Transparency enhancing tools (TETs): an overview

Milena Janic, Jan Pieter Wijbenga
TNO
Delft, The Netherlands

Thijs Veugen
TNO
Delft University of Technology
Delft, The Netherlands

Abstract—**As the amount of users' information collected and exchanged on the Internet is growing, so are, consequently, the users' concerns that their privacy might be violated. Some studies have shown that a large number of users avoid engaging in online services due to privacy concerns. It has been suggested that increased transparency of privacy related mechanisms may promote users' trust. This paper reviews the relationship between users' privacy concerns, transparency enhancing and privacy enhancing mechanisms on the one hand, and users' trust on the other, based on the existing literature. Our literature review demonstrates that previous studies have produced inconsistent results, implying this relationship should be re-examined in future work. Impact of higher transparency on users' trust has been insufficiently studied. Current research seems to suggest that the increase of the understanding of privacy issues increases importance of privacy for trust. Use of privacy enhancing mechanisms by service provider also seems to promote the trust, but this may only hold when these mechanisms are understood by the user. A need for tools that would provide users with this kind of knowledge has also been repeatedly recognized. Additionally, this paper provides an overview and description of the currently available transparency enhancing tools. To the best of our knowledge, no such overview has been available to this end. We demonstrate that the majority of tools promote awareness. Most of them attempt to provide a better understanding of privacy policies, or provide insight in the third party tracking behavior. Two tools have been identified that provide some insight in the collected user's data. No tool providing specific information on, or access to, processing logic has been identified.**

Keywords— privacy, privacy enhancement tools, transparency enhancement tools, trust

I. INTRODUCTION

With the increased use of the Internet, the amount of users' information being collected, stored and exchanged is increasing accordingly, and so are the risks related to sharing personal data. Identity theft is the fastest-growing crime in the US today [1]. Consequently, users' concerns about the protection of their personal information have grown.

In order to improve the privacy protection, Privacy Enhancing Technologies (PETs) emerged. According to the definition given in [2], Privacy Enhancing Technology is a system of ICT measures protecting informational privacy by eliminating or minimizing personal data, thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system. Some examples of PETs are interactive anonymity systems (e.g. the onion router [3]), communication privacy systems (e.g. PGP [4]) or counter profiling measures [5], (see [6] for more examples).

Often, data protection regulation (e.g. EU Data Protection Directive 95/46/EC in Europe) requires that users are properly informed about the fact that personal information is collected, stored, processed and disclosed, to what purpose, and how exactly, when they use a certain system. User should also be informed about third parties with which information is shared. In To meet this need, the concept of Transparency Enhancing Technologies (TET) was proposed. If we define transparency as insight in how user's data is being collected, stored, processed and disclosed, TETs can then be viewed as tools providing this insight in an accurate and comprehensible way.

In contrast to PETs, these technologies exercise no particular action to enhance users privacy. They rather provide the user with necessary information on how her data is being stored, exchanged, processed and used, and as such, preserve user privacy indirectly, by enabling the user to make an informed choice on the action she finds she needs to take. Some authors use the term privacy awareness tools when referring to tools that increase privacy awareness by informing users on how their personal information is used by the service provider(s) [7]. We believe, based on the description of functional requirements of privacy awareness tools given in [7] that these two terms (transparency enhancing tools and privacy awareness tools) can be used interchangeably.

Various studies report that users are reluctant to give out personal information in Internet-based transactions, due to concerns about how their personal data is being handled [8][9]. It has been suggested that higher transparency by organizations on this issue might promote trust of the users and their willingness to use a particular online service.

This paper addresses the following questions:

(*i*)(*a*) *What is the relation between user's privacy concerns and their trust in a particular service, based on the research available to this end?*

(*i*)(*b*) *Does the available body of evidence support the assumption that more transparency would lead to more trust? And, if so, which information should be presented to the user to promote her trust?*

(*ii*) *Which transparency enhancing tools are available at this moment, and do they incorporate such information?*

The remainder of the paper is organized as follows. Section II presents the literature overview of the relation between privacy concerns, privacy enhancing measures and trust.

Section III provides an overview of 16 transparency enhancing tools (TETs) identified, 13 of which operable at the time of writing. This paper provides an overview of TETs only; PETs are out-of-scope of this paper. To the best of our knowledge, the only overview of the existing TETs has been provided in [10]. However, the study in question primarily provides a theoretical framework for TETs benchmark criteria, and reviews only 4 TETs (discussed in this paper as well). Finally, we conclude in Section IV.

II. PRIVACY AND USERS' TRUST

This section presents the literature review of the relation between privacy concerns, privacy enhancing measures and users' trust. Subsection II.A. summarizes research reports on the users' privacy concerns. Subsection II. B. discusses which factors seem to impact the users' trust in the online environment, and addresses the relation between privacy related issues and trust. The need for easy-to-understand privacy transparency mechanisms is discussed in Subsection II.C. The findings are discussed in II.D.

A. Internet users' privacy concerns

Over the course of the last decade, different surveys have taken place to assess users' attitude toward online privacy. Most studies report that the majority of the surveyed users indicate to be concerned about their online privacy and online security [8][9][11][12][13][14][15][16][17]. According to Pew Internet & American Life Project, between 80% – 95% of Americans, depending on question framing, indicate they find privacy to be very important [12]. Also European Internet users seem to be well aware of the various hazards related to their online activity [9]. 90% of European respondents in [9] indicated to be aware that their privacy may be violated by leakage or an abuse of their personal information sent via the Internet.

Studies have shown that both individual-level factors, such as age, gender and education level, as well as socio-cultural factors influence user's perception of privacy [13][14]. Cho *et al.* conducted a survey among Internet users from 5 multinational cities. They demonstrated that more than 70% of the Internet users expressed privacy concerns, but that the level of concern varied across factors such as age, gender and nationality [14].

Different surveys have demonstrated that different people have different interpretations of privacy and related concerns [12]. Some users prefer not to disclose anything about themselves, in order not to be identified. Others want their personal data not to be shared with third parties without their permission. Again others are worried about whether their shared data is protected well enough. Also, respondents in some surveys tend not to distinguish between their privacy and security concerns. Paine *et al.* reported in [15] that the majority of respondents (56%) confirmed having privacy concerns when online. However, most of them (27% of respondents) appeared to have security related concerns (such as viruses and spam). Only 2.2% and 1.2% of the total respondents specifically indicated to worry about access to their personal information and identity theft, respectively.

Most studies so far have focused on user's attitude toward privacy. User's privacy protection behavior has received much less attention, with few notable exceptions [14][16][17]. Cho *et al.* found in [14] that both demographic and cultural values influenced the online privacy coping strategy applied (avoidance, opting out, or proactive self-protection). A survey by Annalect Research and Platform Logistics [18] showed that 93% of questioned Internet users indicated that they would use a 'do not track' button in their browser if it were available. However, only 22% seemed to be aware of this function being embedded in web browsers, and only 2% reported using it. This finding seems to suggest there is a low level of awareness of available privacy enhancing measures among Internet users.

B. Relation between privacy concerns, privacy enhancing measures and trust in an online environment

The trust of the user appears to be essential for her engaging in commercial transactions via Internet [19][20][21]. Different models, both conceptual and empirical, have been proposed over a course of years to determine the factors that impact user's perception of trust. Empirical studies vary in the respondents sample size and representativeness of general population, as a majority of studies was conducted with university students as subjects. In this subsection we present the results of the survey on the available literature we performed.

In [22] Corritore *et al.* proposed a theoretical model of trust, consisting of three major (groups of) factors: perceived credibility (such as perceived reputation, perceived honesty and perceived expertise), perceived usability and perceived risk. Several empirical studies confirmed the relevance of these individual factors on trust formation [19] [21][23][24][25].

Another important factor that influences trust seems to be the user's understanding of the technology used. Consumers' knowledge of the Internet mechanisms may determine their level of trust in online retailers and their intention to purchase online. The relation between such knowledge and trust is however a matter of debate. Hoffman *et al.* reported in [26] that increase in expert knowledge damages trust. Later studies supported the opposite effect: the more the consumers know, specifically, the more knowledge they have about the functioning principles underlying how the system works, the more they appear to trust online shopping [25] [27]. Obtaining such knowledge on topics of online security and privacy does seem to be challenging for average users, even for highly educated ones, as suggested by respondents' responses in [28].

The research on relation between privacy concerns and online trust also provides contradictory results. A 2005 survey conducted by Privacy & American Business [8] reported that, due to concerns about the use of personal information, 64% of respondents decided not to purchase something online as they were unsure how their personal information would be used, and 67% of respondents indicated to decline to register at a website, or shop online, as they found the privacy policy too unclear. On the other hand, a study by Pew Internet & American Life Project performed the same year showed that, although majority of Americans claimed to have privacy concerns, 67% gave up personal information to buy something online [29].

Also empirical research by Bart *et al.* [30] demonstrated that privacy was a most important factor determining the trust for a specific web site category: web sites with high information risk. A survey conducted among a group of 1042 Dutch citizens in September 2012 [31] reported that 34% of respondents indicated that the major reason for their distrust of online services was their perception of insufficient privacy guarantees of a particular online service. The authors provide in [31] one possible explanation for such dominant impact of privacy concerns on distrust: a high media coverage on privacy incidents in the several weeks prior to the survey.

On the other hand, Costante *et al.* showed in [32] that, when asked to assign weight to different factors of trust, respondents assigned low weight to privacy compared to other factors (such as brand name, website reliability, reputation, to name a few), however, the weight users assigned to importance of privacy increased with the level of user's knowledge. This finding may be a result of the way the privacy research question was framed: whether users read long and complex privacy policy statements. As authors pointed out, the question should be reformulated in such a way that it reflects the importance users award to how service providers treat their privacy. A different outcome would not only suggest that privacy issues may be more relevant for trust formation, but would also suggest that other mechanisms are needed for enabling users to understand the privacy policies specifically, and how their personal information is being handled in general. Interesting to note is that the weight users assigned to importance of privacy in [32] increased with the level of user's knowledge, which may support the suggestion that current privacy transparency mechanisms are not easy enough to be understood.

Though inconsistent about importance of privacy for trust, literature suggests that if users do trust a provider, they seem to be willing to share personal information [19][33]. The willingness to share the data can also increase if the user finds the advantages of engaging in such a transaction more valuable than the loss of her privacy [34][35].

We can conclude that, due to the inconsistency in the results on importance of privacy for user's trust formation, future work should reexamine this relationship. Perceived risk seems to be one of the factors of trust, hence future work should examine to which extent perceived privacy concerns influence perceived risk. Future work should also take into account multidimensionality of privacy concerns, and re-examine this relationship for each of the facets. For example, a possibility of personal health or financial information disclosure can have a much higher impact on trust, than disclosure of user's behavior. Future research should also attempt to identify reasons users indicate for their lack of concern, in order to identify whether it may be a result of their misconception of their knowledge level.

The relationship between privacy enhancing measures and transparency enhancing measures on the one hand, and the trust of the user on the other, has not yet been extensively examined. The presence of privacy policies on a website seems to augment users' trust [36], although 70% of people surveyed disagreed with the statement "privacy policies are easy to understand" [37], and they are rarely read [38].

Indications that the provider has implemented additional technological measures, such as PETs, seem to augment the trust of new users [23]. These indications seem to have a stronger impact on users' trust, than the privacy policies [33]. On the other hand, in [39], several examples of privacy enhancing technologies (PETs) were discussed with the participants of the study. Participants expressed to find it difficult to form their opinion about PETs in general, as they considered themselves not to be informed enough on the details and the mechanisms of a particular technology (how it works). This may suggest clearer mechanisms are needed to explain these technologies to users. Furthermore, participants in this survey pointed out that even when a particular technology was well understood, e.g. data anonymization, they were still unable to fully trust whether this technology was also applied and effective (whether data was truly anonymized). However, it is difficult to extrapolate these results to the general population of Internet users, as their findings are based on a survey conducted with a very limited users' sample size (30 respondents, while majority of empirical studies included approximately 250 subjects). Hence, the influence of PETs on trust, as well as the influence of understanding the PETs on trust, need to be subjected to further examination.

Last but not least, also increased transparency may have opposite effects on willingness of users to perform electronic purchases, depending on the knowledge level of the user. Considering the example of privacy policies, Tsai *et al.* discuss in [40] that consumers may perceive greater risk and uncertainty when dealing with organizations whose privacy policies are unknown; as a result, they may be reluctant to engage in transactions with those organizations. However, if the lack of information is so profound that consumers are not even aware that their personal information might be exchanged or misused, it may make them more likely to engage in such risky (from a privacy point of view) transactions. Therefore, the effect of privacy transparency on user's trust in itself, and as a function of the user's knowledge level, needs to be further assessed in future.

C. Discussion

A large body of evidence seems to confirm the growing privacy concerns among Internet users, though research conducted is not always strict on the definition of privacy-respondents tend to confuse privacy with general security. Respondents that indicate not to be concerned about privacy seem not to be well acquainted with possible consequences, or may have a false sense of safety due to misconceptions on their knowledge level [28]. The effects of privacy concerns, PETs and transparency on trust have been studied to some extent, but provide inconsistent results. Therefore, we define 4 research topics to be addressed in future work:

(*i*) *Do privacy concerns, and which (concerns about which specific information discosure), increasingly impact trust if user's awareness level is higher, or if level of understanding of privacy mechanisms is higher?*

(*ii*) *Does presence of privacy policies increase trust by itself, or only if privacy policies are understood?*

(*iii*) *Do indications that PETs are applied improve trust, or only when PETs are understood?*

(*iv*) *Does increase in transparency increase trust by itself, or combined with increase in awareness level, or with increase in underlying privacy mechanism principles understanding?*

D. Need for better understanding of privacy mechanisms

Despite the discrepant results on importance of privacy for user's trust, several studies recognized the need for tools that would facilitate easy understanding of privacy mechanisms [23][25][29][32]. In [29] respondents pointed out that new, easy-to-use technological tools, which would provide users with a sense of control, or at least transparency, would be appreciated. Respondents also expressed that an education campaign aimed at improving user's understanding of threats they face, and of protection mechanisms, was also desirable. Pieters discusses in [41] explanation-for-trust and defines it as explanation of how a system works, by revealing details of its internal operations. He further argues that explanations, should (1) aim for the right goal (why or how) and (2) carry the right amount of information: too little detail does not explain-for-*trust*; too much detail does not *explain*-for-trust. In [25] Kini and Choobineh differentiate between three knowledge levels. The first level is *awareness knowledge*, which is knowledge that a system exists. The second level is *how-to knowledge*, which is knowledge about how to use a system properly. The third stage is *principles' knowledge*, which is knowledge about the functioning principles underlying how the system works. Authors argue that *principles knowledge* is key in developing trust in the system, and that further research is needed to identify which information presentation modes, which amount of information presented, and which content of the information would impact trust most. They recognized that even if the information presented is complete and accurate, if it is not understood by users it would not increase trust. In the following section we present some tools available to this end that aim to provide the user with such information.

III. TRANSPARENCY TOOLS OVERVIEW

As discussed in previous section, a need for tools that would enable easy understanding of privacy mechanisms has been repeatedly recognized. We extend the definition of a transparency enhancing tool (TET) for privacy purposes given in [10], and define a TET as a technological tool that has one or more of the following characteristics:

– provides user with information on intended data collection, storage, processing and/or disclosure (how service providers claim to handle user's personal information)

– provides user with information on data collected, stored, processed and/or disclosed (how service providers actually handle user's personal information)

– present the above listed information in an accurate and for an average Internet user comprehensible way.

We have collected, downloaded and tested 13 identified operable TETs. However, as we performed no tests with a group of users, we can provide no evaluation of how the end users perceive the TETs to achieve transparency. Collected TETs have been classified in five categories, presented in Sections III.A. – III.E, according to the transparency functionality they offer. Section III.F. presents TETs that are currently under development.

A. Transparency as insight in intended data collection, storage, processing and/or disclosure

This subsection describes the tools which attempt to provide a better comprehension of a website's privacy policy.

1) Mozilla Privacy Icons

Description: Privacy Icons [42] is a joint work in progress between Mozilla, the company Disconnect and Stanford. Privacy policies and terms of service are often long-winded, complex documents that encapsulate a lot of situation-specific details. Privacy Icons help users to understand these privacy policies, which indicate how their personal data will be transacted and thereby enable users to make informed choices about whether to share their data. Privacy Icons make use of simple visual language to make privacy policies more understandable—the complexity of privacy policies is reduced to an indicator that is scannable in seconds. Privacy policies are translated into and visualized with the use of 4 icons, each depicting one of the following categories: expected use, expected collection, requests for data, and data retention. However, the definition of the categories is not definite and is subject to change. At the time of writing, 2,640 major sites were provided with Privacy Icons.

Transparency functionality: this tool enhances transparency of a website's privacy policy, as it provides the user with a simple visual representation of the most relevant implications of complex privacy policy documents.

2) Privacy Bird

Description: Privacy Bird [43] is an add-on for Internet Explorer (IE), that automatically searches for privacy policies at every web site a user visits. It automatically reads policies encoded according to the Platform for Privacy Preferences (P3P) standard, nowadays pretty much defunct, and displays them in an easy to understand language. Privacy Bird matches user's personal privacy preferences with the privacy policy, and notifies the user as to whether her privacy preferences are met by displaying a bird icon in the top right of user's browser's title bar. The singing green bird appears when a website's privacy policy matches user's preferences. If the site contains images or other embedded content that do not have privacy policies associated with them, a red exclamation point would appear next to the notes in the bird's song bubble. If Privacy Bird determines that a website's privacy policy conflicts with user's preferences, the angry red bird appears. If privacy bird is unable to read a privacy policy from the site the user is visiting, an uncertain yellow bird would appear.

Transparency functionality: this tool enhances transparency of a website's privacy policy as it automatically matches user's privacy preferences to the website privacy policy (provided the latter is encoded according to the P3P standard).

3) Privacyscore

Description: Privacyscore [44] is an add-on for Firefox and Chrome that represents an assessed privacy risk, to both personal and anonymous data (e.g. users' preferences), of using a website. A Privacyscore is computed out of nine factors. Four factors are based on the site's privacy policy and cover how websites promise to handle user's personal data (such as user's name or email address). Privacyscore goes beyond privacy policy, as five factors are computed based on privacy qualifications of the third companies collecting data on the website. The user interface makes this tool very clear and easy to use.

Transparency functionality: this tool enhances the transparency of how a particular website may treat users' information (both personal, e.g. name, and anonymous, e.g. interests).

B. Transparency as insight in collected and/or stored data

The group of tools described in this subsection provide the user with insight in the information she has disclosed.

1) Primelife Privacy Dashboard

Description: PrimeLife's Privacy Dashboard [45] (formerly known as Data Track), one of the deliverables of a PrimeLife project, is a transparency-enhancing tool that provides the user with a history function, describing which documents, containing what personal data, the user has disclosed, to whom, and under which conditions, as well as with functions for accessing her personal data through online remote services. This data is presented on packet level and it is questionable whether it provides a level of comprehensibility necessary for an average Internet user.

Transparency functionality: This tools promotes transparency by providing insight in information visited websites gather, however has a low level of comprehensibility.

2) Google Dashboard

Description: Google Dashboard [46] is a website that allows Google users to see some of the personal data that Google stores, like web search history, Google Agenda and Android devices used by this Google account. It links to settings where users can influence the storage and visibility of data. The dashboard shows only a subset of all the data that Google may store about the user. The dashboard has a link that shows some examples of how Google stores data that is not linked to your Google account, such as advertising profiles, cookies and server log files. It also states that there is more user data stored without stating the nature of that data, and it points to the privacy policy for more information.

Transparency functionality: this tool provides the user with information on some of the data that Google has stored about her.

C. Transparency as insight in third party tracking (insight in user behaviour data disclosure)

Tools described in this subsection provide users with information on the third parties that track users as they surf through the Internet.

1) Collusion

Description: Collusion [47] is an add-on for Firefox, Chrome and Safari which provides an interactive, real-time visualization of the third parties that track users' movements across the web. It shows how that data creates a spider-web of interaction between companies and other trackers. The presentation of the traffic flows and user interface makes Collusion very easy to follow and use. Each dot in the web represent a visited website, and is linked to the dots that represent advertising sites that have created cookies in user's browser and are tracking his behavior on this website. Advertising sites are colored red, as privacychoice.org determined they are behavioral tracking sites. When the user moves to another site, the same cookies are transmitted to the same advertisers. Those advertisers can effectively track the user across them, and can use this information to determine the content the user will read. By hovering the mouse over any of the dots presented the user learns more about those entities and is provided insight in sites they are affiliated with. At the time of the writing, there were 204,000 and 140,000 users of Collusion, for Firefox and Chrome browsers respectively.

Transparency functionality: this tool provides web users with the list of entities that are tracking them through the websites they visit. It demonstrates the consequences of the user's browsing activities, and leaves it up to the user whether she wishes to continue activities on a particular website in an unchanged manner, or act upon it by engaging additional privacy enhancing functions (e.g.'block').

2) Netograph

Description: Netograph [48] is an add-on (available for Chrome and Firefox browsers) that provides a user with a quick view of what a website on the 'social web' actually does (in terms of which resources are requested, and by whom) before the user visits it. Netograph monitors links passing through the social web in realtime, and provides a visual representation of it (graph). User can click on the objects and move them around to create the clearest picture. The layout is very straightforward, making the website very user-friendly.

Transparency functionality: this tool promotes insight in unwanted disclosure.

D. Transparency as insight in data collection, storage, processing and/or disclosure based on website's reputation

1) Web of Trust (WOT)

Description: WOT [49] is a reputation based add-on for Firefox, Chrome, Internet Explorer, Opera, and Safari browsers. Reputation icons, shown on popular search engine results, social media platforms, online email, shortened URLs, and many popular sites, demonstrate how much other users

trust a certain website. Ratings are based on information from millions of users and trusted third-party sources. Users can contribute to the service by rating websites based on their own experiences. Sites are evaluated on 4 criteria: trustworthiness, vendor reliability, privacy and child safety. At the time of writing, WOT had 1,590,475 and 21,000 users for Firefox and Chrome browsers, respectively.

Transparency functionality: this tool increases transparency by demonstrating to the user other people's experiences with a certain website.

E. Transparency as insight into (possibly) unwanted user's data disclosure (awareness promoting)

Although they differ in the specific information they demonstrate to the user, all tools presented in this subsection have in common that their goal is to provide users with insight into some specific risks for their privacy they may face when using the Internet, and as such promote users awareness regarding privacy.

1) Me & My Shadow

Description: Me &My Shadow [50] is a website designed to raise awareness and educate Internet users about what is happening to their information when they use the Internet. Basically, it gives insight in the digital shadow that a user leaves online. This website provides also links to external applications that enhance privacy. For each of the third-party applications, Me & My Shadow provides a description, and additional reading related to each tool. This website also contains a section 'Lost in Small Print', which magnifies the information control points of End User License Agreements of popular websites, like Google and Facebook.

Transparency functionality: this tool is a typical example of a privacy awareness promoting tool, as it informs the user of her digital shadow, and provides her with tips to enhance her privacy protection.

2) Priveazy

Description: Priveazy [51] aims at enabling the user to make the informed decision on how much she wishes, and should wish, to protect herself. The goal of this site is to educate, through videos, quizzes, lessons and tasks, so that the layman can understand what the critical issues are. It also provides specific step-by-step guidelines for users to be implemented for different applications and services. This website is very easy to use.

Transparency functionality: this tool enhances users' awareness as it educates the user on privacy related issues in general, and provides information on how the user can protect her privacy.

3) Firesheep

Description: Firesheep [52] is an add-on allows the user to retrieve cookies from people who have logged in via a wireless network to different websites that are not secured (i.e. through https or SSL). Therefore, it demonstrates the ease at which one can hack into user's accounts if the user is browsing on an insecure website on an open wireless network.

Transparency functionality: this tool provides transparency into user's own activities and promotes awareness, as it demonstrates how easily users' login information can be stolen when on a public network.

4) Panopticlick

Description: Panopticlick [53] is an online tool developed by the Electronic Frontier Foundation (EFF) that tests the user's browser in order to identify how unique this browser is. The tool deploys a browser fingerprinting algorithm which collects a number of commonly and less-commonly known characteristics that browsers make available to websites. In [54] authors reported that out of 470,161 tested browsers operated by informed participants who visited their website, 83.6% of the browsers seen had an instantaneously unique fingerprint, and a further 5.3% had an anonymity set of size 2.

Transparency functionality: this tool promotes awareness as it demonstrates to the user how unique such a trivial thing as a browser can be. The browser information allows websites to track the user, if her browser's fingerprint is unique.

5) Creepy

Description: Creepy [55] is an application that allows the user to gather geolocation related information about users from social networking platforms (such as Twitter) and image hosting services. Given a user name it provides a map of the location associated with that content and links to that content, through the help of third-party applications like Google Maps. It is moderately easy to use, one just needs to understand that latitude and longitude are provided.

Transparency functionality: this tool provides insight into user's own activities, and, hence, promotes awareness as it makes the user aware of the location information that she submits when engaging in various social networking and photo sharing applications.

F. Transparency tools under development

1) Transparen.cc

Description: Transparen.cc. [56] is a proxy service serving as an independent, transparent inter-mediator between social data and the apps that want to use them. It keeps a log of every time social applications try to access personal data, when it was requested, what they were asking for and how much data they obtained. Finally, it builds a profile on what the application is -really- asking for and how often it asks for it. There is no available preview of the user interface.

2) Privacy Bucket

Description: Privacy Bucket [57] is a Chrome extension that measures the extent to which individual third-party trackers can discover demographic information about the user, based on user's browsing history. A tracking company gets access to a portion of the user's web history. Given a set of visited sites, it is possible to determine the probability of a hidden variable, for example a user's age, being a certain value (e.g. visiting a lot of sports sites might suggest that the user is male; visiting aarp.org may suggest that the user is in an older

age range.). For each third-party tracker that is encountered by the user, Privacy Bucket will combine a profile of observations made by the tracker about the user with background information about the browsing habits of a large population, in order to characterize the amount of information the tracker possesses about that user's hidden variables.

3) Online interactive (OI) privacy feature tool

Description: *Online Interactive (OI) privacy feature* tool as introduced in [7] is a tool or an user interface that promotes user's privacy awareness and that incorporate features such as *interactive social translucence* map that discloses the flow of personal information, a *privacy enquiry* for a direct chat about users' privacy concerns, and a *discussion forum* presenting users' privacy concerns using their language in an interactive FAQ format. An evaluation of a prototype of a set of embedded OI privacy features is presented and discussed in [7]. The result from the user study indicated that users favored the interactive data flow map and preferred to be informed of their personal information privacy. However, authors concluded further work was needed privacy communication channels, as the online chat tool was the least appreciated privacy feature.

IV. CONCLUSIONS

The purpose of this paper was twofold:

(*i*) We addressed the question of the effect of privacy concerns, privacy enhancing measures and privacy transparency on trust in online environment based on available literature to this end. Research on these relations provided inconsistent results, and no conclusions can be drawn with confidence. We identified four research topics to be investigated in future work. The current body of evidence seems to suggest that the increase of the understanding of privacy issues increases importance of privacy for trust. A need for tools that would provide users with this kind of knowledge has also been repeatedly recognized. As demonstrated in Section III, there already exist tools to make complex privacy policies more understandable to users, however, no such tools have been identified for more complex privacy enhancing or user data processing mechanisms. Future work includes identifying which information about these mechanisms and/or data processing logic, or what kind of representation of these mechanisms and/or of data processing logic, should be given to an average user to promote trust, and designing a tool that incorporates such information.

(*ii*) We identified 16 transparency enhancing tools (TETs), available to this end, out of which 13 operable at the time of writing. To the best of our knowledge, no such overview of TETs was available to this end. A TET is a technological tool that should provide user with information on (intended) data collection, storage, processing and disclosure in an accurate and comprehensible way. Identified tools were classified in the following categories:

- tools that provide insight in intended data collection, storage, processing and/or disclosure, based on website privacy policy

- tools that provide insight in collected and/or stored data

- tools that provide insight in third parties tracking the user

- tools that provide insight in data collection, storage, processing and/or disclosure based on website's reputation

- tools that provide insight into (possibly) unwanted user's data disclosure (awareness promoting)

No tool giving insight into, or access to, or explaining processing logic has been identified. This seems to indicate a lack of urgency from existing service providers to give insight into exactly which data is processed and exactly how it is processed. Combined with the indications that increased understanding of privacy issues increases the importance of privacy for trust, this may indicate that the users' ignorance of what happens to their personal data is a desired situation for some service providers, who are profiting from sharing the personal data. Good transparency enhancing tools may lift the veil on what is actually happening to the users' personal data.

ACKNOWLEDGMENT

This publication was supported by the Dutch national program COMMIT.

REFERENCES

[1] US Postal Service, "Identity Theft", https://postalinspectors.uspis.gov/investigations/mailfraud/fraudschemes/mailtheft/identitytheft.aspx, Accessed 14 April 2013.

[2] G. W. van Blarkom, J. J. Borking, and P. Verhaar. PET. In G. W. van Blarkom, J. J. Borking, and J. G. E. Olk, editors, Handbook of Privacy and Privacy-Enhancing Technologies - The case of Intelligent Software Agnets, chapter 3, pages 33–54. College bescherming persoonsgegevens, The Hague, The Netherlands, 2003.

[3] S. Garfinkel, PGP: Pretty Good Privacy. O'Reilly, December 1994.

[4] P. F. Syverson, D. M. Goldschlag, and M. G. Reed, "Anonymous Connections and Onion Routing," In Proceedings of the 1997 IEEE Symposium on Security and Privacy, Oakland, CA, May 1997, pp. 44–54.

[5] Z. Erkin, T. Veugen, T. Toft, and R. L. Lagendijk, "Generating Private Recommendations Efficiently Using Homomorphic Encryption and Data Packing", IEEE Transactions on Information Forensics and Security, Vol. 7 (3), June 2012, pp. 1053-1066.

[6] I. Goldberg, Privacy Enhancing Technologies for the Internet III: Ten Years Later, In A. Acquisti, S. Gritzalis, C. Lambrinoudakis, and S. D. C. di Vimercati, editors, Digital Privacy: Theory, Technologies, and Practices, chapter 1. Auerbach, 2007.

[7] E. Kani-Zabihi and M. Helmhout, "Increasing Service Users' Privacy Awareness by Introducing On-Line Interactive Privacy Features," Lecture Notes in Computer Science, Vol. 7161, 2012, pp 131-148.

[8] Privacy & American Business (P&AB). 2005, "New Survey Reports an Increase in ID Theft and Decrease in Consumer Confidence," Conducted by Harris Interactive, May 2005, http://www.e-commercealert.com/article696.shtml, Accessed 14 April 2013.

[9] The Gallup Organization, "Confidence in the information society: analytical report," Flash EB FI 250, http://ec.europa.eu/public_opinion/flash/fl_250_en.pdf, Accessed 14 April 2013.

[10] H. Hedbom, "A Survey on Transparency Tools for Enhancing Privacy", The Future of Identity in the Information Society, IFIP AICT, vol. 298, Springer, Heidelberg, 2009, pp. 67–82.

[11] N.K. Malhotra, S. Kim, and J. Agarwal, "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal

Model", Information Systems Research, Vol. 15(4), Dec. 2004, pp. 336-355.

[12] L. Rainie, "Transportation and privacy in the mobile age", Pew Internet & American Life Project, January 25, 2012, http://www.slideshare.net/PewInternet/transportation-and-privacy-in-the-mobile-age, accessed on April 14, 2013.

[13] S. Bellman, E. Johnson, S. J. Kobrin, and G. L. Lohse. "International Differences in Information Privacy Concerns: A Global Survey of Consumers," Information Society, Vol. 20, no. 5, 2004, pp. 313-324.

[14] H. Cho, M. Rivera-Sanzhez, and S.S. Lim, "A multinational study on online privacy: global concerns and local responses," New Media Society, vol. 11(3), May 2009, pp. 395-416.

[15] C. Paine , U-D. Reips, S. Stieger, A. Joinson, and T. Buchanan, "Internet users' perceptions of 'privacy concerns' and 'privacy actions'," International Journal of Human-Computer Studies, Vol.65(6), June 2007, pp.526-536.

[16] T. Buchanan, C.B. Paine, A.N. Joinson and U.-D. Reips, "Development of Measures of Online Privacy Concern and Protection for Use on the Internet", Journal of the American Society for Information Science and Technology, Vol. 58(2), Jan. 2007, pp. 157–165.

[17] D.J. Phillips, "Privacy Policy and Pets: The Influence of Policy Regimes on the Development and Social Implications of Privacy Enhancing Technologies," New Media & Society, Vol. 6(6), 2004, pp. 691–706.

[18] Annalect Research and Platform Logistics, "Internet Users' Response to Consumer Online Privacy," White paper March 14, 2012, http://annalect.com/wp-content/uploads/2012/06/Consumer_Online_Privacy_Whitepaper.pdf, accessed 14 april 2013.

[19] D. H. McKnight, H.Choudhoury, and C. Kacmar, "The impact of initial consumer trust on intentions to transact with a web site: A trust building model", Journal of Strategic Information Systems, Vol. 11, Issues 3–4, Dec. 2002, pp 297–323.

[20] O.B. Buttner, and A.S. Goritz, "Perceived trustworthiness of online shops", Journal of Consumer Behavior, Vol.7, Jan/Feb 2008, pp. 35-50.

[21] D. Gefen, E. Karahanna, D.W. Straub, "Trust and TAM in online shopping: an integrated model, MIS Quarterly, Vol. 27(1), March 2003, pp. 51–90.

[22] C. Corritore, B. Kracher, and S. Wiedenbeck, "On-line trust: concepts, evolving themes, a model," International Journal of Human-Computer Studies, Vol. 58, no. 6, Jun. 2003, pp. 737–758.

[23] M. Koufaris, and W. Hampton-Sosa, "The development of initial trust in an online company by new customers," Information & Management, Vol. 41, Issue 3, Jan. 2004, pp. 377–397; S-J. Yoon, "The Antecedents and Consequences of Trust in Online Purchase Decisions," Journal of Interactive Marketing, Vol. 16 (2), 2002, pp. 47–63.

[24] A. Everard and S. McCoy, "Effect of Presentation Flaw Attribution on Website Quality, Trust, and Abandonment", Australasian Journal of Information Systems, Vol 16, no. 2, 2010.

[25] A. Kini and J. Choobineh, "An Empirical evaluation of the factors affecting trust in web banking systems," in Americas Conference on Information System, 2000, pp. 185–191.

[26] D. Hoffman, T. Novak, and M. Peralta, "Building consumer trust online," Communications of the ACM, Vol. 42, no. 4, 1999, pp. 80–85.

[27] C.-C. Wang, C.-A. Chen, and J.-C. Jiang, "The Impact of Knowledge and Trust on E-Consumers' Online Shopping Activities: An Empirical Study", Journal of Computers, Vol. 4, no. 1, Jan. 2009, pp. 11-18.

[28] S. Flinn and J. Lumsden, "User perceptions of privacy and security on the web," in The Third Annual Conference on Privacy, Security and Trust (PST 2005), Oct. 2005.

[29] L. Rainie, "Privacy Online: How Americans feel… the ways they are responding to new threats … and why they are changing their online behavior", Pew Internet & American Life Project, March 11, 2005, , accessed on April 14, 2013.

[30] Y. Bart, V. Shankar, F. Sultan, and G.L.Urban, "Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study," Journal of Marketing, Vol. 69, no. 4, Oct. 2005, pp. 133-152.

[31] N. Huijboom, B. vsn Schoonhoven and G. Bodea, "Trust in ICT", submitted for publication

[32] E. Costante, J.I. den Hartog, and M. Petkovic, "On-line trust perception: what really matters," Proceedings of the First Workshop on Socio-Technical Aspects in Security and Trust, STAST'11, Milan, Italy, September 8, 2011, pp. 52-59.

[33] F. Belanger, J.S. Hiller, and W.J. Smith, "Trustworthiness in electronic commerce: the role of privacy, security, and site attributes," Journal of Strategic Information Systems, vol 11, Dec. 2002, pp. 245–270.

[34] B. Berendt, O. Gunther, and S. Spiekermann, "Privacy in e-commerce: stated preferences vs. actual behavior," Communications of the ACM Vol. 48 no.4, April 2005, pp.101-106.

[35] A. Acquisti, and J. Grossklags, "Privacy and Rationality in Individual Decision Making," IEEE Security and Privacy, Vol. 3(1), Jan-Feb. 2005, pp. 26-33.

[36] T.W. Lauer, and X. Deng, "Building online trust through privacy practices," International Journal of Information Security, Vol 6, Sep. 2007, pp. 323–331.

[37] J. Turow, L. Feldman, and K. Meltzer, "Open to Exploitation: American Shoppers Online and Offline," A Report from the Annenberg Public Policy Center of the University of Pennsylvania, 2005.

[38] M. Arcand, J. Nantel, M. Arles-Dufour, and A. Vincent, "The impact of reading a website's privacy statement on perceived control over privacy and perceived trust," Online Information Review, Vol. 31(5), 2007, pp. 661−681.

[39] L. Kool, B. van Schoonhoven, M. van Lieshout, A. Vedder and F.M. Fleurke (in dutch), Trusted Technology: Een onderzoek naar de toepassingsvoorwaarden voor Privacy by Design in de elektronische dienstverlening van de overheid," http://www.rijksoverheid.nl/onderwerpen/digitale-overheid/documenten-en-publicaties/rapporten/2011/12/05/trusted-technology-een-onderzoek-naar-de-toepassingsvoorwaarden-voor-privacy-by-design-in-de-elektronische-dienstverlening-van-de-overheid.html, April 14 2013

[40] J. Tsai, S. Egelman, L. Cranor, and A.Acquisti, "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," Information Systems Research, Vol. 22(2), June 2011, pp. 254-268.

[41] W. Pieters, "Explanation and trust: what to tell the user in security and AI," Ethics and Information Technology, Vol. 13(1), 2011, pp.53–64.

[42] https://icons.disconnect.me/icons, Accessed on April 14, 2013.

[43] http://www.privacybird.org/, Accessed on April 14, 2013.

[44] http://privacyscore.com/, Accessed 14 April 2013.

[45] http://primelife.ercim.eu/results/opensource/76-dashboard, Accessed 14 April 2013.

[46] https://accounts.google.com/ServiceLogin?service=datasummary&passive=900&continue=https://www.google.com/dashboard/?hl%3Den&followup=https://www.google.com/dashboard/?hl%3Den&hl=en, Accessed 14 April 2013.

[47] http://www.mozilla.org/en-US/collusion/, Accessed 14 April 2013.

[48] http://netograph.com/, Accessed 14 April 2013.

[49] http://www.mywot.com/, Accessed 14 April 2013.

[50] https://myshadow.org/#, Accessed 14 April 2013.

[51] https://www.priveazy.com/, Accessed 14 April 2013.

[52] http://codebutler.com/firesheep/, Accessed 14 April 2013.

[53] https://panopticlick.eff.org/, Accessed 14 April 2013.

[54] P. Eckersley, "How unique is your web browser", Proceedings of the 10th international conference on Privacy enhancing technologies, July 2010, Berlin, Germany, pp. 1-18.

[55] http://ilektrojohn.github.io/creepy/, Accessed 14 April 2013.

[56] https://www.hackerleague.org/hackathons/wsj-data-transparency-code-a-thon/hacks/transparen-dot-cc, Accessed 14 April 2013.

[57] https://github.com/mfredrik/Privacy-Bucket/wiki, Accessed 14 April 2013.