 2012 study[ii] found that 81% of respondents to their survey objected to the transfer of telephone number data to retailers where they used mobile payment services (e.g. Near Field Communication). The same percentage of respondents objected to the transfer of their home address to the retailer. Another report from the Pew Research Centre[iii] found that 68% of respondents were "not okay" with targeted advertising as they did not like

having their on-line behaviour tracked and analysed. Interestingly, 55% of 18-24 year olds shared this view despite the 'conventional wisdom' that that demographic is less concerned with their privacy.

Recent research has highlighted the risks to personal privacy arising from the ability to analyse large volumes of even anonymized data. For example:

- 80% of Netflix users can be re-identified from an anonymous data set based solely on when and how they rated movies they had rented[iv]
- Researchers analysing anonymous Facebook "Likes"[v] were able to:
    - Identify sexual orientation in men with a .88 probability
    - Distinguish between African Americans and Caucasian Americans with 0.95 probability
    - Distinguish between Republican voters and Democrat voters with a 0.85 probability

Legislative responses, while increasingly powerful (for example the EU Data Protection Regulation proposes fines of up to 5% of global turnover, and almost 100 countries world-wide either have or are in the process of enacting strong general Data Protection rules) often lag the capability of technology.

A case in point is the position of anonymized data under EU Data Protection laws. If data has been anonymized so that it no longer identifies an individual it falls outside the scope of current and proposed EU laws. *However*, if that data can be re-identified in any way (either through analysis or combination with other data) then the data is covered by the definition of Personal Data under EU law[vi].

While anonymisation of data has long been seen as a key mitigating action to prevent privacy breaches, research has consistently demonstrated the potential to re-identify individuals based on analysis of this data. As far back as 1990, researchers demonstrated how it was possible to re-identify 87% of the US population based only on the five digit Zip code, gender, and date of birth[vii]. In that context legislative restrictions or mandates to anonymize data are toothless where organisations lack controls to prevent re-identification of that data. Those controls constitute a definable set of decision rights, responsibilities, and accountabilities which must be defined in organisations to ensure that the wrong things are not done with the right data.

With the EU set to enact legislation that will extend the application of its Data Protection legislation to organisations based outside the EU who are processing data that identifies EU citizens or is processed as a result of products or services being offered for sale in the EU, organizations are facing potential penalties of up to 5% of global turnover if they breach those rules.

To paraphrase a song from the recently released Lego Movie: "Everything is Outcomes". And how well we identify and achieve the correct information outcomes will ultimately determine the quality of our Big Data future.

What do we mean by "Outcomes" (and how do we identify them)

It is important to understand what we mean by "outcomes" in this context. What we are actually talking about are the experiences that the customer gets from availing of a product or service. This is what Michael Lanning terms a "Customer Resulting Experience" in his book *Delivering Profitable Value*[viii].

Lanning defines a "Resulting Experience" as consisting of:

1. An event or sequence of mental and/or physical events which happen in the customer's life as a result of doing what some business proposes…
2. An end-result consequence of this event for the customer…
3. Which is a consequence that is either superior, equal, or inferior to any of the other potential resulting experiences that the customer might have had to choose from…
4. The value of this relative consequence to the consumer
5. Specific and measurable characteristics that allow you to objectively determine if the customer has experienced the events, consequence, and value compared to their alternatives.

Lanning is very clear that the essence of a Resulting Experience is not and should never be

- Defined from the perspective of the organization, its products or services, or the features, attributes of those products
- Defined on the basis of the plans, assets, resources, current capabilities and processes of the organization, or the reputation or descriptions of excellence the company might put forward
- Vague and ambiguous platitudes such as "superior quality", "timeliness", "reliability" or "convenience" – these in particular must be defined and measured from the perspective of the customer.

So, outcomes are specific and measurable Key Resulting Experiences that a customer has from availing of a product or service that uses their data or from consuming a piece of information. Lanning gives the examples of the use of the microwave oven, the instamatic camera, and Honda's approach to vehicle design.

Examples of "Key Resulting Experiences" in an information context might include:

- Being able to ship an order without having to contact the customer to verify their delivery address (an internal Key Resulting Experience)
- Customers being able to easily correct errors in the data you hold about them
- Being able to trust that you are not sharing data with 3rd parties without their awareness or consent
- Being able to trust that you have appropriate information security controls in place to ensure that their personal data is kept safe and secure.

Privacy is itself a key resulting experience that individuals consistently wish to avail of from any processing of personal data. Where individuals give up their private data, they usually do so because the trade off in resulting experiences means there is more value to them in exchanging data for a good, service, or outcome. Michael Lanning reminds us that price is a key resulting experience. In today's information economy, the impact on privacy is part of the price. However that price tag is not always

clearly visible to the individual and the onus is on organisations to ensure that the customer doesn't wind up paying more than they had intended due to a breach of their privacy.

So is "Data Privacy" an Information Quality Concept?

Bluntly… yes. Privacy, or more accurately how well our information systems and processes are engineered to support, nurture, and protect the privacy of individuals about whom we process information, is an increasingly important qualitative differentiator in how organisations process information.

In the EU Data Privacy Directive and the forthcoming Data Protection Regulation many of the core rules for Data privacy in Europe are defined as "Principles for Data Quality". When we look at the specifics of these rules we find clear statements of measurable Information Quality attributes:

- Completeness
- Relevance
- Timeliness
- Accuracy

We also find requirements to ensure that the data has an appropriate and verifiable lineage that allows it to be used for the proposed purpose (data must be processed for a specified and lawful purpose and must have been obtained fairly). Individuals are entitled to have a copy of their data, and any codes or abbreviations used in that data need to be explained – which means you need to have some MDM and meta-data management in place.

Figure 1 below gives a crude "ready reckoner" for the overlap of Data Protection, Data Governance, and Information Quality.

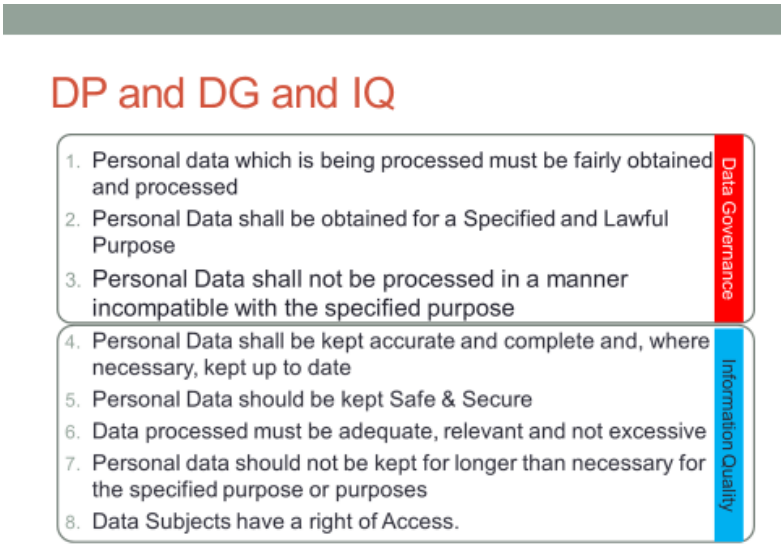

Figure 1 A quick ready-reckoner for the link between EU Data Privacy rules, Information Quality, and Data Governance

Larry English's classic definition of Information Quality is

> *"The degree to which information consistently meets the requirements and expectations of all knowledge workers who require it to perform their processes"*[ix].

This definition is, to my mind, insufficient in the context of today's approaches to and methods for gathering and processing information about people and their habits, interests, and lifestyles. However it is still important as it stresses the need for information to *consistently* meet the *requirements* and *expectations* of people in the performance of their processes.

Furthermore, if we extend the definition of "knowledge worker" slightly to include any potential consumer of the information, then the rights of access to personal data under Data Privacy rules mean that we *have* to consider the individual whose data we are processing and their requirements and expectations.

Requirements

The *requirements* for Data Privacy are set out either in standards such as the OECD Fair Information Processing Requirements or in legislation such as the 100 or more Data Privacy laws that have been enacted globally in the past few years based on these principles. For example, in the European Union there are clear statutory requirements that must be met around how personal data must be processed.

EU Principle	Related OECD Principle
1. **Personal Data must be obtained fairly and lawfully**	Collection Limitation Principle; Openness Principle
2. **Personal data must be processed for a specified and lawful purpose**	Purpose Specification Principle; Openness Principle
3. **Personal data cannot be processed for any other purpose that is incompatible with the specified purposes**	Use Limitation Principle
4. **Personal data must be kept safe and secure**	Security Safeguards
5. **Personal data must be kept accurate and up to date, relative to the purpose for which it was obtained.**	The Data Quality Principle;
6. **Personal data must be adequate, relevant, and not excessive in the context of the purpose for which it was obtained.**	The Data Quality Principle;
7. **Personal data must not beretained for longer than is necessary for the purpose for which it was obtained.**	The Purpose Principle; The Data Quality Principle
8. **Data Subjects have Rights of Access/Rectification/Erasure/Blocking**	The Individual Participation Principle
Criminal Sanctions and Civil Liability	The Accountability Principle

Figure 2 EU Principles mapped to OECD Guidelines

Data Protection laws and regulations can best be described as *the definition of expectation by society of how organizations who are processing data about individuals can ensure an appropriate balance is struck between the right to privacy of the individual and the objectives and goals of the organization*. The legislative or policy recommendations that are set out by the law makers or Regulatory bodies

represent a statement of duties and standards of care that should be met and principles that should be followed. Failure to comply with these principles and standards means that the organization has failed to meet the expectation of society. This non-quality outcome can lead to financial or other criminal sanctions, risk of litigation, and inevitable brand damage to the organization due to negative publicity.

Expectations

The expectations that consumers have regarding the ways in which their data is processed and the 'covenant' that exists between the processor of personal data and the provider of it should be the key area of focus for Information Quality and Data Governance practitioners. Legislation can often lag both technology capability and societal concerns. After all, legislators usually legislate based on priorities set at the ballot box. But how those priorities can be set is often influenced by the messages the law makers get about what their constituents feel are important priorities.

Successful Organisations seek to anticipate the emergence of, or create a desire for, a particular set of outcomes. They try to identify the Expectations of their customers. Michael Lanning identifies three fundamental strategies that organisations adopt when trying to develop their competitive advantage.

Internally Driven	Customer Compelled	Exploring Experiences
This is what we do and we're great!	Ask the customer what will make them happy	Develop deep understanding of what they do and why
Focus on finding/countering objections to product	Ask what features they want and what price they'll pay	Creatively infer what experiences/outcomes would be most valuable
Write a proposition to help sell product	Ask them what proposition they want to hear	Discover experiences/outcomes that could form a superior proposition
Present a 'sales pitch' to influencers, buyers, and sponsors	Focus on getting customers to specify requirements	Joint teams study customers multi-functional experiences

Figure 3 Three general approaches to innovation

Internally driven organisations develop a product or service and then push it to the market, countering objections as they arise. Examples of this would include social media businesses such as Facebook or LinkedIn or other 'Big Data' behemoths such as Google. Internal engineering teams identify or develop a new technology or a new way of doing things, roll it out, and then watch as issue of information quality (the traditional completeness, consistency, accuracy, timeliness factors for example) or data privacy arise which affect user adoption as a result of objections being raised to the privacy impacting aspects of the offering.

Examples of this "Internally Driven" approach to data quality and data privacy would include Google Buzz, the early days of Facebook, and much of what is emerging in the area of 'Life Logging'.

The "Customer Compelled" approach to building Privacy in as a quality characteristic of information in the organization arises when an organization has to amend how it does things either as a result of a

Regulatory body taking enforcement action (yes, Regulators are customers too), enforced response to customer push-back against the use of the data (example being “Care.Data” in the UK NHS, the roll out of which was suspended due to concerns about the implications for patient data privacy resulting from the sharing of medical data with drug companies).

This “Customer Compelled” perspective tends to focus on meeting the literal requirements of regulations or responding to what customers tell the organization they expect when it comes to how the personal information that they give or which is derived about them from their interactions with products and services. Of course, this relies on legislation being ‘fit for purpose’ in how it can be interpreted and applied to the specific instance of a product, service, or act of processing data. It also calls for the consumer to be aware of how your planned use of their data might impinge on their “right to be left alone”, as Louis Brandeis so eloquently defined the right to Privacy.

And let’s not lose sight of the fact that the “Customer Compelled” perspective is still largely reactive, depending on organisations to be able to engage with their range of potential customers and stakeholders to determine what it is that the customer wants to hear and then working out how (if at all) you can deliver that.

Henry Ford famously said that if he had asked his customers what they had wanted when designing his Model T they would have told him they wanted a faster horse. In a context where often skilled and experienced professionals have a difficult time identifying and assessing the privacy implications of new technologies or methods of processing data, it is unrealistic to expect regulators or individuals to be able to correctly identify and assess those self-same risks.

Moving our focus to the identification of the key resulting experiences changes the frame through which the privacy issues are viewed and allows for the explicit identification of trade-offs between competing resulting experiences. For example, if you don’t want to have the contents of your email scanned for keywords that will be linked to your profile for the purposes of pushing targeted adverts, then the key resulting experience you get from one email platform might be less valuable to you then the experiences you get from competitor.

It is worth remembering that the essence of a Key Resulting Experience is an outcome that has value. When John Land developed the Polaroid camera, he did so not because he could or because Polaroid’s market research team had identified a customer opportunity. He did so because his daughter had a tantrum at her birthday party because she wanted to see the photographs he had taken there and then.

The emergence of ‘Privacy by Design’ and ‘Privacy Engineering’ are examples of the evolution of quality systems thinking in the realm of Privacy, an evolution that is particularly important as we continue to feed steroids and growth promoters to our Big data and as we rapidly begin to switch on ‘The Internet of Things’. But these new paradigms simply provide tools and frameworks to work through the process of design and execution of systems of processing of personal data that meet desired and desirable outcomes with regards to personal data privacy. If we continue to approach the challenge from an internally driven or customer compelled perspective we continue to risk missing the opportunity for improved quality of outcome and customer experience through better management of privacy.

Only by beginning to Explore Experiences and defining what the Key Resulting Experiences our customers and our societies wish to have from the processing of data about and relating to people can

we begin to properly develop the Value Delivery Systems required to deliver on those outcomes. Only by understanding what those Key Resulting Experiences are can we ever hope to articulate the value proposition of Privacy or from its sacrifice for a bigger benefit.

The Value Delivery System

Once we have identified what our Key Resulting Experiences will be and have identified what "quality" means in the context of the value proposition trade-offs that the customer wants to make, we then need to consider the mechanisms by which that bundle of Key Resulting Experiences can be delivered. In this context the relationship between Data Privacy, Data Governance, and Information Quality, as well as an array of other information management disciplines must be clearly understood.

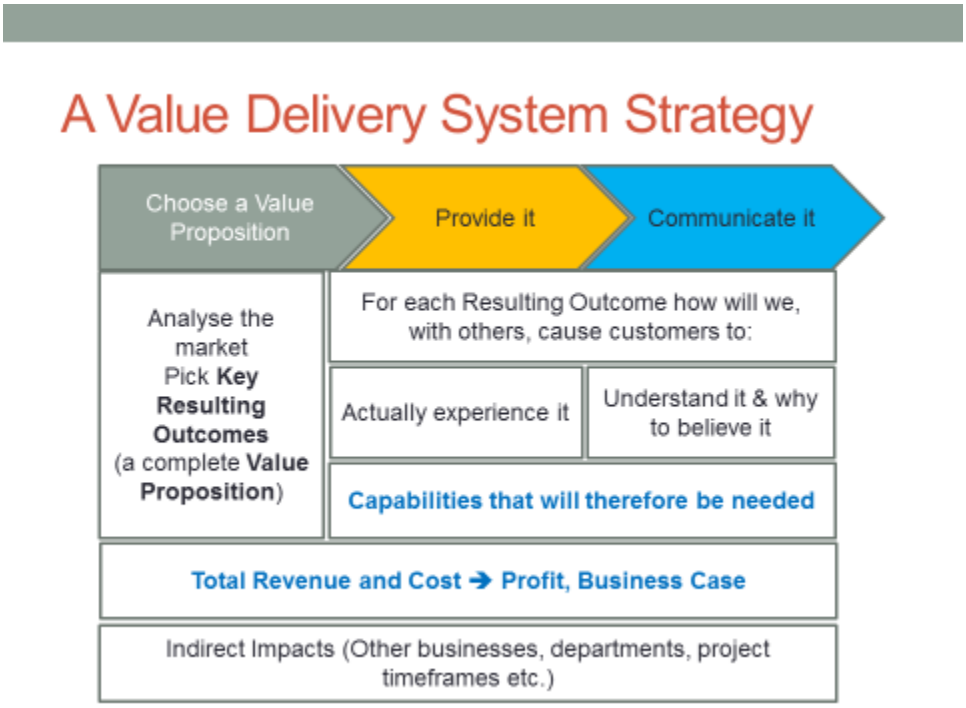

Figure 4 The generic value deliver system framework, based on Lanning

Once we have selected our Key Resulting Outcomes and bundled the value proposition, it is necessary to figure out how those outcomes will be provided and how the customer will be communicated with so that they will both understand the value proposition being presented to them and believe that it is of value to them.

Data Governance practices and Information Quality methods have a key role to play in developing the core capabilities that enable the experience of privacy and data protection to be delivered to the individual. Whether it is ensuring that marketing permissions are correctly modelled in your systems[x], or ensuring that there are strict protocols in place around the use of data for new purposes or the re-identification of anonymized data, or ensuring that Privacy Impact Assessments are conducted on new projects or processes, the core functions of Data Governance and Information Quality directly contribute to the development of a capability to manage data in a way that preserves privacy.

In addition, the way in which the organization communicates with their customers about the uses that data is being put to, or the way in which privacy is impacted or protected by proposed changes in processing is essential to ensuring that the trade-offs between competing key resulting experiences are correctly understood. This communication need is at the core of the Transparency principles in many Data Privacy law frameworks, but it is the one area where organisations consistently fail.

For example, when a customer opts out of SMS marketing but may have been included in other forms of SMS promotion, the customer may expect a key resulting experience of no more spam SMS. However if the organization does not communicate back the possibility of other opt-ins still being active and advise the customer how to check this, the customer is likely to complain to a privacy regulator when they continue receiving messages that they had opted out of. But to achieve and successfully execute the simple process of being able to do that the organization needs:

a. To be able to generate a short and intelligible return message to the customer (requires an SMS platform capability and trigger rules to be set up
b. To have identified the scenarios where customers might have tried to opt-out but had it fail because they used the wrong short code or the wrong key words (is the data received valid in the domain of values for a valid opt-out)
c. To have the capability to present accurate information to the customer via a web-portal about the messaging services that they are currently opted into
d. To have the capability in that web-platform to consistently and correctly reflect and update any changes the customer might make to their profile and
e. To have that propagate around all relevant systems used in marketing and communications processes.

That combined bundle of things represents the Value Delivery System necessary to ensure the customer's key resulting experience of "I will only get SMS messages I want and expect" is delivered consistently.

Trust

Ultimately, when we consider the interplay of Data Protection/Privacy, Information Quality, and Information Governance, we must consider what are the fundamental expectations that individuals might have and what are the Key Resulting Experiences that the organization (or society) must trade off against each other. The right to communicate without being monitored is traded off against the right of a State to have a 'panopticon' of intelligence gathering that lets threats be identified. A personal email account is profiled by a free email service provider to provide grist to the advertising mill that keeps the lights on in the freemium service.

Often, however, it is in the iterative evolution of a product or service as data becomes available for processing and action that the undesirable Key Resulting Outcomes are identified. In this context the concept of trust becomes very important. We, as individuals, must be able to trust organisations who are processing our information. Likewise, organisations must be able to trust that, as they begin to use data in new and innovative ways, that the data they are using is fit for purpose and that the outcome they are seeking to achieve is a valued Key Resulting Experience for their customers. If it is not they may find themselves acting on poor quality data (leading to brand damage) or encountering Regulatory or Consumer push-back (a good example of this is the challenges faced by Google Glass).

Let's examine this with a hypothetical:

- If an automobile manufacturer was to install a device to test for the presence of alcohol on a driver's breath, and then immobilize the vehicle, this would doubtless be a desirable outcome.
- If the automobile manufacturer was to retain a log of the data of each breath sample, along with the date, time, and location of the vehicle for each sample, this too might be a valued key resulting outcome for the driver
- If the automobile manufacturer was to tie the breath test data to the identity of the driver using biometrics, and was able to generate a log of *who* was too drunk to drive the vehicle *when* and *where they were* when that happened, and *how often that happens to that individual*, that might be of use to the driver or their household.
- If the automobile manufacturer was to make that data available to the vehicle owner (for example the driver's employer) would that be a valuable Key Resulting Experience? ("Hey Tom, the computer tells us you were too drunk to drive the company car home 16 times last quarter. We need to talk.")
- If the data was provided to the driver's insurance company and caused their insurance premium to go up? And any insurance policy they were a named driver on (after all, we've identified them using biometric data)?
- If the data was to be provided to the driver's insurance company and was then used as part of their medical insurance risk profile causing them to have coverage curtailed due to their alleged drink problem?
- Or what if the data was provided to the driver's insurance company which is part of the same group of companies as the driver's mortgage lender, who takes the data obtained by the insurance arm and uses it in their risk profiling for credit risk? What if the driver's car was usually in the vicinity of a well-known gambling establishment every time the car was immobilized? Or what if the data shows that drivers of a particular make, model, and year of car are statistically more likely to be heavy drinking gamblers? How might that affect other individuals?

As we move up the spectrum from a simple obtaining of data for a specific immediate action (fail the breath test, take the bus) towards "big data" realm of potential additional uses for data we need to consider the value of the Key Resulting outcomes and the trade-offs that are possible between different outcomes for different categories of consumer. Otherwise each individual may individually choose to 'game the system' by providing junk data. For example, maybe the driver has a sober friend blow in the tube while they scan their fingerprint for the biometric id.

And this is the flipside of the "trust" question. Danette McGilvray defines 'quality information' as information that is a "trusted source for any and all uses". The automobile manufacturer needs to be able to trust the information they might be gathering, particularly as the complexity and impact of the processing increases. However they also need to be able to trust that they can use the information in the way they wish to, from the perspective of legal controls, technology design and modelling, and customer acceptance and agreement to the proposed processing.

That trust is a two-way street and it is equally important that the individual be able to trust the automobile manufacturer not to try to put their data to a new use that doesn't deliver a valued and valuable Key Resulting Experience for the individuals described by the data in question. Unfortunately

what happens when that circle of trust is broken is that people start opting out of the product or service, either quietly or with fanfare and lobbying of law makers.

The mechanism that must be in place to ensure that that trust is developed and maintained is a value delivery system that is aligned with the delivery of an identified set of key resulting outcomes and within which the value of a product or service or other outcome can be weighed against the risks to and impacts on personal Data Privacy.

Conclusion

Everything is outcomes. Privacy was the word of the year in 2013 according to Dictonary.com. To deliver outcomes that reflect and respect privacy in an age of Big Data we need to be able to articulate the trade-offs between the Key Resulting Experiences that can be delivered through new technology, processes, or processing we need to move from an Internally-driven innovation culture to one which considers those experiences and can define a value proposition that reflects the off-setting of one experience against another.

Those key resulting experiences need to be defined in a clear and concrete fashion. Bland statements about how it is important that we can "trust" data or that people should be able to have trust in how their data is processed are increasingly meaningless as organisations begin to compete on privacy. What is required is a clearly articulated Value Delivery System that encompasses Data Governance, Information Quality, and a host of related disciplines so that internal and external stakeholders can have confidence in how data is being managed. This Value Delivery system needs to be engineered and governed with demonstrable evidence of its effectiveness.

While legislators rush to keep pace with technology, Regulators are increasingly looking to apply core principles and fundamental expectations to their assessments of new technologies or threats to privacy. With the penalties for getting it wrong set to rise significantly with the emergence of new and stricter Data Privacy laws, it is more important than ever that organisations focus on the outcomes of their processing and the impacts on privacy.

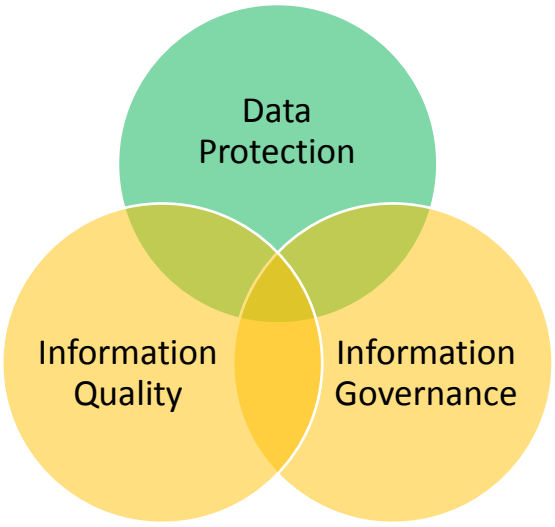

Figure 5 A set theory view of DP, DG, and IQ

[i] Pew Research, "*More online Americans say they've experienced a personal data breach",* April 14 2014, http://www.pewresearch.org/fact-tank/2014/04/14/more-online-americans-say-theyve-experienced-a-personal-data-breach/ (last accessed April 21 2014).

[ii] Hoofnagle, C. J., Urban, J. M., & Li, S. (2012). *Mobile Payments: Consumer Benefits and New Privacy Concerns.* Berkley Center for Law and Technology

[iii] Purcell, K., Brenner, J., & Rainie, L. (2012). *Search Engine Use 2012.* Pew Research Center.

[iv] Narayanan, A. and Shmatikov, V, *Robust De-anonymization of Large Sparse Datasets*, 2008 http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf

[v] Kosinskia, M., Stillwell, D., and Graepel, T. *Private traits and attributes are predictable from digital records of human behavior,* Proceedings of the National Academy of Sciences of the United States of America, March 2013 *http://www.pnas.org/content/early/2013/03/06/1218772110.full.pdf+html*

[vi] Under EU Directive 95/46/EC personal data is defined as "*any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".*

[vii] Sweeney, Latanya, *Simple Demographics Often Identify People Uniquely,* Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000. http://dataprivacylab.org/projects/identifiability/paper1.pdf

[viii] Lanning, Michael J., *Delivering Profitable Value: A Revolutionary Framework to Accelerate Growth, Generate Wealth, and Rediscover the Heart of Business*, Perseus Books, 1998.

[ix] International Association for Information & Data Quality, *IQ/DQ Glossary,* http://iaidq.org/main/glossary.shtml#I (last accessed April 21st 2014).

[x] O Brien, Daragh, *Data Protection & Marketing Suppressions: Act on Fact* http://castlebridge.ie/insights/blog/daragh-o-brien/data-protection-marketing-suppressions-act-fact