Privacy	Human Rights	Competitive Advantage	Policies	Attitudinal Differences
key topic of interest and concern for those involved with any aspect of online activity (Furnell & Phippen, 2012, p. 12)	In Magna Carta, one of the first definitions of the rights of the individual in history, there is no mention of privacy and personal information had little value (Furnell & Phippen, 2012, p. 12)	With the advent of the merchant classes came competition and with it the concept of competitive advantage, the value of personal information began to increase and with it the need for privacy (Furnell & Phippen, 2012, p. 12)	Further exploration of key policies illustrates the complexity or verbosity of language, and the lack of adherence to standards (Furnell & Phippen, 2012, p. 12).	Data from the I in Online project, which explored young people's attitudes toward data protection (including their appreciation of privacy policies), highlights a tension between the understanding of what a policy is, and what it actually conveys (Furnell & Phippen, 2012, p
It is only in post-war capitalist societies that we see an exponential interest. It is the advent of the Internet, with its facilitation of global instant access to information at virtually no cost, that has raised massive concerns for the privacy of one's personal data. And this is due to the number of companies and organisations wishing to access such	Data sovereignty, explicit consent and transparency are only achievable if users understand how their privacy is protected (Feth, 2017, p. 290).	There are occasions when people end up imparting information that might be useful to someone who'd like to social engineer them later (Furnell & Phippen, 2012, p. 13).	Health care privacy is an increasingly complex legal and operational issue facing the healthcare industry (Fung, Paynter, 2008, p. 187)	Social norms evolve over time (Furnell & Phippen, 2012, p. 13). There are great variations in users' natural privacy stances and behaviours. Some seem to protect their online privacy as a point of principle over practicality, others seem to want to share everything and anything with their online friends (Furnell & Phippen, 2012, p. 13).

information, and their reasons for doing so (Furnell & Phippen, 2012, p. 12).				
A key example of where users are able to post and share sensitive data is within social networks. However, these are often contexts in which they tend to show little regard for privacy. (Furnell & Phippen, 2012, p. 13).	Privacy policies are written by lawyers for lawyers (Waldman, 2016 as cited by Feth, 2017, p. 290).	Advances in information technology have increased the efficiency of providing healthcare services to patients (Fung, Paynter, 2008, p. 187)	A substantial barrier is the lack of enforceable privacy rules (Fung, Paynter, 2008, p. 187)	Much of what gets posted could be dismissed as innocuous 'noise' (Furnell & Phippen, 2012, p. 13).
Privacy concerns include: -healthcare Web sites that do not practice the privacy policies -computer break-ins -Insider and hacker attacks -temporary and careless employees -virus attacks -human errors -system design faults -social engineering	Over the years, a drastic increase in online information disclosure spurs a wave of concerns from multiple stakeholders (Ermakova, Baumann, Fabian & Krasnova, 2014, abstract).	These systems justify themselves in terms of cost and life savings (Fung, Paynter, 2008, p. 187)	Unlike other personal information, there is very little legal protection for medical records (Fung, Paynter, 2008, p. 187)	According to (Wirtz et al., 2007, p. ?), "increased concern resulted in higher power-enhancing responses such as the fabrication of personal information, use of privacy-enhancing technologies and refusal to purchase" (Feth, 2017, p. 289).

(Fung, Paynter, 2008, abstract)				
Unauthorized disclosure of an individual's private medical information can affect one's career, insurance status, and even reputation in the community (Fung, Paynter, 2008, p. 187)	Jensen and Potts (2003, p. 1) state that the concept of privacy policies "builds on the idea of fair warning and implicit consent" (as cited by Ermakova, Baumann, Fabian & Krasnova, 2014, p.1).	Modern IT systems are getting more and more customized and aligned to the user. However, this comes along with massive collection, processing, and potentially sharing of sensitive data (Feth, 2017, p. 289).	Privacy policies are the state of the practice technique to achieve data transparency (Feth, 2017, abstract).	The user has to decide whether he believes that the provider adheres to the privacy policy (Feth, 2017, p. 290).
Without adequate privacy protection, individuals must take steps to protect themselves from what they consider harmful and intrusive uses of their health information, often at significant costs to their health (Fung, Paynter, 2008, p. 187)	In this new context, privacy guarantees are essential: guarantees about the potential release of data to unintended recipients and the use of user data by the service provider (dos Santos Brito, Cardoso Garcia , Araujo Durao, & Romero de Lemos Meira, 2013, abstract)	Privacy policies are written by lawyers for lawyers (Waldman, 2016 as cited by Feth, 2017, p. 290).	Instead of having one generic privacy policy that has to fit every use case and every user group, contextual privacy statements provide concrete information about privacy data protection in a specific use case or activity (Feth, 2017, abstract).	An example for that is Android's permission system that presents the app permissions at installation time. Only 17% of users paid attention to this information and only 3% understood the information that was presented (Feth, 2017, p. 290).
When people publish a lot of personal data, privacy requirements are very hard to satisfy (dos Santos Brito,	People view their profiles as a form of self-expression (dos Santos Brito, Cardoso Garcia , Araujo Durao,	All of these issues result in a high mental load, which users are typically unable or unwilling to spend.	Privacy policies are legally demanded (Feth, 2017, p. 290).	In a survey by Obar and Oeldorf-Hirsch (2016) it is stated 74% of users skipped the privacy policy completely. For

Cardoso Garcia , Araujo Durao, & Romero de Lemos Meira, 2013, p.1)	& Romero de Lemos Meira, 2013, p.1)	Even if they are willing to spend high effort, some aspects are still not possible to understand (Feth, 2017, p. 290).		the remaining 26% of the users, the average reading time was only 73 seconds (Feth, 2017, p. 290).
Questions of selective exposure are enhanced in the Internet era (Coppini, Duncan, McLeod, Wise, Bialik, Wu, 2017, p. 766). This development has raised concern about ideologically based selective exposure as audience members tailor their media exposure to fit their political ideology (Iyengar & Hahn, 2009; Kinder, 2003; Stroud, 2008 as cited by Coppini, Duncan, McLeod, Wise, Bialik, Wu, 2017, p. 766).	Accidental data release to unintended recipients is one possible way in which privacy of a social media user's information can be compromised (dos Santos Brito, Cardoso Garcia , Araujo Durao, & Romero de Lemos Meira, 2013, p.1)	Earp et al., (2005) observes the way most privacy policies are written protects the organization from potential privacy lawsuits than addresses users' privacy concerns (Ermakova, Baumann, Fabian & Krasnova, 2014, p.1).	(Waldman 2016) study observed the average word count of a privacy policy is 2716 words (Feth, 2017, p. 290).	Users resent the "behind the closed doors" processing of their personal data by companies (Ermakova, Baumann, Fabian & Krasnova, 2014, abstract).
Surveillance devices such as closed-circuit television (CCTV), camera, and	People are no longer simply receivers of information, but they are senders and	Consumers often need a higher than average reading level and vocabulary of legal	(Cranor 2012) posited users would need 244 hours per year in average to read the	The study shows that the stronger a user believes in having understood the privacy

smartphone play an important role in monitoring human activities, behavior, and any varying information. In other words we can say surveillance devices are sensing devices for monitoring purpose (Chui, Vascant, & Liu, 2019, p. 112)	creators as well (Coppini, Duncan, McLeod, Wise, Bialik, Wu, 2017, p. 766).	terms to properly comprehend the text presented to them (Hochhauser, 2001; Anton et al., 2004; McDonald et al., 2009 and Signh et al., 2011 as cited by Ermakova, Baumann, Fabian & Krasnova, 2014, p.1).	privacy policy of every website they visit (Feth, 2017, p. 290).	policy, the higher he or she trusts a web site across all companies we studied (Ermakova, Baumann, Fabian & Krasnova, 2014, abstract).
It is estimated that the world collects 566 petabytes of video data every day(Data, 2016) which has already putting challenges in data transmission and storage and even more complicated when it comes to data analytics (as cited by Chui, Vascant, & Liu, 2019, p. 112)	Information receivers today are interactive participants in news distribution. They not only seek information, but pass it along to others (Coppini, Duncan, McLeod, Wise, Bialik, Wu, 2017, p. 766).	When a network mimic in-person interactions, people are often willing to reveal many more private details than they would otherwise (3, 4 as cited in dos Santos Brito, Cardoso Garcia , Araujo Durao, & Romero de Lemos Meira, 2013, p.1)	Privacy policies are written by lawyers for lawyers (Waldman, 2016 as cited by Feth, 2017, p. 290).	Legitimately drives companies to question their effectiveness in addressing user privacy concerns as well as their role in promoting trust (Ermakova, Baumann, Fabian & Krasnova, 2014, p.1).
One of the most important surveillance cameras' applications is to detect and prevent	Online news media platforms allow individuals to comment on media stories, pass	But as the digital media environment continued to evolve into the 21st century with the advent	Privacy policies are abstract and generic. There is only one single policy for the whole service. It remains the	Content sharing services have become immensely popular on the Web. More than 1 billion people use this kind of

crimes (e.g. violent crime, theft from auto and auto theft) (Chui, Vascant, & Liu, 2019, p. 115)	along links to those stories to other individuals, and add commentary along with the link Coppini, Duncan, McLeod, Wise, Bialik, Wu, 2017, p. 766).	of technologies that facilitated mobile, diversified, personalized and interactive media experiences, the traditional uses and gratifications typology that has formed the basis for this approach proved in need of a makeover (Coppini, Duncan, McLeod, Wise, Bialik, Wu, 2017, p. 766).	users' task to map this policy to the current activity or data he is dealing with (Feth, 2017, p. 290).	services to communicate with friends and exchange all sorts of information (dos Santos Brito, Cardoso Garcia , Araujo Durao, & Romero de Lemos Meira, 2013, abstract)
In general, video data are used only after the fact as a forensic tool, thus losing their primary benefit as real-time and active medium (Chui, Vascant, & Liu, 2019, p. 115)	As news consumers we have become news curators, contributing to the information flows and discussion through networked communities, individuals have more opportunity to express themselves, their identity and solidarity with others at less cost (Loader & Mercea, 2011; Rainie & Wellman, 2012 as cited by Coppini, Duncan,	These labels recognize that information behaviors represent active attempts to have an impact on the self or on others (Coppini, Duncan, McLeod, Wise, Bialik, Wu, 2017, p. 767).	Existing research offers limited insight into the connection between readability and comprehensiveness of privacy policies and users' willingness to trust (Pan and Zinkhan, 2006; Sultan et al., 2002 as cited by Ermakova, Baumann, Fabian & Krasnova, 2014, p.1).	Although the general public is concerned about privacy questions related to unintended audiences, data usage by service providers is still misunderstood (dos Santos Brito, Cardoso Garcia , Araujo Durao, & Romero de Lemos Meira, 2013, abstract)

	McLeod, Wise, Bialik, Wu, 2017, p. 767).			
Society has also generated a progressive invasion of privacy, which sometimes remains unnoticed (Aïmeur, Lafond, 2013, p. 821).	Literature on cognitive dissonance (Festinger, 1957), mass communication researchers theorized that citizens would stay away from media content that is inconsistent with their opinions and beliefs to avoid exposure to dissonant information (Klapper, 1960 as cited by Coppini, Duncan, McLeod, Wise, Bialik, Wu, 2017, p. 767).	There exist greater opportunities for individuals to engage in politically motivated selective exposure to news and information (Coppini, Duncan, McLeod, Wise, Bialik, Wu, 2017, p. 767).	Even if people want to protect their privacy and read every policy they stumble upon, they face too many hurdles: privacy policies are hard to understand, often requiring a considerable amount of background knowledge to make an informed choice and do not offer the user a choice that reflects his or her preferences (Solove (2013) as cited by Aïmeur, Lafond, 2013, p. 822).	The aim of the survey was to discover how people care about the use of their personal data by service providers in terms of social media (dos Santos Brito, Cardoso Garcia , Araujo Durao, & Romero de Lemos Meira, 2013, abstract)
This is what privacy scholars call "security by obscurity" (Morosov, (2011) as cited by Aïmeur, Lafond, 2013, p. 821).	Civil liberties activists and groups are usually opposing the full-scale deployment of surveillance system that cannot guarantee perfect privacy (Chui, Vascant, & Liu, 2019, p. 119)	Citizens engage in selective expression when they share media content congruent with their political views (Coppini, Duncan, McLeod, Wise, Bialik, Wu, 2017, p. 767).	It is important to ensure that EHRs are used in a way that the integrity of personal information is preserved and that patients have control and access to their records (Aïmeur, Lafond, 2013, p. 822).	In general we found that people: -do not read license terms -do not know much about service policies -when presented with the policies people do not agree with them -there are some differences between generations in relation

				to how they care about their data (dos Santos Brito, Cardoso Garcia , Araujo Durao, & Romero de Lemos Meira, 2013, abstract)
Personal information collected includes: • Identifying information • Buying patterns • Navigation habits • Lifestyle • Sensitive Data • Biological information (Aïmeur, Lafond, 2013, p. 821).	One issue that has been debated for more than a decade revolves around the legislation of information collection measures (Aïmeur, Lafond, 2013, p. 821).	Sharing information has beneficial effects on the sender (Namkong, Shah, Han, Kim, Yoo, Fan & Gustafson, 2010: Namkong et al., 2013) and on discussion and deliberation (Cho et al., 2009 as cited in Coppini, Duncan, McLeod, Wise, Bialik, Wu, 2017, p. 767).	Security protects learners' information against unwarranted access, but not against abuse from authorized access (Aïmeur, Lafond, 2013, p. 823).	This study integrates theories of selective exposure with an updated uses and gratifications typology to account for partisans' motivations for consuming and sharing ideologically consistent information (Coppini, Duncan, McLeod, Wise, Bialik, Wu, 2017, abstract).
Canada began digitizing all its citizen's medical records in 2012 implementing an Electronic Health Record (EHR) at an estimated cost of 10 billion (Aïmeur, Lafond, 2013, p. 822).	Individuals are never forced to give away their personal data to the websites they visit (Aïmeur, Lafond, 2013, p. 822). Therefore it is possible to argue that it is legitimate for collectors	When people share content from the opposing side, it is often to ridicule it and portray it in a negative way (Mitchell et al., 2014, Coppini, Duncan, McLeod, Wise, Bialik, Wu, 2017, p. 768).	Enforcing the Integrity and Confidentiality of the learner's information does protect the learner's data from unauthorized access (Aïmeur, Lafond, 2013, p. 823).	Uses and gratifications is a theory that explains the choices that people make in terms of selecting media, channels and programming (Blumler, 1979 as cited by Coppini, Duncan,

The recorded information includes: -individual's features -height -waist -body fat -past diseases -last visits to emergency clinics -fertility status -emotional problems (Yin Ling Fung (2008) as cited by Aïmeur, Lafond, 2013, p. 822).	to use that information (Aïmeur, Lafond, 2013, p. 822).			McLeod, Wise, Bialik, Wu, 2017, p. 766).
Hackers are always on single step behind the development of a new technology (Aïmeur, Lafond, 2013, p. 822-823).	One major concern regarding the centralization of data as sensitive as health information is the protection of privacy (Aïmeur, Lafond, 2013, p. 822).	Individuals tend to act differently depending on whether their choices are public or private (Coppini, Duncan, McLeod, Wise, Bialik, Wu, 2017, p. 768).	The tutor has access to virtually all the remaining information including, but not limited to who the students are, what parts of the course they referred to, how many times and for how long, as well as ll the messages in the forums and all the information about the quizzes and tests the learner took in his course (Aïmeur, Lafond, 2013, p. 823).	For these reasons, motivations such as shaping social identity and influencing others become more relevant in the interactive social media environment (Coppini, Duncan, McLeod, Wise, Bialik, Wu, 2017, p. 767).

Then comes the question of whether or not digital traces (cookies, etc) should be considered as personal data (Aïmeur, Lafond, 2013, p. 823).	Concerns: -one could sell this information -steal someone's identity -Malevolently use the information to exploit one's medical weaknesses (Aïmeur, Lafond, 2013, p. 822).	Motivations related to status, image and persuasion tend to be more closely associated with expressive behaviors than with consumption behaviours (Lee & Ma, 2012, as cited by (Coppini, Duncan, McLeod, Wise, Bialik, Wu, 2017, p. 768).	The Data Loss Data base regularly reports on breaches concerning student records (Aïmeur, Lafond, 2013, p. 823).	The updated uses and gratifications theory presenting in this study is based on five motivations: -mood management -information management -opinion management -relationship management -identity management (Coppini, Duncan, McLeod, Wise, Bialik, Wu, 2017, p. 767).
Traces divulge information on the browsing habits of users, allowing the collection of personal information without the individual's knowledge or consent (Aïmeur, Lafond, 2013, p. 823).	A debate that has yet to be resolved is whether a patient can have free access to his own records. Or more specifically, who owns this information? (Aïmeur, Lafond, 2013, p. 822).	When individuals make choices for the purpose of passing that information on to others, individuals, and in particular partisans, should be more motivated to choose sources that can reaffirm their identity and possibly affect public opinion (Coppini, Duncan, McLeod, Wise, Bialik, Wu, 2017, p. 768).	The majority of Internet users do not read privacy policies because of their lengthy verbose format (Aimeur, Lawani, Dalkir, 2016, abstract).	Citizens are more likely to consume content that is consistent with their views and interests (Prior, 2007 as cited by Coppini, Duncan, McLeod, Wise, Bialik, Wu, 2017, p. 767).

These systems collect large amounts of information about the learner, information that could be misused, therefore violating his privacy, which is the claim of individuals to determine what information about themselves is known to others, as well as how it is used (Westin (1967) as cited by Aïmeur, Lafond, 2013, p. 823).	It is difficult to find a balance between the well-being of a patient and the preservation of his privacy (Aïmeur, Lafond, 2013, p. 822).	Identity and opinion management are likely motivations when projected to the public (Coppini, Duncan, McLeod, Wise, Bialik, Wu, 2017, p. 768).	Privacy policies are the main source of information for users about how their data are collected and used (Aimeur, Lawani, Dalkir, 2016, abstract).	The Internet complicates this picture because exposure to disagreement online could attenuate the negative effects of selective exposure (Jun, 2012; Kim, Chen & Gil de Zuniga, 2013 as cited by Coppini, Duncan, McLeod, Wise, Bialik, Wu, 2017, p. 767).
Privacy is nearly absent in current E-learning systems (Aïmeur, Lafond, 2013, p. 823).	Mobile payment technology requires businesses to be aware of the potential security threats it incurs (Aïmeur, Lafond, 2013, p. 822).	Sharing news online should activate motivations that are more closely related to identity and persuasion (Coppini, Duncan, McLeod, Wise, Bialik, Wu, 2017, p. 768).	Privacy policies are the channel through which Internet services disclose to their users the data they collect from them and use that is made of it (Aimeur, Lawani, Dalkir, 2016, p. 368).	Empirical research has shown that partisans are more likely to select news sources that are consistent with their political beliefs and orientation. Classical experiments on selective exposure show that, when given a choice, partisans will select choices that are consistent with their views (Coppini, Duncan,

				McLeod, Wise, Bialik, Wu, 2017, p. 767).
Only primitive forms of privacy are offered in some platforms, for example, restricting tutor access to certain pieces of data such as auto-evaluations performed by the learners (Aïmeur, Lafond, 2013, p. 823).	Users are practically forced to fully accept the terms of the policy in order to use the service (Aimeur, Lawani, Dalkir, 2016, p. 368).	At the age of exposure, Internet communication and exchanges between different entities(such as individuals, businesses, governments and information systems) have grown at an ever-increasing speed (Aïmeur, Lafond, 2013, p. 821).	Few users take the time to read the policies before making a purchase or using a service, this is due to the length of the privacy policies (Ermakova et al, 2014, McDonald & Cranor, 2008 as cited by Aimeur, Lawani, Dalkir, 2016, p. 369) and the difficulty of reading and understanding them (Furnell & Phippen, 2012 as cited by Aimeur, Lawani, Dalkir, 2016, p. 368) and their non specific and vague content and their non-standard formats (Schaub, Breaux, & Sadeh, 2014 as cited by Aimeur, Lawani, Dalkir, 2016, p. 368).	A new paradigm in the field of communication now focuses on sender effects, including studies that investigate the effects that sharing media messages can have on individuals (Pingree, 2007 as cited by Coppini, Duncan, McLeod, Wise, Bialik, Wu, 2017, p. 767).
Users do not really know what information	Users face a dilemma where they generally	It is not always clear whether the individuals have clear knowledge of		Acts of selective expression have been

is collected about them and shared with third parties (Richards & King, 2014 as cited by Aimeur, Lawani, Dalkir, 2016, p. 369).	lose as they must select between two unappealing choices (Aimeur, Lawani, Dalkir, 2016, p. 368).	the information that is gathered and how it is used (Aïmeur, Lafond, 2013, p. 822).		under-studied and the contours of when and why individuals engage in such behaviors remain unclear (Coppini, Duncan, McLeod, Wise, Bialik, Wu, 2017, p. 767).
Data Protection authorities are faced with an unclear role running the risk of creating false expectations among the general public (Aldhouse, 2018, p. 816).	Users either accept the terms of the policy at the risk of losing their privacy, or they refuse to adhere to the policy and then they do not have access to the service (Aimeur, Lawani, Dalkir, 2016, p. 368).	-can be very useful for the storage of patient records or the execution of repetitive tasks in a clinical environment (Aïmeur, Lafond, 2013, p. 822). -potential cost reduction (Aïmeur, Lafond, 2013, p. 822). -process optimization (Aïmeur, Lafond, 2013, p. 822).	Knowing that privacy policies are the main source of information for users about the services' privacy practices and the place where users give their consent to those practices, they should be presented in a friendly format allowing users to read and really understand their contents (Aimeur, Lawani, Dalkir, 2016, p. 368).	More than a billion web users are blogging, Googling, Facebooking, Tweeting- and most of the information they divulge is simply lost in the endless ocean of digital ephemera produced by others (Aïmeur, Lafond, 2013, p. 821).
Spiros Simitis is a distinguished father of data protection. He believed in 1985 there were four essentials for	The introduction into the parliamentary organization also underlies the essential difference between the	it has been demonstrated that the introduction of automated medical systems could	More than 50% of Canadians never read privacy policies (Canada, 2013 as cited	There are many users who are still willing to share their personal information, even if they are aware of the consequences. These

an efficient regulation of personal data processing, the fourth being there must be an independent authority to enforce data regulations (2- Spiros Simitis Reviewing Privacy in an Information Society' 135 U Pa Law Review 707 (1987) as cited by Aldhouse, 2018, p. 816).	Data Protection Commissioner and nearly every other state agency created during the last decades. Its task consists not of helping government enforce its policies but of preventing both government and private institutions from overstepping the boundaries guaranteeing the democratic structure of society (2- Spiros Simitis Reviewing Privacy in an Information Society' 135 U Pa Law Review 707 (1987) as cited by Aldhouse, 2018, p. 816).	- improve the relationship between the patients and the physicians (Aïmeur, Lafond, 2013, p. 822). -compensate for staff shortages (Aïmeur, Lafond, 2013, p. 822). -ease the jobs of nurses (Aïmeur, Lafond, 2013, p. 822). -encourage collaboration between distant health facilities (Aïmeur, Lafond, 2013, p. 822).	by Aimeur, Lawani, Dalkir, 2016, p. 369).	are advocates of open access information called "publicness" (Jarvis (2011) as cited by Aïmeur, Lafond, 2013, p. 822).
David Flaherty in 1986 stated: "It is the task of the data protection office to articulate the privacy interests at stake, as elusive as they may be on occasion. It is not the task of data protectors to draw the	Data protection enforcement or prosecution is of necessity a balancing act or rather a careful decision about which of several competing rights should prevail (4- Professor Francois	Marketing and advertising companies have understood the power of information for a very long time. The more thy know about demographics, consumer habits, and preferences of particular customer types, the	Only 4% of Internet users regularly read privacy policies, while 55% of respondents never read the terms of the agreement (dos Santos Brito, Cardosa Garcia, Araujo Durao & Romero de Lemos	Users do not trust online services with respect to the use of their private data… they find it unfair that their data are used to generate revenue by online services without their knowledge or

suitable balance between personal privacy and competing values' (3- David Flaherty on making Data Protection Effective Paper presented to the National Forum on Access to Information and Privacy, Ottawa, Canada 6-7 March 1986 as cited by Aldhouse, 2018, p. 817).	Rigaux, 'La vie privee, une liberte parmi les autres' Pr as cited by Aldhouse, 2018, p. 817).	more they can tailor their product offerings and the more sales they can make (Morosov (2011) as cited by Aïmeur, Lafond, 2013, p. 822).	Meira, 2013 as cited in Aimeur, Lawani, Dalkir, 2016, p. 369).	without their benefit from this (Aimeur, Lawani, Dalkir, 2016, abstract).
Complex orchestrations of co-operations between multiple actors, the processing of personal data is becoming intransparently complex …if trust in such services is eroded, the growth of the Web and the digital economy itself, and therefore the prosperity of society in general are endangered (Bonatti et al., 2018, p. 1).	Managing privacy and understanding the handling of personal data has turned into a fundamental right- at least for Europeans (Bonatti et al., 2018, p. 1).	Companies need to put effort into making word of mouth as positive as possible (Aïmeur, Lafond, 2013, p. 822).	It takes approximately 76 working days to read all the privacy policies of all websites visited in one year (Aimeur, Lawani, Dalkir, 2016, p. 369).	In their paper, the authors believe that giving users control of their data coupled with caring about their interests would restore the trust of users (Aimeur, Lawani, Dalkir, 2016, abstract).

	General Data Protection Regulation came into force May 25th (Bonatti et al., 2018, p. 1).	One of the main advantages of E-Learning and Intelligent Tutoring systems is their adaptability to the learner's specific needs and preferences. Users are increasingly aware of the value of their data (Aimeur, Lawani, Dalkir, 2016, p. 368).	There is a need to enable true transparency, user configuration, and manageable privacy policies and data portability (Bonatti et al., 2018, p. 1). The authors argue that the need can be met through agreed upon vocabularies (Bonatti et al., 2018, p. 1).	In an experimental comparative study (717 participants surveyed) of user trust results show that allowing personalization and management in privacy policies affects user trust and makes online services appear more trustworthy to their users (Aimeur, Lawani, Dalkir, 2016, p. 368).
	The level of privacy and trust concerns has raised to a point where regulator, citizens and companies have started to take action (Bonatti et al., 2018, p. 1).	In a study that investigated the differences between experts and typical users, results show that there were important discrepancies in the interpretation of privacy policies language, mostly with respect to data sharing (Reidenberg et al., 2014 as cited by Aimeur, Lawani, Dalkir, 2016, p. 369).	The challenge is how to convey the transparency to the user to allow for informed personal data self determination (Bonatti et al., 2018, p. 1).	We hypothesise that users' control over their data, as well as caring about their interests in exchange for the use of their data can actually help reach this level of trust (Aimeur, Lawani, Dalkir, 2016, p. 368-369).

		The study indicates that privacy policies are sometimes unfair and may mislead people's decision making (Aimeur, Lawani, Dalkir, 2016, p. 369).		A study of current attitudes noted that people's attitudes have not changed between 2005 and 2014, stating that privacy policies are still too long, too complex and serve mostly to protect organizations (Williams, Agarwal & Wigand, 2015 as cited by Aimeur, Lawani, Dalkir, 2016, p. 369).
		For the few people that take the time to read privacy policies, they often lack the expertise to adequately assess the **consequences** of agreeing to the collection, usage or disclosure of their personal data (Aimeur & Lafond, 2013, as cited by Aimeur, Lawani, Dalkir, 2016, p. 369).		There is a need for a level of trust (Bonatti et al., 2018, p. 1).