University of Dublin



TRINITY COLLEGE

***Developing a Privacy Canvas Model***

Maurice Buckley

B.A.(Mod.) Computer Science

Final Year Project April 2019  
Supervisor: Dr. Dave Lewis

School of Computer Science and Statistics

O’Reilly Institute, Trinity College, Dublin 2, Ireland

Table of Contents

[Acknowledgements 2](#_Toc5642182)

[Abstract 3](#_Toc5642183)

[1. Introduction 4](#_Toc5642184)

[1.1 The Problem 4](#_Toc5642185)

[1.2 Project Aim 5](#_Toc5642186)

[The Business Model Canvas 5](#_Toc5642187)

[GDPR First Step 6](#_Toc5642188)

[Privacy By Design 6](#_Toc5642189)

[1.3 Readers Guide 7](#_Toc5642190)

[Chapter 1: Introduction 7](#_Toc5642191)

[Chapter 2: Motivation and Background 7](#_Toc5642192)

[Chapter 3: Method/Design 7](#_Toc5642193)

[Chapter 4: Research and Evaluation 7](#_Toc5642194)

[Chapter 5: Conclusion 7](#_Toc5642195)

[2. Motivation and Background 8](#_Toc5642196)

[2.1 Surveying the field 8](#_Toc5642197)

[2.2 Similar Problems 9](#_Toc5642198)

[The Ethics Canvas 9](#_Toc5642199)

[2.2 Critique Of the Field 10](#_Toc5642200)

[Privacy Canvas (Peter O’Leary, 2018) 10](#_Toc5642201)

[Data Protection Impact Assessment(DPIA) 11](#_Toc5642202)

[2.3 Summary 13](#_Toc5642203)

[3. Method/Design 14](#_Toc5642204)

[3.1 Design Intention 14](#_Toc5642205)

[3.2 Design 15](#_Toc5642206)

[Bibliography 16](#_Toc5642207)

# Acknowledgements

# Abstract

Data privacy is an issue of growing importance. Data creation and collection has increased drastically in the past decade

The Privacy Canvas is for early innovators with little knowledge of GDPR. It provides a first step towards GDPR understanding and GDPR compliance by using the canvas alongside the Business Model Canvas, effectively implementing privacy by design. Unlike other privacy and data protection tools, the Privacy Canvas provides a learning tool suitable for the early innovation stage.

# 1. Introduction

## 1.1 The Problem

In the twenty-first century, privacy and data protection has become a huge part of every day life, particularly in the working world where businesses must uphold strict policy’s and laws to protect themselves and their customers from data breaches. Failure to meet these privacy demands can result in huge fines and sanctions that can have a lasting effect on any business, large or small. The importance of adhering to data protection laws has increased dramatically with the introduction of the General Data Protection Regulation (GDPR) on the 25th of May 2018.

GDPR directly concerns all organisations within EU member states and any non-EU member state organisation that handles information to do with EU citizens. It imposes strict new rules regarding the collection, storage and use of personal data belonging to EU citizens in which failure to comply with these rules can result in huge fines to businesses or organisations. Prior to GDPR fines of up to £500,000 could have been issued depending on the severity of the breach but with the introduction of the new regulation, fines can reach as much as 4% of annual global turnover or £20 million, with the fine being the larger of the two options (ITG, 2019).

Due to these new strict regulations and even stricter punishments, it is abundantly clear to any organisation or business that privacy and data protection is now an essential part of running any company. Businesses since the announcement and introduction of GDPR have been on catchup trying to change the operation of their business to now comply with GDPR which has imposed a huge cost due to the restructuring, redesign and change of policy, not to mention the cost of the mandatory training of staff. To avoid such heavy costs and problems later in a business’s lifecycle, privacy and data protection must now be treated as an integral part of any business or project during the early innovation stages. Privacy by design should be a fundamental rule when starting any business and therefore privacy and data protection should be considered as the business model and plan is being created.

The problem most unexperienced entrepreneurs and the majority of the general population have is that they don’t understand GDPR and don’t know where to begin in attempting to prepare themselves for its implications. There needs to be a first step to GDPR compliance that starts the discussion within a business that helps prepare them to meet these new obligations and protect themselves by incorporating privacy by design into their business model.

## 1.2 Project Aim

The Privacy Canvas was initially created as part of a final year project by former student at Trinity College Dublin Peter O’Leary in April 2018. As well as continuing his work and improving where possible, this author has taken his own approach to the Privacy Canvas and how it addresses privacy and data protection concerns. This project aims to address these privacy and data protection issues businesses have in three main ways; provide an easy to use iterative tool like the Business Model canvas which addresses privacy concerns to be used alongside the Business Model Canvas, create a tool suitable to be the first step towards understanding GDPR and GDPR compliance, and by effectively putting privacy by design into practice early on in the business innovation stage. The Privacy Canvas also has a technical implementation that was used for evaluation of this project while also demonstrating the proof of concept of a virtual Privacy Canvas.

### The Business Model Canvas

The Business Model Canvas (Osterwalder & Pigneur, 2010) is an easy to use tool that helps a group or person create an early model of their business during the innovation stage. The Business Model Canvas is highly practical due to its simplistic nature and how it creates a visual representation of their business that can be iterated over time after pivot points in the business’s development. Visually representing information like this is very effective for any group as it creates a brainstorming atmosphere and opens the discussion within the group for possible changes and improvements. The Business Model Canvas has become very successful and popular within the business world and has been adopted by many.

This project intends to address the privacy and data protection concerns a business may face during early innovation stage by following the lead of the Ethics Canvas (Lewis, Reijers, & Pandit, 2018 ), a canvas similar to the Business Model Canvas which addresses ethical issues, by redesigning the Business Model Canvas to address privacy and data protection concerns. It is intended to take advantage of the popularity of the Business Model Canvas and create a canvas to be developed with the BMC which will open the discussion on privacy within a new business or project and be the first step to GDPR compliance. This project will evaluate its use alongside the Business Model Canvas.

### GDPR First Step

General level of knowledge of everything GDPR including compliance and its consequences is extremely low in early innovators particularly innovators leaving or just left college. My aim is to create a canvas tool that requires no previous knowledge of GDPR and introduces all the main concepts and compliance regulations in an easy to use and painless manner. It is my hope that the Privacy Canvas could be the first stepping stone for people trying to learn about GDPR by opening the thought process on privacy and data protection and as it will present it in a far less daunting way than other GDPR introductions. The Privacy Canvas could also be a pre cursor to a “Data Protection Impact Assessment”(DPIA) which is designed for more established businesses that hold highly sensitive data and not suitable to any business or organisation during the early innovation stage.

### Privacy By Design

Privacy by design involves incorporating privacy and data protection into every step a business or organisation makes. It is a very important part of GDPR, and it can be described as “Organisations must implement technical and organisational measures to show that they have considered and integrated data compliance measures into their data processing activities.” (Boardman, Mullock and Mole, 2017).

Businesses who follow the principles of privacy by design by always considering privacy and data protection implications during every action they make are far better prepared to meet GDPR obligations and therefore are protecting themselves in the long run. By incorporating the Privacy Canvas into the early stages of the innovation process and continually iterating it as the business develops, I believe the business will be putting privacy by design into practice and effectively demonstrating compliance which is a principle of GDPR.

## 1.3 Readers Guide

The layout of this report is as follows:

### Chapter 1: Introduction

Chapter 1 has introduced this project by briefly stating the problem and how it can be addressed.

### Chapter 2: Motivation and Background

This Chapter covers the background research that went into this project including analysing the field, similar problems and solutions and my critique of the field that covers privacy and data protection.

### Chapter 3: Method/Design

This chapter covers the various requirements that the Privacy Canvas has as well as the thought process behind my design. It will also cover the technical implementation and the issues I faced.

### Chapter 4: Research and Evaluation

This chapter will cover everything to do with my research and evaluation including my testing process, ethical approval and results.

### Chapter 5: Conclusion

This chapter will summarise my project and cover my personal evaluation, learnings and close with closing remarks and future work.

# 2. Motivation and Background

This Chapter covers the background research that went into this project including analysing the field, similar problems and solutions, and my critique of the field that covers privacy and data protection.

## 2.1 Surveying the field

Todays online world has pushed the issue of privacy and data protection to the forefront which has therefore led to the mass creation of various online tools or compliance checkers. A quick google of “GDPR compliance” will show a plethora of these so-called privacy enhancing tools (PETs) that do little else than take advantage of this sprawling new market by charging subscriptions or memberships. Most of these compliance checkers are like a Data Protection Impact Assessment (DPIA) that test your level of compliance and give you a score rather than being a tool that helps you implement privacy by design by demonstrating compliance over time. It is also clear that the current available tools don’t necessarily help organisations address privacy and data protection concerns during the early innovation stage. They are more suited to established business’ with greater GDPR needs and therefore have bigger GDPR implications. They also have far more knowledge and experience of GDPR because of this. There needs to be a tool suitable for the un-informed population when it comes to GDPR and provide a suitable first step towards understanding GDPR and being GDPR compliant.

It is my opinion that there is a gap in the market for tools that help implement privacy by design. The General Data Protection Regulation puts enough emphasis on the importance of privacy by design that it should be considered a necessity in all modern businesses and that should be reflected in the availability of privacy by design enhancing tools. The European Union Agency for Network and information Security (ENISA) defined a fascinating control matrix for evaluating privacy enhancing tools (PETs) in their report “PETs controls matrix - A systematic approach for assessing online and mobile privacy tools” (D'Acquisto et al., 2016). In this report they state that the assessment of privacy by design is a core focus of their control matrix even though there is not a specific assessment criterion. Instead they analyse how the numerous GDPR principles are put into action like accuracy, purpose limitations and transparency to name but a few. This has greatly impacted my thought process on how to best tackle privacy by design and has therefore had a huge influence on the design of the Privacy Canvas by focusing a great deal on the GDPR/privacy by design principles.

## 2.2 Similar Problems

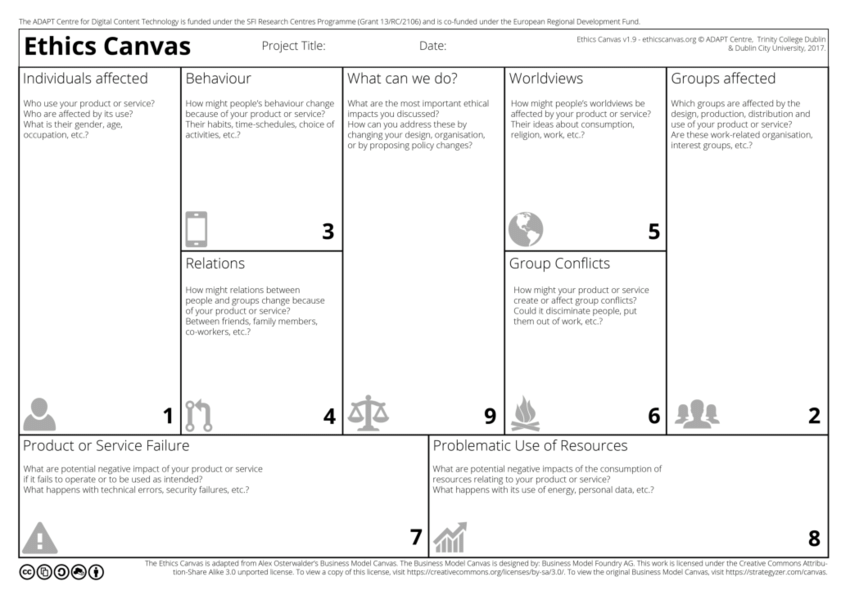
### The Ethics Canvas

The Ethics Canvas (Lewis, Reijers, & Pandit, 2018) is a tool in which this project heavily analysed and studied due to the numerous similarities between the two projects. The Ethics Canvas is a canvas type tool which has also been based on the Business Model Canvas to tackle ethical concerns in the world of research and innovation of technology in a cooperative manner. It was developed here at Trinity College Dublin in the Adapt centre for digital content technology.

The Ethics Canvas like the BMC is divided into nine specific blocks. Unlike the BMC, they tackle ethical concerns and have been subdivided further into four main groups enhancing the way the canvas is completed. Blocks one and two identify relevant stakeholders. Blocks three to six consider the ethical implications on the previously identified stakeholders where as blocks seven and eight consider the ethical impacts that are not stakeholder specific. The last block, nine, was a place where users of the Ethics Canvas could consider how to overcome these discussed ethical implications. These four groups of blocks together made up the canvas (Lewis, Reijers, & Pandit, 2018). This projects author found this design methodology very interesting and noticed how it enhanced the flow of the canvas when it would be created its users. The author took huge inspiration in the design methodology and transferred the thought process behind to the Privacy Canvas where possible.

The evaluation of the Ethics Canvas conducted by the Ethics Canvas team also offered motivation to this project as their findings regarding the usefulness of the canvas and the effect the canvas had, in terms of impact on design or business model, was positive. The outcome of these findings gave this author confidence that a similar canvas that targets privacy and data protection concerns, the Privacy Canvas, would be effective.

**Figure 1: The Ethics Canvas**



## 2.2 Critique Of the Field

The analysis of other resources which also help identify and address privacy and data protection concerns was of great importance to this project. Studying these various tools and resources gave this author an understanding of what works well and what doesn’t when it comes to privacy and data protection. It also gave insight to what is missing in this area or what is not addressed correctly, like privacy by design. Two resources in particular were analysed in depth which gave this author a great appreciation of their work as well providing an understanding of what could be improved/addressed.

### Privacy Canvas (Peter O’Leary, 2018)

As briefly described during the introduction of this project, the Privacy Canvas was originally developed as part of a final year project in 2018 here at Trinity College Dublin. It was designed as a canvas style brainstorming tool for data protection issues, being a proof of concept that such a canvas would have a use in the world of digital application design. Design of the canvas itself was designed as an analogy to the Business Model Canvas where the topics it covers were adapted to suit a Privacy Canvas. The evaluation of the canvas was carried out by getting small groups, who are developing or have developed an application that stores personal data, to fill out their own Privacy Canvas on paper followed by a questionnaire. The results of this study were predominantly positive which gave this author a strong insight into what works well and what doesn’t when redesigning the canvas.

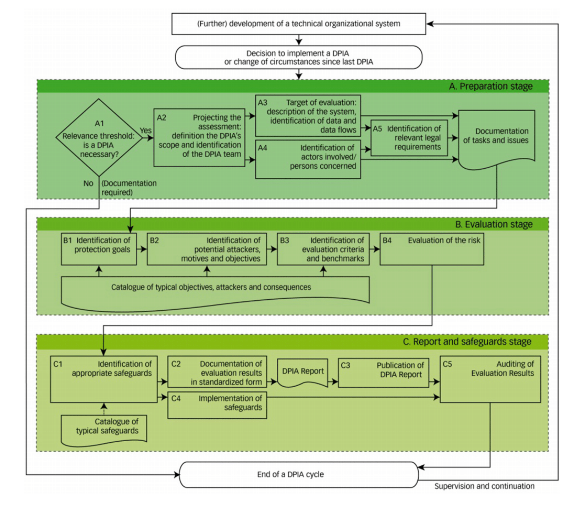
While this project is based on the original Privacy Canvas (O’Leary,2018), this author has adapted the project to try enhancing the Privacy Canvas as a tool for privacy and data protection while also taking his own novel approach to the problem as well as implementing an online version to be used for testing. This approach includes a complete redesign of the canvas and evaluating it’s use alongside the Business Model Canvas, which is required as a precursor to testing. This project also attempts to create a learning tool more suitable as a first step towards GDPR while also targeting privacy by design with more detail by using the whole canvas to demonstrate privacy by design rather than one of the blocks on the canvas.

### Data Protection Impact Assessment(DPIA)

Article 35 of the General Data Protection Regulation describes the execution of a Data Protection Impact Assessment (DPIA), which is mandatory under law for all organisations who collect and process “high risk” data (GDPR Article 35, 2016). A DPIA analyses and identifies data protection concerns and must be carried following strict requirements laid out in article 35 which state when a DPIA is necessary, how it is to be conducted and post assessment requirements to name a few. One of these requirements under article 35(7)(d) is that : *“the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.”* Which means that after the privacy concerns have been formally identified, measures must be put in place to address them.

In the informative paper “A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation” (Bieker et al., 2016), it goes into great detail describing all aspect of a DPIA and has produced the following diagram to help provide an over view of this exhausting process which they have divided into three stages; preparation stage, evaluation stage and the reports and safeguards stage. During the preparation stage the need for a DPIA is considered. If it is deemed necessary, a DPIA team is put together and the relevant information is gathered. During the evaluation stage, data protection goals as well as potential risks are identified and evaluated. Finally, during the report and safeguard stage after privacy and data protection concerns have been assessed, the results are comprehensively documented, and relevant safeguards are identified and implemented. The DPIA report is required to be published to facilitate evaluation and comparison from various data protection authorities and the general public (Bieker et al.,2016).

**Figure 2: DPIA process (Bieker et al., 2016)**



It is clear from the brief summary above, that the process of a DPIA is a long and strenuous task which requires great detail and understanding which may not be suitable for a new business in the innovation stage. The Privacy Canvas would be more suitable to a less established organisation who would not have their own legal department or data protection controller with far greater knowledge of GDPR and its implications. The Privacy Canvas would work far better with an organisation during the innovation stage who are likely to be following the agile development process by allowing continuous development or change and not restrict the organisation to certain assessment criteria outlined in a Data Protection Impact Assessment. The Privacy Canvas could be used as a precursor to a DPIA to help with its implementation further down the line.

## 2.3 Summary

Although there are many different tools available online in the field of privacy and data protection, there are not many tools that are like the Privacy Canvas which are more tailored towards growing businesses in the innovation stage and targets privacy by design. It is this authors opinion that if such a Privacy Canvas could be correctly created and implemented, learning from similar solutions like the Ethics Canvas and the previous Privacy Canvas, there would be a valuable use for it during the development stage of any digital application design.

# 3. Method/Design

This chapter covers the various requirements that the Privacy Canvas has as well as the thought process behind my design. It will also cover the technical implementation and the design issues encountered.

## 3.1 Intentions

As previously stated, the intended purpose of the Privacy Canvas is to be developed alongside the creation of a Business Model Canvas and be a suitable first step towards GDPR in terms of requiring no previous knowledge of GDPR and being a suitable learning tool about GDPR for beginners during the innovation stage. The advantage of creating a brainstorming tool for privacy and data protection to be used when creating your business model is that you are effectively implementing privacy by design, a pillar of GDPR.

As the Privacy Canvas is based on the canvas model like the Business Model Canvas, it will follow the same canvas design principles of being divided into nine main blocks, each with their own unique importance. By sticking to this model, anyone who is creating a Business Model Canvas will also be able to create the Privacy alternative as they will be familiar with its canvas layout and design. The toughest challenge of the Privacy Canvas design is trying to create something that is suitable for someone with no knowledge of GDPR, but still have educational value, and making sure the canvas isn’t daunting to attempt, like most GDPR related things are. It is my opinion that the best way to tackle this problem is to keep the casual brainstorming nature of the Business Model Canvas while also introducing key GDPR concepts and principals informally. The Privacy Canvas will open the discussion on key GDPR concepts but will not assess the user like most GDPR tools available. By removing the assessment aspect that most GDPR tools incorporate, the Privacy Canvas eliminates the intimidating element that is associated with GDPR and maintains the casual, helpful tone that is intended. The fact that the canvas is a brainstorming tool which has no right or wrong answer also aids this casual feel of the canvas. The blocks of the canvas will target the GDPR principles by introducing them informally in each block and starting the discussion around them, during this innovation stage. It is my hope that by introducing these key concepts and creating a thought process involving them, that when the business/organisation meet these concepts again further down the line during something like a Data Protection Impact Assessment, they will be far more prepared as they are familiar with the principles and have already considered them throughout the development of their business.

## 3.2 Canvas Design

The General Data Protection Regulation in total is 99 articles long which gave this project the difficult task of extensively researching GDPR and deciding how to incorporate narrow down the main concepts into a nine block Canvas while remaining true to the project’s intentions described above. This author decided to base the canvas blocks mainly around the widely discussed “GDPR Principles”. The GDPR principles vary in wording and numbers depending on the source but according to the data protection commission of Ireland, the eight principles are described below:

1. **Process it lawfully, fairly, and in a transparent manner;**
2. **Collect it only for one or more speciﬁed, explicit and legitimate purposes, and do not otherwise use it in a way that is incompatible with those purposes;**
3. **Ensure it is adequate, relevant and limited to what is necessary for the purpose it is processed;**
4. **Keep it accurate and up-to-date and erase or rectify any inaccurate data without delay;**
5. **Where it is kept in a way that allows you to identify who the data is about, retain it for no longer than is necessary;**
6. **Keep it secure by using appropriate technical and/or organisational security measures;**
7. **Be able to demonstrate your compliance with the above principles; and**
8. **Respond to requests by individuals seeking to exercise their data protection rights (for example the right of access).**

**3. (The Eight Principles of Data Protection | Data Protection Commission, 2019)**

By remaining true to these principles throughout the Privacy Canvas, the canvas would be instilling the main GDPR concepts into the user’s mind and thought process.

From analysing the evaluation of the previous Privacy Canvas (O’Leary, 2018), multiple users commented that the flow of filling out the canvas was disrupted by having to traverse to canvas consistently to create the next block. O’Leary admits that this is something he overlooked and that it influenced the design flow of the user to a negative effect. This is something that I considered very important to address if I am to be successful in improving the Privacy Canvas. This author took inspiration from the Ethics Canvas (Lewis, Reijers, & Pandit, 2018) in how best to deal with this issue. The Ethics Canvas team decided to sub-divide their blocks into four main groups, with each group consisting of blocks that are somewhat related. They grouped the first two blocks together which identified relevant stakeholders, blocks three to six consider the ethical implications on these identified stakeholders, blocks seven and eight consider the ethical impacts that are not necessarily stakeholder specific, and the last block was a block where ideas to overcome these ethical impacts could be discussed which I thought was an exceptional way to finish a canvas. The Ethics Canvas’ influence can be observed in The Privacy Canvas’ layout as it too has been subdivided into four groups which are described below:

**Blocks 1-3:** These blocks are about the data subjects and the data that is being stored.

**Blocks 4-6:** How the business/project cooperates with the data subjects.

**Blocks 7-8:** Privacy and how the data is being protected.

**Block 9:** Preparation for a data breach.

The Individual Blocks and the thought process behind them are described next, as well as the helpful information that is provided in the user manual which aids the user when brainstorming about each block:

***1. Data Group(s)***

*What type of people do you hold personal data on? Employees/Customers/Adults/Children etc?*

A very simple opening block but fundamental for the purpose of the Privacy Canvas. The user must identify who they are holding data on. The block is first as completing it will help the user finish the rest of the canvas.

***2. Data Type***

*What type of data do you hold? Children data? Sensitive data? Biometric data(data that could identify a person)?*

A similar block to block one in terms of importance and complexity.

***3. Purpose and Accuracy***

*What is the purpose of keeping this data? Is the data being updated to uphold its accuracy? Is there a time limitation on the storage of the data? Is the data only being used for the initial required use?*

***4. Consent***

*Has consent been asked for data collection or will it be asked? Is it presented clearly? Is consent revocable?*

***5. Transparency***

*Is there transparency in the processing and use of the data? I.e: Info notices, paper trails etc.*

***6. Data Rights***

*Can data subjects access their data on request? Can the data be erased? Can data subjects object to certain types of use of the data eg: direct marketing? Will data subjects be notified on a data breach?*

***7. Storage***

*Is there a storage time limitation? What technical measures have been taken to protect personal data from un-authorised access? What level of security is needed?*

***8. Data Governance***

*What measures have been implemented/completed to reduce the risk/impact of a breach? Eg: Data Protection Impact Assessment (DPIA), audits, policy reviews, data protection officer, privacy canvas, certifications.*

***9. Breach***

*What happens after a data breach? Who is notified? Do you maintain an internal breach register? Possibility of administration fines.*

# Bibliography

PETs controls matrix - A systematic approach for assessing online and mobile privacy tools. (2019). [online] Available at: https://www.enisa.europa.eu/publications/pets-controls-matrix/pets-controls-matrix-a-systematic-approach-for-assessing-online-and-mobile-privacy-tools [Accessed 28 Mar. 2019].

Itgovernance.co.uk. (2019). *GDPR Penalties and Fines | IT Governance UK*. [online] Available at: https://www.itgovernance.co.uk/dpa-and-gdpr-penalties [Accessed 28 Mar. 2019].

Osterwalder, A., & Pigneur, Y. (2010). Business Model Generation. Hoboken, NJ: Wiley.

Lewis, D., Reijers, W., & Pandit, H. (2018 ). Discussing Ethical Impacts in Research and Innovation: The Ethics Canvas. IFIP TC9 Human Choice and Computers Conference (in press).

Boardman, R., Mullock, J. and Mole, A. (2017). [online] Twobirds.com. Available at: https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en [Accessed 30 Mar. 2019].

D'Acquisto, G., Domingo-Ferrer, J., Kikiras, P., Torra, V., de Montjoye, Y. and Bourka, A. (2016). Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics. *ENISA*. [online] Available at: https://www.enisa.europa.eu/publications/pets-controls-matrix/pets-controls-matrix-a-systematic-approach-for-assessing-online-and-mobile-privacy-tools [Accessed 1 Apr. 2019].

Ethicscanvas.org. (2017). *The Ethics Canvas*. [online] Available at: https://www.ethicscanvas.org/ [Accessed 4 Apr. 2019].

General Data Protection Regulation (GDPR). (2016). *Art. 35 GDPR – Data protection impact assessment | General Data Protection Regulation (GDPR)*. [online] Available at: https://gdpr-info.eu/art-35-gdpr/ [Accessed 7 Apr. 2019].

Bieker, F., Friedewald, M., Hansen, M., Obersteller, H. and Rost, M. (2016). A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation. *Privacy Technologies and Policy*.

The Eight Principles of Data Protection | Data Protection Commission. (2019). *The Eight Principles of Data Protection | Data Protection Commission*. [online] Available at: https://www.dataprotection.ie/en/individuals/eight-principles-data-protection [Accessed 9 Apr. 2019].