Sender vs Recipient Orientated Information Systems Revisited

ABSTRACT

Purpose

Belkin and Robertson (1976a) reflected on the ethical implications of theoretical research in information science, and warned that there was potential for abuse of knowledge gained by undertaking such research and applying it to information systems. In particular, they identified the domains of advertising and political propaganda that posed particular problems. The purpose of this literature review is to revisit these ideas in the light of recent events in global information systems that demonstrate their fears were justified.

Design/methodology/approach

We revisit the theory in information science that Belkin and Robertson used to build their argument, together with the discussion on ethics that resulted from this work in the late 1970's and early 1980's. We then review recent literature in the field of information systems, specifically information retrieval, social media and recommendation systems that highlight the problems identified by Belkin and Robertson.

Findings

Information science theories have been used in conjunction with empirical evidence gathered from user interactions that have been detrimental to both individuals and society. It is argued in the paper that the information science and systems communities should find ways to return control to the user where at all possible, and ways to achieve this are considered.

Research limitations/implications

The ethical issues identified require a multidisciplinary approach with research in information science, computer science, information systems, business, sociology, psychology, journalism, government and politics etc. required. This is to large a scope to deal with in a literature review, and we focus only on the design and implementation of information systems (Zimmer, 2008a) through an information science and information systems perspective.

Practical Implications

We argue that information systems such as search technologies, social media applications and recommendation systems should be designed with the recipient of information in mind (Paisley and Parker, 1965), not the sender of that information.

Social Implications

Information systems designed ethically and with users in mind will go some way to addressing the ill effects typified by the problems for individual and society evident in global information systems.

Originality

We synthesize the evidence from the literature to provide potential technological solutions to the ethical issues identified, with a set of recommendations to information systems designers and implementers.

KEYWORDS
Information science theory, Information systems, ethics, privacy, security, user interaction

1 Introduction

Claude Shannon (1948) in his seminal work on communication identified three main components in an interaction in telecommunication: the message sender, the message recipient and a communication channel between them (see figure 1). His model was influential in information science (Belkin and Robertson, 1976b) and has been used as a theory to understand how information is exchanged between users and how users can gain knowledge by engaging with the information obtained (Belkin and Robertson, 1976a; Belkin and Robertson, 1976b), despite warnings the the theory could be oversold (Shannon, 1956). A typical example is a searcher (the recipient) who uses an information retrieval system (e.g. Google, Dialog ProQuest) as a channel to retrieve documents to resolve an information need (documents written by an author or authors – the sender). The actor who controls the communication channel (the information system) is an intermediary between a sender (message generator) and a recipient (message consumer) and has the power to provide the information needed, deny access or even provide information that is misleading. To ensure the recipient obtains a message they actually need (i.e. information that is relevant and appropriate to address the knowledge gap), information systems should focus more on the needs of end users primarily in mind, namely the message recipients. Paisley and Parker (1965) argued that information systems should be adapted to the user providing them with maximum control, rather than the user having to adapt to the system. We should therefore design information systems, applications and services with needs of the user (message recipient), connecting them with senders with good intent (providing useful, accurate and relevant information), rather the senders with malicious intent (e.g. the propagandist, advertiser or spammer).

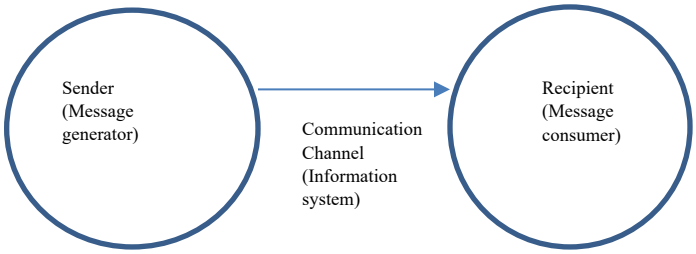

Figure 1: The Shannon Model of Communication

The information system designer or service provider has a great deal of power over what information the end user obtains, and hence on what they use it for (e.g. to fulfill a certain task). It is therefore incumbent on the designers to act in an ethical manner, and they should not be swayed by the needs of a malicious sender (e.g. spammer), or use their privileged position for their own benefit. Privacy is a universal human need (Acquisti et al, 2015), and has become a significant concern in information systems (Nissenbaum, 2020). The key argument of this paper is to assert ethical behavior in information system to address issues such as privacy. We review this argument in light of historical perspectives on the problem of ethical information communication and recent events that have shed light on this problem. The aim of the paper is therefore to highlight the urgent need to return to a design/service ethos that is recipient-focused rather than sender-focused, to ensure that the user obtains information they need, without undue influence. Furthermore, the paper argues for greater user control of the system and the data held on it, returning autonomy to the user (Susser *et al*, 2019a;2019b). We argue for a move away

from systems that are opaque to the user (Rieder 2005), to systems that provide explanations of sender and system intent using the assumption that the most intelligent part of any system is the end user (Ingwersen, 1992). The argument therefore is very much in line with Paisley and Parker's (1965) idea of a recipient controlled communication system that they characterized as an information system with maximal user control. Whilst the paper draws heavily on theoretical ideas in information science, it focuses mainly on the practical applications of these theories in information systems such as information retrieval, information filtering, recommendation etc. The scope is therefore limited to these technologies, and does not address business models (that many information systems rely on for revenue) or other (e.g. psychological) perspectives on influence. We start by providing an historical perspective on the problem of ethical information communication (section 2) and give an overview of the present day effects (section 3) addressing the problem of designing sender orientated systems. We outline key ethical principles in section 4, providing overall strategic and architectural solutions to the problems identified. We apply these principles to the proposed solutions and provide high level recommendations for systems design and implementation, focusing on how to design information systems that are truly recipient-oriented (Zimmer, 2008a). A conclusion is provided at the end suggesting a general approach to the problem.

2 A historical perspective on the problem

Wiener (1954) introduced the term Cybernetics to argue for a theory to understand the transmission of messages between different types of actors (human, machine) that can influence or assert control on other actors. His writing was influenced by Shannon (1948). Wiener identified various problems in the use and application of automatons (a machine or computer program) such as human loss of control, leading to dependency or control by the automatons themselves. Furthermore, trusting decisions made by such automatons may be detrimental to human interests, as they do not share the same value system as the humans they serve. Although these ideas are rather abstract, there are key lessons to be learned if we consider an information system to be an automaton; such an automaton could learn from users' interactions and this could result in the user surrendering control to the system. Consider, for example, how using machine learning algorithms to infer user interests can lead to control of the user's interactions passing from the human (user) to the automaton (information system). Blanke (2005) observes this effect on search engines using Wiener's ideas. This highlights the need to consider the impact of technology before introducing it into society. He did however point to potential positive outcomes where such automata can be 'used for the benefit of man, for increasing his leisure and enriching his spiritual life' (Wiener, 1954; p162).

Belkin and Robertson (1976a) address the issue of ethical information communication head on - in the specific context of information science research. They identify different types of information systems, such as sender or recipient controlled information systems (analogous to the Shannon model (Shannon, 1948) overviewed above). Their focus was on an information scientist being the interface (or communication channel) between the sender and recipient, but theories developed since them such as the Robertson/Sparck Jones probabilistic model (Robertson and Sparck Jones, 1976) have allowed information software and systems to take over that role. A key concern voiced by Belkin and Robertson (1976a) was that study of recipients (users) might shed light on a user state of knowledge before and after an information request was made, and that this evidence could be used by the sender to provide the recipient with a message which suits the sender's (rather than the recipient's) purposes. They expressed concern that such systems could be used for malign purposes e.g. in political propaganda or advertising, potentially harming the interests of the user (recipient) or manipulating them (Susser *et al*, 2019a;2019b). They therefore posed questions on whether or not research into theories of information

science that provide a theoretical foundation for developing sender-oriented information systems should be carried out at all. They point to examples of research in nuclear physics and genetics, where researchers faced the same kinds of dilemmas we face in the discipline. However, plenty of theoretical development in information science has been undertaken. In particular, the cognitive model of information retrieval (Ingwersen and Järvelin, 2006) has now become the standard theory used to design and evaluate information systems. The political implications of these development on information systems such as the web are documented by Introna and Nissenbaum (2000a;2000b), where potential bias could lead to narrowing choices for users. Particular issues for bias in search engines has long be recognized (Halavais, 2017). Some predictions about the technological developments to address the problem such as personalization (Goldman, 2008) have been refuted (see below), with concerns about facilitating surveillance justified (Nissenbaum, 1998; Zuboff, 2019). We review the current situation in section 3, examining the present day effects of the problem of ethical information communication.

3 Present day effects

Belkin and Robertson (1976a) expressed the hope that there would be sufficient differences between sender and recipient-controlled systems to prevent information misuse. However, they expressed fears that misuse might not be preventable; *"it is difficult to predict exactly to what use any research results will be put, but…if the possibility for malign application exists, it will be realized"* (Belkin and Robertson, 1976a). Recent events have demonstrated their fears were justified. For example, news about global information systems such as Google, Facebook and Twitter have brought the issue to the fore, particularly given their ubiquitous nature (Haider and Sundin, 2019). Choices for users have narrowed due to key economic factors e.g. the dominance of advertising as business models (Van Couvering, 2008) leading to the emergence of oligopolies. These systems are built on data collected from users and used to build business models for profit largely from an engineering perspective (Mager, 2012). Commercial interests are built into the systems and evaluated using systems criteria that may be in conflict with consumer or user interests (Van Couvering, 2007). This may lead to difference kinds of bias in systems including sociopolitical (Diaz, 2008), gender (Martey, 2008), commercal (Lewandowski,and Sünkler, 2019), race (Noble, 2018) etc that may favour one type of content over another (the 'long tail' problem). Trust in such systems may be misplaced (Schultheiß, and Lewandowski, 2021). The implications for the generation of knowledge through access to such global information systems are profound (Hinman, 2008) as systems such as Google act as gatekeepers and shape what we know (Schroeder, 2014). Known problems such as privacy (Nissenbaum, 1997), 'fake news' and 'misinformation', and addressing them given the commercial interests may be difficult. The future examples and the terms that refer to such phenomena may change, but the ill effects will be evident. The key concern is that access to information has become inequitable (DiMaggio, P. and Hargittai , 2001; Lievrouw and Farb, 2003). To better understand the present day effects of the problem, a review of work on users' interactions with information systems is necessary.

3.1 Data recorded in user interactions

When a user searches, they leave all kinds of traces of their intent via their interactions with the system. These traces can be used to find out about them and their interests. After navigating to the information system via a URL (or running an application on a device), the first major interaction is to type in a query which allows them to express what they are looking for. Depending on the user's state of knowledge, this initial query may provide useful information about the user's intent and gap in knowledge. The system produces a set of results for the user to inspect, and those that the user thinks are relevant to their needs

will be selected for viewing (e.g. manifesting as click-throughs on search engines). Once the item is retrieved, the user may express an opinion on the usefulness of the retrieved item by clicking on a 'find more like this' button or link, liking/disliking the item (e.g. on YouTube, Facebook and Twitter), re-posting/re-tweeting the item (e.g. on Twitter) or rating a film or book (e.g. on IMDb or Amazon). This gives an indication of the user's interest. Additional interactions such as this provide more data about their overall interests, or even personal attributes. Interactions with query issuing, results list and document inspection are the key areas of concern here, but eye tracking can also be used to record a user's interaction with an information system interface, for example to imply implicit relevance feedback (Moe *et al*, 2007). Mouse movements are another potential source of user interactions. We focus only on data on queries, results and documents, where there is evidence from literature to outline issues to be addressed. We examine these data using the concept of contextual integrity that posits two norms – appropriateness of the use of data and distribution of that data (Nissenbaum, 2004).

3.2 Query interactions and Data

The first issue is the initial interaction with the system – entering queries. Queries provide a lot of information about the user, and their intent will often become clearer as they issue further queries and refine and reformulate existing queries as part of their search session. An illustration of the problems that can occur is the AOL log scandal (Barbaro *et a*l, 2006). In 2006, AOL released a log of 20 million search keywords for 650k users over a three month period, intended to be used for research purposes. Although no personal information was directly revealed, user IDs were left in the log. This allowed any interested party to uniquely identify a searcher and their interests. Journalists at the New York Times were able to identify individuals from their search sessions and were able to contact one particular searcher about them – the journalists used this example in a published news article to highlight the problem. The ethics of using this data were therefore questioned (Anderson, 2006). The privacy implications are clear; even with anonymized information, any malicious actor could violate a user's privacy by building up a picture of their interests (which they may not want to be revealed to anyone) or even make inferences about them that are invalid (e.g. a journalist investigating a crime could be mistaken for someone who plans to commit one). The log was taken offline quite quickly, but it is still available for researchers (for ethical reasons we will not link to the source here). The example given here violates the principle of contextual integrity by inappropriate use of data, outside of the context in which it was originally collected e.g. to optimize the search for the user, not for research purposes.

3.3 Results lists interaction and data

Once the user has issued a query, the system presents a set of results to them. This is generally in the form of a linear list with a synopsis of the item together with a link with which the user can obtain that item (e.g. a URL in web searches). Interaction with the results lists can also provide a lot of information about a user. This is the 'click-through' data that can be collected in terms of user interactions. Libert (2015) investigated how third parties can obtain information about users through access to their retrieved documents in the context of health. This domain is particularly sensitive. Visits to health-related web pages were investigated and 91% of HTTP requests were found to make requests to third parties, whilst 70% of the HTTP referrer strings contained health information (given conditions, treatments and diseases). Information can be gathered through embedded code in a search result or through an open connection to a Facebook, Google or Twitter account on the same device. An example ethical issue is the ability of third parties to find out a user's health status, potentially raising their health premiums or deny them insurance altogether. This violates contextual integrity of the data by providing data to third

parties without the consent or knowledge of the user, with serious legal implications under legislation such as the General Data Protection Regulation (GDPR) in jurisdictions such as the European Union (2016).

A further issue to consider concerning ethical information communication is how results are ranked (in a given order, usually by estimated relevance). Most systems, including Web search engines, use some form of ranking model e.g. (Robertson and Spark Jones, 1976). It has long been known that users rarely look beyond the first page of results. For example an examination of 51k queries to the Excite web search engine found that the majority of users (58%) only viewed the first page (Jansen *et al*, 1998), whist one which examined 285 million search session on the AltaVista search engine found that around 85% of users inspected one screen per query (Silverstein *et al*, 1999). Many users may not even scroll down beyond the first set of results. Therefore, the first screen of results is expensive real estate, and authors/senders will want their content placed in that space. Tufekci (2014a) points to evidence that suggests that slight alterations in search engine ranking could potentially influence election results (Epstein and Robertson, 2013). This double blind experiment involved showing search engine results to different groups of users, showing preferences shifting toward favored candidates by ranking accordingly, with 75% of the cohort unaware of the manipulation (Epstein and Robertson, 2013). Manipulation of search engine rankings through the study of user interactions may well be detrimental - not just to the individual but to society as a whole.

A related problem is one of filter bubbles (Pariser, 2011), defined as user isolation within a given political or ideological viewpoint, where the system shows information that is different from other users who hold contrasting or opposing viewpoints. Why do researchers assert that the filter bubble phenomenon exists? From 2009, Google began to personalize search results using various data about the user such as their search interactions IP address etc. Users found search results would be different at home and at work. Therefore, user interactions were built in to Google's ranking function, in the hope that users would obtain relevant results. The downside of this is users may be driven down a path in which there is little diversity (e.g. they will only see results that reflect their existing political or ideological views). A good example of this is provided by Tufekci (2018) searching video content using two different YouTube accounts, to find information about the 2016 US presidential election. She found that she was recommended the most extreme video content in short order (far left or far right), and that the results presented were different depending on the politics of the candidate being searched for. Algorithms that leverage user interactions can therefore push users into directions where they may not wish to go, or in fact may mislead them into taking a direction the system wants them to go in (consider clickbait, for example).

However, some researchers have questioned the impact of filter bubbles and have found that there is no real effect (Robertson *et al*, 2018), or if it exists the impacts are modest (Guess *et al*, 2018; Flaxman *et al*, 2016; Haim *et al*, 2018). Some argue that search engines reduce the capacity for the emergence of filter bubble by exposing users to diverse and opposing views (Lev-On, 2008). Robertson *et al* (2018) undertook an algorithmic audit of partisan audience bias and personalization with Google search results, and found little support for the hypothesis that personalization increases partisan bias in web search. Guess *et al*. (2018) reviewed the literature and suggested that concerns about echo chambers (another phrase for filter bubbles) is overstated. They found evidence that users prefer ideological congenial content, but weaker evidence that people avoid uncongenial content - there is some evidence in fact that users seek out alternative viewpoints (McKay *et al*, 2020). Endorsements from online friends or algorithmic rankings can influence what people consume, but effects are modest. Flaxman *et al* (2016) in an empirical study found that social media and web search engine articles were associated with higher

ideological separation than news sites, whereas Haim et al. (2018) focused on personalization in Google news and found minor effects. It is therefore easy to overstate the case, but we present examples below where those who produce information (senders) can create filter bubbles by sending information to a select group or population (section 3.6). The effects of user defined filter bubbles may be modest, but the effects can be profound (e.g. in a close election).

Why can this phenomenon occur? A good example is social media algorithms that use collaborative filtering (CF) methods (Belkin and Croft, 1992) to adjust posts provided to users, reflecting the interests of their social network. Non-transparent filters are applied to the user's information feed reflecting the narrow interests of their network. This practice can make discovering new perspectives, ideas and facts more difficult – given the caveat from research discussed above (Robertson *et al*, 2018; Guess *et al*, 2018; Flaxman *et al*, 2016; Haim *et al*, 2018). It should be remembered that 'needs' are not the same as 'wants'. Contextual integrity can easily be violated as user models for CF are enriched with data from other users (Toch *et al*, 2012).

3.4 Document interactions and data

Just as there are several ethical information communication issues associated with search result interactions, there are also issues with interactions with documents once the user has obtained them. Users will often make judgements on information seen by 'liking' it (in Facebook, Twitter and YouTube), 'disliking' it (in YouTube) or providing a rating with some comment to justify that rating (IMDb and Amazon). Content-based Filtering or CBF (Ricci *et al*, 2011) has a similar effect to collaborative filtering (CF) methods when implemented in recommendation algorithms. CBF analyzes the descriptions or content of items previously rated, liked or shared by the user and filters posts according to this interaction data. More specifically, CBF builds a user model or profile that represents the user's long-term interests. Filtering is achieved by limiting the recommendation to what matches the user profile (Lops et al, 2011), diminishing information diversity and violating contextual integrity through the use of other users data (as with CF).

There are also significant privacy issues associated with document interaction data. Tufekci (2014a) points to evidence which shows that many personal attributes can be inferred from 'likes' made on Facebook (Kosinski, 2013), with high accuracy for predicting party affiliation (85%), sexuality (88%) and race (95%) recorded. This was from a cohort of 58k volunteers. These figures, based on a simple activity such as 'liking', are particularly striking. A further example is the Netflix prize offered as part of a TREC style competition to test collaborative filtering algorithms for films or movies (Bennet and Lanning, 2007). The data set related contained 100 million 'anonymous' movie ratings on 18k movies from 480k subscribers to be used in the challenge. Narayanan and Shmatikov (2006) easily broke the user's anonymity by using openly accessible IMDb ratings to identify individual raters by matching records to the Netflix dataset. This allowed the researchers to identify sensitive personal information about users, using de-anonymization algorithms (Narayanan and Shmatikov, 2006). This highlights that even partial de-anonymization can be problematic. As with the AOL log scandal (Barbaro, *et al*, 2006) it is clear that even the most rudimentary information about how users interaction with documents could be used to identify them, and contextual integrity can be violated in the same manner.

3.5 Ethical issues arising from data use/misuse

The above examples illustrate that data that contains query terms, clicks on results lists and relevance assessments can be used unethically to violate users' privacy. This data allows global information systems to build an infrastructure of 'dataveillance' on their users (Zimmer, 2008a; 2008b). The deep

learning revolution (Pouyanfar, 2019) has provided much more effective and efficient ways of analyzing large datasets to find trends or identify individuals, enhancing 'dataveillance' capabilities (Zimmer, 2008b). Tufekci (2014a) points to this development as well as other developments in other disciplines (e.g. behavioral science) that give interested parties the ability to unduly influence users to suit their own ends. We provide some specific examples to illustrate this point.

Tufekci (2015) shows how harms can come about either through the Gatekeeper effect (who sees what and why), or by providing too much control to the algorithm (echoing Werner's (1954) warning). Two examples of manipulation of social networks are used to illustrate this point. Using data from 689K Facebook users, Kramer *et al* (2014) demonstrated that it was possible to manipulate users' emotions by altering the sentiment of content they viewed (either positive or negative), and that reducing in one or other of those emotions had a material effect. For example by reducing the number of positive posts users *viewed*, users tended to *make* fewer positive posts on the platform. The same was the case with negative posts. While even in an experimental context manipulating emotions is ethically questionable, the editor of the proceedings where the paper was published explained the reasons for doing so (Verma, 2014). The rationale given was that all Facebook users agreed to the Data Use policy when they signed up to the platform (which would allow researchers to view private posts with permission of Facebook), and this was not covered by the 'informed consent' requirements of most research as set either by University ethics/review panels, research funding bodies or publishers (Zimmer, 2010b). Use of such datasets has been severely criticized (Zimmer, 2010a; Zimmer and Proferes, 2014) and has lead to withdrawal of datasets (Lewis *et al*, 2008) due to privacy violations (Zimmer, 2010a).

A further example given by Tufekci (2015) citing an experiment with 61 million Facebook users (Bond et al, 2012), where targeted political messages for a given election resulted in a material change in users' information seeking and political views and acts (e.g. voting patterns). The messages imparted by the researchers were amplified by the network effect i.e. users connected to the 61 million experimental cohort also received the same message, with the same impact. This effect is similar to the filter bubble problem explained above. Releasing this kind of research is very problematic, but the publications do highlight the considerable problems that need to be addressed.

User are not always aware of the consequences of online behaviors on their privacy, but given the right context they can be given information on how to alter their behavior to meet their needs. (Acquisti et al, 2015). However this is a complex issue as there is evidence of a control paradox in privacy (Brandimarte et al, 2013; Kokolakis, 2017). Giving users more control over data privacy can lead to situations where users provide more information about themselves. Risks of data sharing must be made clear to the user (Brandimarte et al, 2013) and the level of control over sharing needs to be such that maximal control is achieved (Paisley and Parker, 1965) limiting potential harm whilst adhering to contextual integrity principles.

3.6 Real world examples of information-related ethical issues

There have been many examples of real world issues that have arisen due to the issues identified above. We provide two key examples here – the United Kingdom Brexit referendum (Shipman, 2016) and the Cambridge Analytica scandal (Isaak and Hanna, 2018). Shipman (2016) provides a detailed analysis on the use of social media and search engines by both sides of the Brexit referendum (pp.407-425). One leave campaign used social media 'likes' to locate geographical areas where sending their 'leading light' to best effect (locations that would more likely vote for their side). Another campaign used the 'Waterloo Strategy', in which 450 different types of adverts (Facebook posts, videos etc.) were tested

to see which was the most effective. The most effective ads were then used in the last four weeks in the run up to the referendum. A third (opposing) campaign was hampered by lack of social media data to target their message at users who were sympathetic to the campaign viewpoint (one side of the debate were more vocal about their views on the subject historically). The Cambridge Analytica scandal (Isaak and Hanna, 2018) is a particularly prominent case of the misuse of social media data. This came about through the use of a psychological test designed and built by an academic researcher, allowing Cambridge Analytica to gather personality data about the respondents and their entire social network on Facebook. This data was used to build up a picture of the electorate for the 2016 US presidential election. Analysis of a significant dataset (said to be 230 million adults) allowed the company to target particular messages to those people who might be persuaded to vote for a particular side (rather than abstain), or to change sides. Other data such as click-throughs were also collected to find out users' viewpoints, and merged to create a more accurate picture for message targeting – where information these 'persuadable' users would likely be susceptible to was presented to them. As Belkin and Robertson (1976a) warned, such information aimed at persuasion *"could be used equally well by someone designing a propaganda-campaign as by an information scientist concerned with how to find the information relevant to a particular request."* For example Social Media and the Web are now rife with 'propaganda campaigns' and misinformation.

The evidence presented here demonstrates that the concerns of both Belkin and Robertson (1976a) and Wiener (1954) were very much justified and that information science research has been misused; the ideas generated have been used in ways that are not desirable. While addressing these concerns now may be akin to 'closing the stable door after the horse has bolted', it is imperative that the information science and information systems communities face up to their ethical responsibilities. We propose some design suggestions for addressing these concerns in sections 5 and 6. Before that, however, we discuss some key principles of ethics in information systems.

4 Information Science, systems and ethics

Belkin and Robertson (1976a) state that *"influencing peoples' images without their consent and knowledge is unethical, if not immoral."* The examples in the previous section clearly demonstrate that unethical practices abound and immoral behavior on data use is widespread. Ethics and morality in information science has been recognized as important (Kostrewski and Oppenheim, 1979; Capurro, 1985; Adam, 1991; Himma and Tavani, 2008; Stanford, 2016) ever since Belkin and Robertson (1976a) expressed their concerns. We now analyze the impacts illustrated above specifically using examples of the ill effects of sender-orientated information systems. We focus on three main principles from this literature that apply to our information systems context.

Principle of confidentiality (Capurro, 1985): The system should keep user enquiries confidential (Kostrewski and Oppenheim, 1979). This includes all the data about their searches from search keywords, query modifications and results inspected (Capurro, 1985). This principle addresses potential ethical issues related to the users queries and data generated during search sessions. The principle may apply to activities such as 'liking/disliking', rating and re-tweeting etc. depending on the context. Service providers should record accurate information about their users and should be obliged to provide this any data to them on request (Verma, 2014). Services such as Google do comply with this sub-principle. However, given the evidence from the AOL log scandal (Barbaro *et al*, 2006)) and the Netflix prize (Ricci *et al*, 2011), it is clear that this principle is all too easy to break, even if attempts have been made to anonymize the datasets. It is good practice to ask for users' consent in an easy, accessible way (e.g. avoiding legal jargon) before using their data for a particular purpose. There are plenty of examples where

this has not happened. For example, in Facebook research (Kosinski *et al*, 2013; Bond *et al*, 2012), consent has been inferred the from platforms data use policy. The authors hold the view that this is not sufficient, and it is unethical to use data without the users explicit and informed consent to any given study (Zimmer, 2010a; 2010b). Study participants should have the right to ask researchers to remove their data from any study if they do not wish their personal data to be used for the purposes outlined.

Principle of accessibility (Capurro, 1985): users should not be discriminated against on the basis of their individual attributes. This principle relates to activity on individual items or documents. Information relevant to two more users should be presented to all those users without fear or favor – the information broker problem (Kostrewski and Oppenheim, 1979). Examples of this are provided above from the Brexit referendum (Shipman, 2016) and the Cambridge Analytica scandal (Isaak and Hanna, 2018). This principle attempts to address the filter bubble problem where, for example, targeted political messages to a given set of users but not to others. Users should not be prevented from being able to inspect all items and make their judgement upon them, irrespective of their political leanings.

Principle of completeness (Capurro, 1985): The system should not present a biased set of results to users (Kostrewski and Oppenheim, 1979). Information flow to a given user group should not be distorted or interrupted, thereby discriminating against them. This means that information should not be presented in a way that implies completeness or impartiality, but where it is actually biased towards the system designer or service provider's interests. This principle also relates to the presentation of information to the user, as completeness requires new ways of conceptualizing personalization, beyond selective filtering. Evidence from search engine research demonstrates how easily this principle can be broken (Jansen *et al*, 1998; Silverstein *et al*, 1999). For example, on the Web it has long been recognized that there is bias inherent in web content either through an incomplete or out of date index and reliance on links between pages (Lawrence and Giles, 1998) as well as through web use (Baeza-Yates, 2018). Users should know that the search results provided by the system are meant to resolve their information needs, rather than serve the interests of the service providers or other third parties. Transparency should be a guiding principle for information systems, not just web search engines (Welp and Machill, 2005) to encourage oversight and accountability (Hinman, 2005) shifting power back to the user (Rieder, 2005).

The question is: how do we return to these principles as best we can? That is, how do we return 'control' of the system and the information presented to the user, where at all possible (Paisley and Parker, 1965)? While we cannot address all the ethical issues raised in this paper, we do make suggestions for how the information systems community might begin to address several of these issues through systems design and implementation. Therefore, in the rest of this paper we discuss technological solutions. We discuss algorithmic, policy and architectural solutions in section 5, followed by recommendations for systems design and implementation in section 6.

5 Algorithmic, Policy and Architectural Solutions

So far, we have discussed ethical issues to do with the use (or misuse) of user interaction data in various information systems. In this section and the next, we propose some potential solutions to problems identified, while fully recognizing that these are complex issues where there is no single 'silver bullet' solution; a combination of social, technical and educational approaches and sustained research into reducing online information-related harms is likely necessary. In this light we discuss context-aware algorithmic solutions (section 5.1) together with privacy by architecture (5.2) and privacy by policy solutions (5.3) derived by (Toch *et al*, 2012).

5.1 Context and Information Systems

While an awareness of the user's context can potentially create 'filter bubbles,' through over-personalization, it also has the potential to burst them – by providing a balance, or diversity of content. For example, context has long been thought to bring potential benefits to searchers (Ingwersen, 1992). Goker et al. (2009) outline different types of context, a key one being the user context that can be represented by various factors including the environment, personal interests, tasks undertaken, social connections or place and time. Any or all of these factors can be used in information systems to personalize or offer potential ways for users to customize the information they see. How can we use the benefits of context, ameliorating the potential ill effects of privacy violations and filter bubbles? We recognize a tension here, but if we start a discussion along the lines of empowering users to leverage their own context, rather than allowing the system to personalize (effectively filter) based on context, we may be able to address this tension to the benefit of users. In particular we can foster contextual integrity, encouraging the use of data as and when necessary but not otherwise (Nissenbaum, 1998; Nissenbaum, 2004; Zimmer, 2007; Zimmer, 2008c).

A general approach is to consider *context-aware* technological solutions (Tamine-Lechani, 2008) together with the issue of who *controls* the system and the data held by it (we argue that it should be the recipient). Currently, advances in technology allow to capture the user's context easily and effectively to effect behavioral, social and location based personalization (Toch *et al*, 2012) e.g. search on mobile devices where users' temporal/geographical contexts can be gathered (Mountain and MacFarlane, 2007). The importance of context in information systems has been recognized given the availability of multiple contextual factors (Goker *at al*, 2009). These factors may affect the user's experience positively as well as negatively. Baltrunas et al. (2011) studied the effect of contextual factors on recommendation effectiveness at different granularities. Their findings revealed that when a contextual factor or attribute has no influence on the user's preferences, it becomes 'noise'. But what does 'noise' mean in the context of applications such as recommendation or search? Usually we refer to any results that do not match the user's profile (predefined preferences and interests) as noise. Any results that do not enhance the system relevance will be considered to be noise and will be filtered out. However, this limits novelty and serendipity (Shani and Gunawardana, 2011) in the system's results. Hence, in response to the filter bubbles issue, exploiting the knowledge of the contextual situation the user finds themselves in can enhance information diversity and expand the user's choices – allowing them to decide whether to stay within their existing knowledge boundaries, or expand those boundaries by following-up on encountered information. Removing reliance on content (the content based filtering problem outlined in section 3.4 above) and a subset of context factors and attributes is key.

Combining context-awareness with providing user *control* over the system may be key to addressing ethical issues related to information misuse. With current algorithmic opacity, we exist in a world in which algorithms presents users with what it estimates is wanted, but not necessarily what the user needs to see. The user has no control on the selection criteria and cannot see removed items (however there may be valid reasons to remove content which is dangerous or libelous etc.). Control will enable the personalization process to be more verifiable and balanced, providing explanations on decisions made by the system in presenting information to the user (or message recipient). If filtering is employed, a key principle might be to allow the option for users to view what information has been filtered-out – e.g. search results related to places that are not near the user's current location when they are searching for somewhere to eat, papers from non-computing disciplines when searching for a particular computing topic etc. Providing new forms of transparency in information systems therefore has the potential to

provide greater user control. We now examine how privacy by architecture and policy can also provide greater user control.

5.2 Privacy by Architecture Solutions

Shen et al. (2007) discuss various privacy strategies and recommend an architecture to use when considering implementing systems to ensure user privacy. They identify two elements for consideration when reviewing privacy: the user's identity and their information need (e.g. query) - to which we can add related data on results lists and document interaction. Four levels of privacy protection are identified Shen *et al*. (2007) together with their associated risks (Toch *et al*, 2012):

1. *Pseudo Identity* – the user is given a pseudo identity and user data is aggregated by the system. This has proved to be a poor method of preserving user privacy (see above).
2. *Group Identity* – users are given a group identity and user data is aggregated by the system. This has the potential to create filter bubbles if not handled carefully, as the system might assume an individual user shares the interests of the group.
3. *No Identity* – the user's identity is not available to the system, but some information about user interactions are recorded (e.g. query/session logs). This reduces the system's ability to provide personalized results, but ranking can be improved by reviewing log data. Recall however that even the most rudimentary user data can be used to violate users privacy (see section 3.4 above).
4. *No Personal Information* – No information about the user is available to the system. User interaction data is not stored. User profiles to provide better information to users cannot therefore be created, but is a low risk solution.

There is clearly a tension between each of these levels in terms of privacy vs. benefits provided by using context. The tension can partly be dealt with through careful, contemplative systems design. But no matter what privacy, identity and personalization-related decisions are made, ultimately the user should be able to make an informed choice by providing cues to weighing up the benefits of providing data as against protecting their privacy (Acquisti et al, 2015). The key issue is to distinguish personal publication information (PPI) from nonpublic personal information (NPI) to protect some aspects of personal information (Tavani, 2005). Shen et al. (2007) recommend four different architectures as a start for addressing this tension, which we review in the light of the issue of control:

a) No personalization – complete user control.
b) Service-side personalization – less user control (Toch *et al*, 2012).
c) Client-side personalization – more user control (Toch *et al*, 2012).
d) Client-server collaborative personalization – control negotiation.

We ignore a) as we assert the benefits of using context in search and argue for the approach in d) in section 6, incorporating some aspects from b) and c) Users should be able to determine which of the levels is appropriate for their particular needs by providing them with clear, comprehensive and dynamic control over how information is personalized – allowing them to control their personalization choices at will, rather than having to make blanket choices to cover all personalization situations. In particular users must be able to control access to nonpublic personal information (NPI) attempting to address the problem of privacy in public that is highlighted by Nissenbaum (1998; 2004) and address the issue of contextual integrity through negotiation of control.

5.3 Privacy by Policy Solutions

Toch *et al* (2012) provides a framework by for deriving privacy by policy solutions. These can be stand alone or mixed with privacy by architecture solutions. The key issue is establishing user control through transparency that can be achieved through interpretability and explainability built into information systems. This will encourage trust and highlight issues of contextual integrity. One simple and clear way to do this it to provide privacy controls that are interpretable to the user (Toch *et al*, 2012). Interpretability can also be achieved through the development of scrutable user models that are pervasive (Kay, 2006) and under the control of the user. Contextual integrity can be encouraged by the use of selective personas that differ across applications e.g. one for twitter one for Facebook (Kay et al, 2003). Privacy controls and user models can be used to tailor privacy constraints dynamically, further enhancing contextual integrity (Wang et al, 2007). Finally, simple 'Do not Track' schemes can be adhered to by ensuring users have control over who records their interactions (May and Narayanan, 2011).

6 Recommendations for system design and implementation

In this section we present several system design and implementation ideas and strategies. The focus here is to affect the design of systems to address the ill effects highlighted above as suggested by Zimmer (2008a). All are user-focused and attempt to give them more control over the software or services they use. Server side strategies are presented in section 6.1 (focusing on ethical implementation of systems from the sender perspective) and client side strategies (focusing on ethical implementation of systems from the recipient perspective) are presented in section 6.2. We address the principles outlined in section 4 and directly apply these principles using the privacy solutions from section 5, highlighting limitations. This to encourage the 'baking in' of contextual integrity into systems design and development (Nissenbaum, 1998; Nissenbaum, 2004), moving away from commercial focused view that limits privacy (Nissenbaum, 2011). This is to address different variants of bias (Friedman and Nissenbaum, 1996) such as preexisting, technical and emergent bias.

6.1 Server side user-focused strategies

It is at the server side that the principle of completeness (Capurro, 1985) should be adhered to. This is done for example by ensuring diversity of results when a response to queries are processed and presented to the user. This can reduce the filter bubble effect and mitigate the consequences of the ill effects discussed in section 3. There are various bias types (Baeza-Yates, 2018) that need to be addressed for the principle of completeness. It is still an open question as to how can we reduce the ill effects of bias, whilst still maintaining the positive aspects of biasing results that benefit the user (Lev-On, 2008) by promoting fairness (Lewandowski, 2017). We address issues such as preexisting bias and technical bias (Friedman and Nissenbaum, 1996) that emerge from the social sphere and systems design issues respectively.

Data/Content bias: It is well known that content itself can introduce bias due to many factors including: age, economic status, gender, age, language etc. Any algorithm deployed should not rely on either a subset or single attribute or factor of the content in the creation of results for the user. Content can be used, but should not be relied on. An example of good practice is the way web search engines deal with search engine optimization (SEO) by content producers (Weideman, 2009). Users should be encouraged to follow good SEO guidelines (Weideman, 2009) such as writing content that accurately reflects the websites purpose, and system designers should consider schemes to prevent spamming (Spirin and Han, 2012). The user should access the data is that is available to them, in aggregate form.

Sampling bias: data/content bias is compounded by sampling bias. This occurs when a non-representative sample is used to inform the algorithms (and in the case of machine learning algorithms, train them). An example of this is potential bias against a particular cohort given their language norms and training naively e.g. African-Americans who use language about themselves that would not be acceptable if used by other groups (Davidson et al, 2019), leading to discrimination against those the system is designed to protect. Systems designers should not rely on a single sampling strategy, but try several in order to reduce this bias. Typically session data can be used to enhance effectiveness e.g. in searching (Goker and He, 2013), and these advantages should not be lost by any strategy implemented. If possible, the user should be allowed to view different samples used to train the system in aggregate form via user focused explanations. Relying on single sources should be avoided e.g. with social media focusing on one platform such as Twitter (Tufekci, 2014b)

Algorithmic bias: relying on a single algorithm can also produce bias. Systems designers should consider different algorithms and fusing them together. For example, using hill-climbers as well as neural networks. However, it is well known that some standalone algorithms and methods do bring benefits to the user e.g. BM25 (Robertson et al, 1995). In most cases providing information on how the algorithms work to the user might not be worthwhile, but explanations on why particular results are returned could be useful.

Activity bias: Zipf's law and its effect has been known for many years (Zipf, 1949) e.g. some users engage a lot with the system, but many actually do very little. Reliance on certain activities, such as reviews in Amazon or Netflix, or posts on Facebook will bias results to the most active users. This kind of effect was seen in the Brexit referendum (Shipman, 2016). Any system should not over rely on this content for results presentation. User session data must be used with care. A particular danger is click-spam or click-farms (Dave *et al*, 2013), used to alter rankings if items inspected statistics are used in the function. Again, web search engines guard against this, and there is good practice available for the system designer to follow (Blizard, 2012). Aggregate data on activity held in the system and its influence at the system level must be made available to the user.

Considering these forms of bias when designing may prevent either the system or third parties forcing users into filter bubbles, but the system must also take steps to ensure that users themselves do not drift or move into a filter bubble of their own accord. We recognize that there is a tension between allowing the user control over the system and the potential to create filter bubbles, and there is no easy solution to this. However, providing users with appropriate control over their data held on a server will allow them to make their own judgement as to whether this tension has been resolved and adhere to contextual integrity. As Ingwersen (1992) stated, the user must be treated as the most intelligent part of the system.

Giving users access to and control of their server data as appropriate also gives the system designer an opportunity to address the privacy issue simultaneously with the filter bubble problem. Isaak and Hanna (2018) outline several privacy principles from a policy position statement by IEEE-USA (2018). Although we have already begun to make a case for transparency and control, we revisit these principles in a user data context. We also discuss the principles of disclosure and notification in relation to user data.

Transparency: The type of data held about users and nature of data use must be made fully clear e.g., for a profile, what data is stored, how this profile data is used by the system and what data from this profile is shared with third parties. Profiles hold sensitive data such as personal preferences, date of birth, addresses as well as interaction with the system such as likes and dislikes. Any profile data held by third parties must also be made available to the user on request. In certain jurisdictions, legislation mandates this e.g. GDPR in the European Union (2016). Given the legislative environment, all methods used to

develop the user profile, such as tracking user interactions with results lists and documents, should be made transparent to the user, thereby promoting trust (Schultheiß and Lewandowski, 2021). It is only by learning what types of data an organization holds about them that users will understand the nature and scope of their data use and get to know the possibilities for making more specific data access requests. A particular issue with many social media sites is that anonymous or pseudonymous postings are the norm (Tufekci, 2014a). In cases where such information is used to build profiles, the user should be aware of the nature of another user's identity status to give them the ability to act accordingly. This of course does not extend to knowing who that other user is, thereby violating their privacy. The issue of anonymity is a difficult one to solve (Nissenbaum, 1999), and requires careful thought to generate appropriate solutions.

Disclosure: Users should be able to find out what information about them is stored on the system or shared with third parties. For example, any profile information about the user and their interests should be fully accessible to the user, together with any information used to build that profile e.g. interactions such as 'likes' etc. There is some good practice available e.g., users can download and view the information held on them on Google services (2020) and (albeit to a limited extent) correct inaccuracies. If third parties are given this profile information, the manner of its disclosure, including content, rationale and date/time data was shared should be made available.

Notification: Any data breaches must be notified promptly to the user. Legislation in the EU requires services to notify the user of any breaches of data confidentiality and often mandates severe penalties for lost or stolen data. The user must be told about any breach of confidentiality of any data held about them, and the extent of the breach (i.e. the likely data affected – e.g. identity details, contact details, encrypted or non-encrypted passwords etc.). Where profile information is used by the system, or third parties for marketing and/or advertising purposes, users should be informed who used this data and the purpose it was used for.

Control: Users must have full control of any profile data held at the server. This includes the deletion or partial deletion of data held about them. If this means the profile becomes difficult for the system to use, then it must not warn the user of the potential negative consequences of such actions – the profile cannot be used.

In summary, the system should explain what user data is stored and for what purpose and whom it is shared with and why (including when data confidentiality is breached). We turn to the client side next.

6.2 Client side user-focused strategies

While much can be done on the server side to prevent and mitigate for data misuse, the Website or application should also be designed to provide users with control. It is at the client side we can communicate the sender's intent (e.g. by providing explanations to the user of why the message was provided and the systems rationale for providing it) and allow users to provide their consent for data sharing. In this section, we discuss two principles from (Capurro, 1985) - accessibility and confidentiality and their potential to provide users with useful control over their data to address emergent bias (Friedman and Nissenbaum, 1996), that arises in user interaction contexts. We also address the issue of access to and setting of appropriate permissions to content and data (Boyd, 2008), as addressed in section 5 above.

6.2.1 Principle of accessibility.

Where possible and feasible, user profile data should be held at the client rather than the server. The application or software should not use this profile data to prevent access to or manipulate information seen by the user. User centered bias identified in user interaction (Baeza-Yates, 2018) can be used to guide the designer. These can emanate from data and algorithmic bias noted on the server side above, or self-selection bias from user activity.

Data and Algorithmic bias: It is important to pay attention to the way the documents are ranked and presented to the user. Any factors or attributes related to the user and used only at the client via context aware applications should not rely on a subset of factors. Where social factors are used, users must be made aware of when filtering has taken place (to alert them of a potential move into a 'filter bubble') or to provide users with an indication that information outside the filter is available (McKay *et al*, 2020). Individual results must be presented fairly and equally (e.g., particular results should not be emphasized or highlighted using different font and/or size, although we realize there is an advertising tension here). One way to do this is to provide explanations of URLs in retrieved results, that may provide information on the reliability of that source e.g. .org and .gov for medical information (Zimmerman et al, 2020).

Bozdag and van den Hoven (2015) survey a number of user interface design methods to address data and algorithmic bias based on a number of real-world applications and research. Munson and Resnick (2010) present ideas on how to encourage users to engage more widely with information than their own political viewpoint by presenting diverse political views to the user (liberal vs. conservative). They found diversity-seeking and challenge-averse users, the latter being more difficult to encourage. One way of encouraging users to examine different views is by presenting a visualization illustrating the effects of personalization on the information they can see (e.g. what information is shown to or prioritized for them and not other users). Another way might be to present two different sets of results (e.g. personalized for different viewpoints) side-by-side, to encourage the user to make up their own mind on the issue at hand (e.g. Parlia: http://www.parlia.com/). This method could also be used generally, showing personalized vs. non-personalized results. Xing et al. (2014) extend this idea further by showing results *not* found on Google searches in different conditions (e.g. when in a particular geographical location). Allowing the user to 'simulate' results by making personalization choices based on various different factors can allow them to see the impact of their searches in different contexts (and the effects of any filtering).

Other more complex visualizations can also be used. Nagulendra and Vassileva (2014) provide a view of who or what is in their filter bubble (any attribute or factor can be considered) and allows users to remove or add any attributes such as 'friends' in order to give users an opportunity to break out of their filter bubbles by viewing those they are currently in.

Kriplean *et al* (2012) and Freelon *et al* (2012) designed and built and interface that showed a comparison between a user's view on a subject and other views on the same subject. Users could manipulate a horizontal slider to indicate their views on an issue, encouraging them to list pros and cons of the argument. Results lists from different viewpoints can be laid side by side, and there are UI designs that could be used to alter these results lists given the interaction with the slide bar or evidence from the user's pros and cons. The design concept behind this is 'nudging', where users are encouraged to look at other perspectives (Kriplean *et al*, 2011). This concept needs to be used transparently rather than manipulatively (Susser *at al*, 2019a;2019b). Slide bars on various attributes or factors can be used as suggested by Faridani *et al* (2010) e.g., results lists, or a representation of results in a visualization can be changed by users through interaction with similar 'sliders,' to see what different information they are exposed to when they slide the bar. This could help the 'support, not persuade' design recommendation from a study on supporting the change if views in information interaction (McKay et al, 2020).

One way to encourage nudging is to support information literate actions by designing information systems that support metacognition: allowing users to reflect on their own cognitive skills, thereby supporting critical thinking, creativity and learning (Kriplean *et at,* 2012). Smith and Rieh (2019) suggest this can be achieved by showing both bibliographic and inferential knowledge-context results. This has the advantage, once again, of handing control of the system to the user and potentially avoiding problems with manipulation or misuse. Getting users' to think about their actual needs rather than their wants is good practice.

Self-Selection bias: User interactions (or lack of them) can cause bias (Baeza-Yates, 2018) e.g. clicks/selections of results, mouse movements, eye movements, scrolling and panning activity etc. An example of this is users tending to choose documents that accord with their beliefs (Baeza-Yates, 2018). As noted above, user activity varies widely. Any personalization model that uses this evidence (on the assumption this information is held at the client only) should be used with care i.e. any context-aware application should avoid learning on a subset of attributes for factors.

Note that activity bias noted above could have an effect on the impact of any design decisions made at the interface i.e. users may or may not take advantage of the interface functions to the most useful effect. The potential for bias interaction is significant, whereby the effects of each individual bias examined above is exacerbated in an implemented system where all bias is present, creating a 'vicious cycle of bias' (Baeza-Yates, 2018). The issue is even more complex when cognitive bias are considered (Azzopardi, 2021). While there are no simple solutions to preventing bias, providing greater control and more information to the user encouraging meta-cognition thereby identifying bias could be the way forward (Smith and Rieh, 2019).

6.2.2 Principle of confidentiality

The principle of confidentiality can be achieved by considering both design and implementation decisions for the interface. Many of the design decisions mentioned above can also address confidentiality issues, as can the concept of nudging. Zimmerman et al. (2019) provide ideas on nudging by re-ranking, filtering and providing visual cues. The privacy principles outlined by Isaak and Hanna (2018) can also be used to guide design and implementation decisions. We end this section by discussing how confidentiality can be achieved through user control and notification, and system transparency as highlighted in section 5.

Control: User requests to stop tracking them must be adhered to. The user should be provided with control unless there are compelling reasons not to. Attempts by third parties to obtain user data must be stopped by locking down the client e.g. clicking on results should not lead to transfer of data i.e. to prevent the kind of third-party access issues outlined in section 3.3. This is to ensure contextual integrity. Users must be able to delete cookie and session data from their client, along with any results, document or query data held on the client application. Where gesture of assent techniques are used by the system or third parties, information to fulfill a knowledge gap should be meet irrespective of users agreement to the conditions set down. Privacy polices should be clearly stated in a language that the user can understand (Tsai *et al*, 2011).

Notification: Users must be informed of any requests to access the data residing on the client and must be asked to agree to any tracking (e.g. assent to cookies placed on a browser). They should be told what data will be stored, by whom and how it will be used. They should also be provided with easy and accessible ways of viewing and deleting it. Attempts to share user data with third parties must be notified to the user (giving them control – see above). Where possible, details of the source and the rationale for the request should be notified to the user to promote contextual integrity.

Transparency: Where data and/or applications are placed on the user's client, they should be made aware of such events (by notification – see above). Users should be aware of any data collection mechanisms applied to the data on their client.

General implementation considerations should include isolating applications where possible to ensure data does not drift between them, thereby violating privacy through the back door. Simple security mechanisms should be adhered to (i.e. using https to secure communication in web applications rather than http).

7 Conclusion

We argue for a rebalancing of control in information systems; away from the system (the intermediary, the information system or related technology) and towards the user (recipient). The ideas first put forward by Paisley and Parker (1965) about receiver controlled communication systems need to be considered again in the light of recent events. The sender should not have control over the system; even in the case of personalized ads for example (where the sender is a key stakeholder, as they likely fund the ad), users should be given the agency to make meaningful, comprehensive choices about their targeting preferences. Current attempts by Web and social media giants to provide greater control (e.g. enhanced privacy controls) are laudable, but do not even begin to provide the full and unrestricted level of control that may be needed to re-gain users' trust (Nissenbaum, 2001) in these turbulent times of over-tracking, hyper-personalization, data breaches and misinformation. The related principle of transparency is also important; opacity in how systems work and, in particular, how and why certain information is presented can facilitate information misuse by providing user focused explanations. Conversely, transparency, particularly about why a user is seeing particular information can potentially help bridge the gulf between sender and recipient-oriented systems design. The introduction of technologies such as intelligent personal assistants (IPAs) and privacy concerns around them (Liao *et al,* 2019) only enhances an argument that returns control to the recipient.

We need to develop context-aware socio-technical systems (Fischer and Herrman, 2011) that return novel and unique results whilst adhering to the principles of contextual integrity. The results could be uncomfortable, challenging or opposite to the user's point of view. The Context-aware socio-technical systems should have awareness of the user's knowledge background, task and context. Moreover, through interactivity these systems should enable the user to obtain control over the information system. The recommendations we make for systems design in section 6 provide ideas for the community to think about. Both researchers interested in solving the problem and application designers faced with the real world problems outlined in section 3 need to consider these uses. Designers should also try to retain the benefits of technology as stated by Wiener (1954). A general approach is the move to explainable information systems, which is currently gaining traction in the search domain (Zhang *et al*, 2019). Research into de-personalization, filter bubbles and diversification in the context of search (Clarke *et al*, 2008; Bierig *et al*, 2019) and recommendation (Vrijenhoek *et al,* 2021) is also gaining attention in the field, with methods to address bias being developed (Yalcin and Bilge, 2021). Specific methods such as ensuring gender balance in music recommenders are emerging (Ferraro *et al*, 2021). We hope this paper starts a conversation about how best to prevent and mitigate information misuse by bringing as much control as possible back to the user (Paisley and Parker, 1965) – thereby helping to make information systems truly human-centered. We need to reach out to other disciplines such as sociology, psychology, government and politics with our ideas to address what has become a significant societal problem in misuse and misinformation avoiding piecemeal solutions (Bruns, 2018). By addressing this issue there is more chance that the idea of a receiver controlled information system first proposed by Paisley and

Parker (1965) can be achieved, recognizing that there are significant barriers to actually implementing any ideas to achieve such an ethos in practice. We hope that this starts a conversation that will allow the development of methods leading to more equitable access to information (DiMaggio, P. and Hargittai , 2001; Lievrouw and Farb, 2003). To paraphrase Holmes (1974) we “have a duty to see that beneficial uses of the computer are fostered as much a duty to see that detrimental uses are avoided”

REFERENCES

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and Human Behavior in the Age of Information. *Science*, Vol, 347 No. 6221. pp.509-514.

Adam, R. (1991). Laws for the lawless: ethics in (information) science. *Journal of information science*. Vol. 17 No. 6. pp.357-372.

Anderson, N. (2006). The ethics of using AOL search data. *Ars Technica*, August 23. https://arstechnica.com/uncategorized/2006/08/7578/

Azzopardi, L. (2021). Cognitive biases in search: a review and reflection of cognitive biases in Information Retrieval. In Elsweiler, D., Joho, H. Kando, N. & Smith, C. (Eds.) *Proceedings of the 2021 Conference on Human Information Interaction and Retrieval (CHIIR 2021)*, pp. 27-37.

Baeza-Yates, R. (2018). Bias on the web. *Communications of the ACM*. Vol. 61 No. 6. pp.54-61.

Baltrunas, L., Ludwig, B. and Ricci, F. (2011). Matrix factorization techniques for context aware recommendation. In Jannach, D. and Admavicius, G. (Ed.s), RecSys’11: *Proceedings of the fifth ACM conference on Recommender systems.* pp. 301-304.

Barbaro, M., Zeller, T. and Hansell, S. (2006). A face is exposed for AOL searcher no. 4417749. *New York Times*, August 2006. p.8. https://www.nytimes.com/2006/08/09/technology/09aol.html

Belkin, N.J., and Robertson, S.E. (1976a). Some ethical and political implications of theoretical research in information science. In: Martin, S.K, *Proceedings of the 39th ASIS Annual Meeting*. pp.14-23.

Belkin, N.J., and Robertson, S.E. (1976b). Information Science and the phenomenon of information. *Journal of the American Society for Information Science*, Vol. 27 No. 4. pp.197-204.

Belkin, N.J. and Croft, W.B. (1992). Information filtering and information retrieval: two sides of the same coin. *Communications of the ACM*. Vol. 35 No. 12. pp.29-38

Bennett, J. and Lanning, S. (2007). The netflix prize. In: Bennett, J. Eklan, C., Liu, B., Smyth, P. and Tikk, D. *Proceedings of KDD cup and workshop* 2007. 12 August 2007.

Bierig, R. and Caton, S., 2019. Special issue on de-personalisation, diversification, filter bubbles and search. *Information Retrieval Journal*. Vol. 22 No. 5. pp.1-3.

Blanke, T. (2005). Ethical subjectification and search engines: ethics reconsidered. *The International Review of Information Ethics*, Vol. 3, pp.33-38.

Blizard, T. and Livic, N. (2012). Click-fraud monetizing malware: A survey and case study. In Arrott, A. (Ed). *7th International Conference on Malicious and Unwanted Software*. pp. 67-72.

DiMaggio, P. & Hargittai, E. (2001). From the ‘digital divide’ to ‘digital inequality’: Studying Internet use as penetration increases. *Princeton: Center for Arts and Cultural Policy Studies, Woodrow Wilson School, Princeton University*, Vol. 4. No. 1, 4-2.

Bond, R.M., Fariss, C.J., Jones, J.J., Kramer, A.D., Marlow, C., Settle, J.E. and Fowler, J.H. (2012). A 61-million-person experiment in social influence and political mobilization. *Nature*, Vol. 489 No. 7415. pp.295.

Boyd, D. (2008). Putting privacy settings in the context of use (in Facebook and elsewhere). *Apophenia* Available on: http://www.zephoria.org/thoughts/archives/2008/10/ 22/putting_privacy.html (Accessed: 23rd June 2021).

Bozdag, E. and van den Hoven, J. (2015). Breaking the filter bubble: democracy and design. *Ethics and Information Technology*, Vol. 17 No. 4. pp.249-265.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science*, Vol. 4, No.), pp.340-347.

Bruns, A., (2018). Facebook shuts the gate after the horse has bolted, and hurts real research in the process. *Internet Policy Review*, Vol. 25. https://tinyurl.com/urxcx497 (Accessed: 23rd June 2021).

Capurro, R. (1985). Moral issues in information science. *Journal of information science*, Vol. 11 No. 3. pp.113-123.

Clarke, C.L., Kolla, M., Cormack, G.V., Vechtomova, O., Ashkan, A., Büttcher, S. & MacKinnon, I. (2008). Novelty and diversity in information retrieval evaluation. In: Myaeng, S.M., Oard, D.W. & Sebastiani, F. (Eds.), *Proceedings of the 31st annual international ACM SIGIR conference on Research and development in information retrieval (SIGIR 2008)*, pp.659-666.

Dave, V., Guha, S. and Zhang, Y. (2013). Viceroi: Catching click-spam in search ad networks. In Gligor V. and Yung, M. *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. pp. 765-776.

Davidson, T., Bhattacharya, D. and Weber, I. (2019). Racial bias in hate speech and abusive language detection datasets. In: Prabhakaran,V., Roberts, S.T., Tetreault, J. and Waseem, Z. (Eds.), *Proceedings of the Third Workshop on Abusive Language Online, Association for Computational Linguistics*, pp.25–35.

Diaz, A. (2008). Through the Google goggles: Sociopolitical bias in search engine design. In: Spink, A, and Zimmer, M (Eds.), *Web search - Multidisciplinary Perspectives,* Springer, Berlin, Heidelberg, pp. 11-34.

Epstein, R. and Robertson, R.E. (2013). Democracy at risk: Manipulating search rankings can shift voters' preferences substantially without their awareness. In *25th annual meeting of the Association for Psychological Science, Washington D.C. May 2013*.

Ferraro, A., Serra, A. & Bauer, C. (2021). Break the Loop: Gender Imbalance in Music Recommenders. In Elsweiler, D., Joho, H. Kando, N. & Smith, C. *Proceedings of the 2021 Conference on Human Information Interaction and Retrieval (CHIIR '21),* pp.249-254.

European Union. (2016). General Data Protection Regulation. https://tinyurl.com/yygvb6co

Faridani, S., Bitton, E., Ryokai, K. and Goldberg, K. (2010). Opinion space: a scalable tool for browsing online comments. In Brewster, S. and Bodker, S. (Ed.s). CHI'13: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.* pp. 1175-1184).

Fischer, G. and Herrmann, T. (2011). Socio-technical systems: a meta-design perspective. *International Journal of Sociotechnology and Knowledge Development.* Vol. 3 No. 1. pp.1-33.

Flaxman, S., Goel, S. and Rao, J.M., 2016. Filter bubbles, echo chambers, and online news consumption. *Public opinion quarterly*, Vol. 80 No. S1. pp.298-320.

Freelon, D.G., Kriplean, T., Morgan, J., Bennett, W.L. and Borning, A. (2012). Facilitating diverse political engagement with the living voters guide. *Journal of Information Technology & Politics*, Vol. 9 No. 3. pp.279-297.

Friedman, B., and Nissenbaum, H. 1996. Bias in computer systems. *ACM Transactions on Information Systems,* Vol. 14 No. 3, pp.330–347.

Goldman, E. (2008). Search engine bias and the demise of search engine utopianism. In: Spink, A, and Zimmer, M (Eds.), *Web search - Multidisciplinary Perspectives,* Springer, Berlin, Heidelberg, pp. 121-133.

Google. (2020). Manage your information. https://tinyurl.com/yx9f5vlk (Accessed: 23rd June 2021).

Goker, A., Myrhaug, H. and Bierig, R. (2009). Context and information retrieval. In Goker, A. and Davies, J. (Ed.s). *Information retrieval: Searching in the 21st century*. Wiley, London, pp.131-57.

Goker, A. and He, D. (2003). Personalization via collaboration in web retrieval systems: A context based approach. ASIST 2003: *Proceedings of the American Society for Information Science and Technology*, Vol. 40 No. 1. pp.357-365.

Guess, A., Nyhan, B., Lyons, B. and Reifler, J. (2018). Avoiding the echo chamber about echo chambers. *Knight Foundation White Paper*. https://tinyurl.com/ydfu6vby.

Haider, J., and Sundin, O. (2019). Invisible Search and Online Search Engines: The ubiquity of search in everyday life. Routledge.

Haim, M., Graefe, A. and Brosius, H.B., 2018. Burst of the filter bubble? Effects of personalization on the diversity of Google News. *Digital journalism*, Vol. 6 No. 3. pp.330-343.

Halavais, A. (2017). Search engine society. John Wiley & Sons, Hoboken, N.J.

Himma, K.E. and Tavani, H.T. eds. (2008). *The handbook of information and computer ethics*. Wiley, Hoboken, NJ.

Hinman, L.M. (2005) Esse est indicato in Google: Ethical and political issues in search engines. *The International Review of Information Ethics*, Vol. 3, pp.19-25.

Hinman, L.M. (2008). Searching ethics: The role of search engines in the construction and distribution of knowledge. In: Spink, A, and Zimmer, M. (Eds.), *Web search - Multidisciplinary Perspectives*. Springer, Berlin, Heidelberg, pp. 67-76.

Holmes, W.N. (1974). The social implications of the Australian Computer Society. *The Australian Computer Journal*, Vol. 6, No. 3, pp.124-128.

IEEE-USA. (2018). *Digital Personal Privacy, Awareness and Control*. https://ieeeusa.org/wp-content/uploads/2018/08/DigitalPrivacy0618.pdf

Ingwersen, P. (1992). *Information retrieval interaction*. Taylor Graham, London.

Ingwersen, P. and Järvelin, K. (2006). *The turn: Integration of information seeking and retrieval in context*. Springer Science & Business Media, The Netherlands.

Introna, L. D., & Nissenbaum, H. (2000a). Shaping the Web: Why the politics of search engines matters. *The Information society,* Vol. 16 No. 3, pp.169-185.

Introna, L. and Nissenbaum, H., (2000b) Defining the web: The politics of search engines. *Computer*, Vol. 33 No. 1, pp.54-62.

Isaak, J. and Hanna, M.J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*. Vol .51, No. 8. pp.56-59.

Jansen, B.J., Spink, A., Bateman, J and Saracevic, T. (1998). Real life information retrieval: a study of user queries on the Web. *SIGIR Forum. Vol.* 32 No. 1. pp.5-17.

Kay, J. (2006). Scrutable adaptation: because we can and must. In: Wade, V. Ashman, H. & Smyth, B. (Eds.).*Proceedings of the 4th International Conference on Adaptive hypermedia and adaptive web-based systems* (AH 2006), Springer-Verlag, Berlin, pp. 11–19..

Kay, J., Kummerfeld, B., Lauder, P. (2003). Managing private user models and shared personas. In: Cheverst, K, De Carolis, B. & Kruger, A. (Eds.). *Proceedings of Workshop on user modelling for ubiquitous computing, 9th international conference on user modeling (UM 2003),* pp. 1–11.

Kramer, A.D., Guillory, J.E. and Hancock, J.T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. In: Fiske, T. (Ed.). *Proceedings of the National Academy of Sciences*, Vol. 111. No. 24. pp.8788-8790.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, Vol. 64, pp.122-134.

Kosinski, M., Stillwell, D. and Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. In: Wachter, K. (Ed). *Proceedings of the National Academy of Sciences*. Vol. 110 No. 15. pp.5802-5805.

Kostrewski, B.J. and Oppenheim, C. (1979). Ethics in information science. *Journal of information science*, Vol. 1 No. 5. pp.277-283.

Kriplean, T., Toomim, M., Morgan, J.T., Borning, A. and Ko, A.J. (2011). REFLECT: Supporting active listening and grounding on the Web through restatement. In Bardram, J. and Ducheneaut, N. (Eds.). CSCW'11: *Proceedings of the Conference on Computer Supported Cooperative Work, Hangzhou, China*.

Kriplean, T., Morgan, J., Freelon, D., Borning, A. and Bennett, L. (2012). Supporting reflective public thought with considerit. In Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work. pp.265-274.

Lawrence, S. and Giles, C.L. (1998). Searching the world wide web. *Science*, Vol. 280 No. 536., pp.98-100.

Lewandowski, D. (2017). Is Google Responsible for Providing Fair and Unbiased Results? In M. Taddeo & L. Floridi (Eds.), *The Responsibilities of Online Service Providers*, Springer International Publishing, N.Y., pp. 61-77.

Lewandowski, D. and Sünkler, S. (2019). What does Google recommend when you want to compare insurance offerings? *Aslib Journal of Information Management*, Vol. 71 No 3, pp.310–324.

Lewis, K., Kaufman, J., Gonzalez, M., Wimmer, A., & Christakis, N. (2008). Tastes, Ties, and time: A new social network dataset using Facebook. com. *Social Networks*, Vol. 30 No 4, pp.330–342.

Lev-On, A. (2008). The democratizing effects of search engine use: On chance exposures and organizational hubs. In: Spink, A, and Zimmer, M (Eds.). *Web search - Multidisciplinary Perspectives*. Springer, Berlin, Heidelberg, pp. 135-149.

Libert, T. (2015). Privacy implications of health information seeking on the Web. *Communications of the ACM*. Vol. 58 No. pp.68-77.

Lievrouw, L. A. and Farb, S. E. (2003). Information and equity. *Annual Review of Information Science and Technology*, Vol 37 No 1, 499-540.

Lops, P., De Gemmis, M. and Semeraro, G. (2011). Content-based recommender systems: State of the art and trends. In Ricci, F., Shapria, B and Kantor, P.B. (Ed.s). *Recommender systems handbook*. Springer, Boston, MA. pp. 73-105.

Mager, A. (2012). Algorithmic ideology: How capitalist society shapes search engines. *Information, Communication & Society*, Vol 15 No 5, pp.769-787.

Martey, R.M. (2008). Exploring gendered notions: Gender, job hunting and web searches. In: Spink, A, and Zimmer, M. (Eds.). *Web search - Multidisciplinary Perspectives*, Springer, Berlin, Heidelberg, pp. 51-65.

Mayer, J.R., Narayanan, A. (2011). Do not track *iab/w3c/ietf position paper*. Tech. rep., W3C, available at: https://www.iab.org/wp-content/IAB-uploads/2011/03/jonathan_mayer.pdf (accessed 24th June 2021)

McKay, D., Makri, S., Gutierrez-Lopez, M., MacFarlane, A., Missaoui, S., Porlezza, C. and Cooper, G., (2020). We are the Change that we Seek: Information Interactions During a Change of Viewpoint. In Arapakis, I., Hoeber, O, & Lopatovska, I. (Eds.). *Proceedings of the 2020 Conference on Human Information Interaction and Retrieval*, ACM, N.Y. (pp. 173-182).

Moe, K.K., Jensen, J.M. and Larsen, B. (2007). A qualitative look at eye-tracking for implicit relevance feedback. In *Proceedings of the Workshop on Context-Based Information Retrieval*. Vol. 326. pp.36-47.

Mountain, D. and MacFarlane, A., 2007. Geographic information retrieval in a mobile environment: evaluating the needs of mobile individuals. *Journal of information science*, Vol. 33 No. 5, pp.515-530.

Munson, S.A. and Resnick, P. (2010). Presenting diverse political opinions: how and how much. In Fitzpatrick, G., Hudson, S., Edwards, K. and Rodden, T. (Ed.s). CHI'10: *Proceedings of the SIGCHI conference on human factors in computing systems.* pp.1457-1466.

Nagulendra, S. and Vassileva, J. (2014). Understanding and controlling the filter bubble through interactive visualization: a user study. In Almeida, V. and Herder, E. (Ed.s). HT'14: *Proceedings of the 25th ACM conference on Hypertext and social media*. pp. 107-115.

Narayanan, A. and Shmatikov, V. (2006). How to break anonymity of the netflix prize dataset. arXiv preprint cs/0610105.

Nissenbaum, H. (1997). Toward an approach to privacy in public: Challenges of information technology. *Ethics & Behavior*, Vol 7 No 3, pp.207-219.

Nissenbaum, H. (1998). Protecting privacy in an information age: The problem of privacy in public. *Law and Philosophy*, Vol. 17, pp.559-596.

Nissenbaum, H. (1999). The meaning of anonymity in an information age. *The Information Society*, Vol 15 No 2, pp.141-144.

Nissenbaum, H. (2001). Securing trust online: Wisdom or oxymoron. *Boston University Law Review*, Vol 81, pp.635.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, Vol 79 No 1, pp.119-157.
Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, Vol 140 No 4, pp.32-48.
Nissenbaum, H. (2020). Privacy in context: Technology, Policy, and the Integrity of Social Life. Stanford University Press, Redwood City, CA.
Noble, S.U. (2018). Algorithms of Oppression: How Search Engines Reinforce Racism. New York University Press, N.Y.
Pariser, E. (2011). *The filter bubble: What the Internet is hiding from you*. Penguin UK.
Paisley, W. J., & Parker, E. B. (1965). Information retrieval as a receiver-controlled communication system. In Heilprin, L.B. (Ed.) *Proceedings of the Symposium on Education for Information Science* pp. 23-31.
Pouyanfar, S., Sadiq, S., Yan, Y., Tian, H., Tao, Y., Reyes, M.P., Shyu, M.L., Chen, S.C. and Iyengar, S.S. (2019). A survey on deep learning: Algorithms, techniques, and applications. *ACM Computing Surveys*, Vol. 51 No. 5. 92.
Ricci, F., Rokach, L. and Shapira, B. (2011). Introduction to recommender systems handbook. In Ricci, F., Shapria, B and Kantor, P.B. (Ed.s). *Recommender systems handbook*. Springer, Boston, MA. pp. 1-35.
Rieder, B. (2005) Networked control: Search engines and the symmetry of confidence. *The International Review of Information Ethics,* Vol 3, pp.26-32.
Robertson, S.E. and Jones, K.S. (1976). Relevance weighting of search terms. *Journal of the American Society for Information science*, Vol. 27 No. 3. pp.129-146.
Robertson, S.E., Walker, S., Jones, S., Hancock-Beaulieu, M.M. and Gatford, M. (1995). Okapi at TREC-3. *Nist Special Publication Sp, 109*, pp.109-126.
Robertson, R.E., Jiang, S., Joseph, K., Friedland, L., Lazer, D. and Wilson, C., 2018. Auditing partisan audience bias within google search. *Proceedings of the ACM on Human-Computer Interaction*, Vol 2 Article 148, pp.1-22.
Schroeder, R. (2014). Does Google shape what we know? *Prometheus*, Vol. 32, No. 2, pp.145-160.
Shannnon, C.E. (1948). A Mathematical Theory of Communication. *Bell System Technical Journal*. Vol. 27 No.3. pp.379-423.
Shannon, C. E. (1956). The bandwagon. IRE Transactions on Information Theory, Vol 2 No 1, 3.
Shani, G. and Gunawardana, A. (2011). Evaluating recommendation systems. . In Ricci, F., Shapria, B and Kantor, P.B. (Ed.s). *Recommender systems handbook*. Springer, Boston, MA. pp. 257-297.
Shen, X., Tan, B. and Zhai, C. (2007). Privacy protection in personalized search. *SIGIR Forum.* Vol. 41. No. 1. pp.4-17.
Shipman, T. (2016). *All out war: the full story of how Brexit sank Britain's political class*. Harper Collins UK.
Silverstein, C., Hannes, M., Henzinger, M. and Moricz, Michael. (1999). Analysis of a very large web search engine query log. *SIGIR Forum. Vol.* 33 No. 1. pp.6-12.
Smith, C.L. and Rieh, S.Y. (2019). Knowledge-Context in Search Systems: Toward Information-Literate Actions. In Azzopardi, L., Halvey, M., & Ruthven, I. (Ed.s). CHIIR'19: *Proceedings of the 2019 Conference on Human Information Interaction and Retrieval*. pp. 55-62.
Spirin, N. and Han, J. (2012). Survey on web spam detection: principles and algorithms. *ACM SIGKDD explorations newsletter.* Vol. 13 No. 2. pp.50-64.
Schultheiß, S. & Lewandowski, D. (2021). Misplaced trust? The relationship between trust, ability to identify commercially influenced results, and search engine preference. *Journal of Information Science*. https://doi.org/10.1177/01655515211014157 (accessed 24th June 2021).
Stanford Encyclopedia of Philosophy. (2016). *Search Engines and Ethics*. https://plato.stanford.edu/entries/ethics-search/ (accessed 24th June 2021).
Susser, D., Roessler, B. and Nissenbaum, H. (2019a). Online manipulation: Hidden influences in a digital world. *Georgetown Law Technology Review*. Vol 4 No 1, pp1-45.

Susser, Daniel; Roessler, Beate; Nissenbaum, Helen (2019b). Technology, autonomy, and manipulation, Internet Policy Review, 8(2), https://policyreview.info/articles/analysis/technology-autonomy-and-manipulation (accessed 24th June 2021).
Tamine-Lechani, L., Boughanem, M. and Zemirli, N. (2008). Personalized document ranking: Exploiting evidence from multiple user interests for profiling and retrieval. *Journal of Digital Information Management*. Vol. 6 No.5. pp.354-365.
Tavani, H.T. (2005). Search engines, personal information and the problem of privacy in public. *The International Review of Information Ethics*, Vol. 3, pp.39-45.
Toch, E., Wang, Y. and Cranor, L.F. (2012). Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems. *User Modeling and User-Adapted Interaction*, Vol 22 No 1-2, pp.203-220.
Tsai, J.Y., Egelman, S., Cranor, L. and Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information systems research*, Vol 22 No 2, pp.254-268.
Tufekci, Z. (2014a). Engineering the public: Big data, surveillance and computational politics. *First Monday*, Vol. 19 No. 7. https://firstmonday.org/article/view/4901/4097
Tufekci, Z. (2014b). Big questions for social media big data: Representativeness, validity and other methodological pitfalls. In Adar, E. & Resnick, P. (Eds.). *Proceedings of the 8th International AAAI Conference on Web and Social Media,* Vol. 8 No. 1, Available on: https://ojs.aaai.org/index.php/ICWSM/article/download/14517/14366 (accessed 24th June 2021).
Tufekci, Z. (2015). Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. *Colorado Technology. Law Journal*. Vol. 13 No. 2. pp.203-237.
Tufekci, Z. (2018). YouTube, the great radicalizer. The New York Times, 10 March. https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html
Van Couvering, E. (2007). Is relevance relevant? Market, science, and war: Discourses of search engine quality. *Journal of Computer-Mediated Communication*, Vol 12 No 3, 866-887.
Van Couvering, E. (2008). The history of the Internet search engine: Navigational media and the traffic commodity. In: Spink, A, and Zimmer, M (Eds.). *Web search - Multidisciplinary Perspectives*. Springer, Berlin, Heidelberg, pp.177-206.
Verma, I.M. (2014). Editorial expression of concern: experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences of the United States of America*. Vol. 111 No. 29. pp.10779-10779.
Wang, Y., Kobsa, A. (2007). Respecting users' individual privacy constraints in web personalization. In: Conati, C., McCoy, K., Paliouras, G. (Eds.). *Proceedings of 11th international conference on user modeling (UM07),* Springer-Verlag, Berlin–Heidelberg–New York, pp.157–166.
Weideman, M. (2009). *Website visibility: the theory and practice of improving rankings*. Chandos, Oxford, UK.
Welp, C. and Machill, M., 2005. Code of Conduct Transparency in the Net: Search Engines. *The International Review of Information Ethics*, Vol 3, pp.18.
Wiener, N., (1954). *The Human Use of Human Beings: Cybernetics and Society*. Garden City, New York.
Vrijenhoek, S., Kaya, M., Metoui, N., Möller, J., Odijk, D., & Helberger, N. (2021). Recommenders with a Mission: Assessing Diversity in News Recommendations. In Elsweiler, D., Joho, H. Kando, N. & Smith, C. (Eds.) *Proceedings of the 2021 Conference on Human Information Interaction and Retrieval (CHIIR 2021)*, pp.173-183.
Xing, X., Meng, W., Doozan, D., Feamster, N., Lee, W. and Snoeren, A.C. (2014). Exposing inconsistent web search results with bobble. In Faloutsos, M. and Kuzmanovic, A. (Ed.s). PAM'14: *International Conference on Passive and Active Network Measurement*. pp.131-140.
Yalcin, E. and Bilge, A., 2021. Investigating and counteracting popularity bias in group recommendations. *Information Processing & Management*, Vol 58 No 5, https://doi.org/10.1016/j.ipm.2021.102608 (accessed 24th June 2021).

Zhang, Y., Mao, J. and Ai, Q. (2019). SIGIR 2019 Tutorial on Explainable Recommendation and Search. In Maarek, Y., Nie, J. and Scholer, F. (Ed.s). SIGIR'19: *Proceedings of the 42nd International ACM SIGIR Conference on Research and Development in Information Retrieval*. pp.1417-1418.

Zipf, G.K. (1949). *Human behavior and the principle of least effort*. Addison-Wesley, Cambridge, Massachusetts.

Zimmer, M. (2007). Privacy and Surveillance in Web 2.0: A study in Contextual Integrity and the Emergence of Netaveillance. *Society for Social studies of Science*, pp.163-175.

Zimmer, M., (2008a). The gaze of the perfect search engine: Google as an infrastructure of dataveillance. In: Spink, A, and Zimmer, M. (Eds.). *Web search - Multidisciplinary Perspectives,* Springer, Berlin, Heidelberg, pp. 77-99.

Zimmer, M. (2008b). The externalities of search 2.0: The emerging privacy threats when the drive for the perfect search engine meets Web 2.0. *First Monday*. Vol. 13 No. 3. https://firstmonday.org/ojs/index.php/fm/article/view/2136 (accessed 24th June 2021).

Zimmer, M. (2008c). Privacy on planet Google: Using the theory of contextual integrity to clarify the privacy threats of Google's quest for the perfect search engine. Journal of Business & Technology Law, Vol. 3, https://digitalcommons.law.umaryland.edu/jbtl/vol3/iss1/8/ (accessed 24th June 2021).

Zimmer, M. (2010a). "But the data is already public": on the ethics of research in Facebook. *Ethics and information technology*, Vol. 12 No. 4), pp.313-325.

Zimmer, M. (2010b). Is it ethical to harvest public Twitter accounts without consent? MichaelZimmer. org, 12. https://tinyurl.com/hn428ws (accessed 24th June 2021).

Zimmer, M. and Proferes, N.J. (2014). A topology of twitter research: Disciplines, methods, and ethics. *Aslib Journal of Information Management*, Vol 66 No 3, pp.250-261.

Zimmerman, S., Thorpe, A., Fox, C. and Kruschwitz, U. (2019). Privacy Nudging in Search: Investigating Potential Impacts. In Azzopardi, L., Halvey, M., & Ruthven, I. (Eds.). CHIIR'19: *Proceedings of the 2019 Conference on Human Information Interaction and Retrieval*. pp. 283-287).

Zimmerman, S., Thorpe, A., Chamberlain, J. and Kruschwitz, U. (2020). Towards Search Strategies for Better Privacy and Information. In Arapakis, I., Hoeber, O. and Lopatovsak, I. (Eds.). *Proceedings of the 2020 Conference on Human Information Interaction and Retrieval*. pp. 124-134.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile books, London, UK.