Towards Trust-based Decentralized Ad-Hoc Social Networks

Kevin Koidl
Trinity College Dublin
Ireland
kevin.koidl@scss.tcd.ie

ABSTRACT

Social Media has transformed modern day society. It can be argued that one of the main drivers behind this transformation are novel ways to effectively distribute content in a highly targeted fashion and at scale. Recently, this effectiveness has come under attack based on new phenomena known as Fake News, Filter Bubble and Echo Chambers. The public debate about the impact of these phenomena on modern day society ranges from demanding a complete social media shutdown to government intervention and censorship. Furthermore, it appears that Social Media Platform providers are not sure what countermeasures are needed to address these new challenges. The main concern is that Black Mirror like scenarios will emerge simply by allowing privately held companies decide what content is conforming to public norms leading to a distortion of values. This paper presents an alternative solution by focusing on empowering meaningful relationships and not content engagement. The main motivation behind the proposed solution is to create social networks that follow a 'Trust by Design' paradigm. This paper introduces and discusses the above-mentioned challenges and presents a novel new social media concept seeking to overcome current challenges.

CCS CONCEPTS

Networks → Social media networks; Security and privacy → Trust; Human-centered computing → Social networks

KEYWORDS

Social Media, Social Networks, Computational Trust, Online Privacy

1 MOTIVATION

This paper introduces a novel concept for the future design of Social Media applications. To motivate this approach, the following futuristic scenario is presented.

The start of the 21st century was filled with excitement. Several technological advancements painted a bright and wonderful future for mankind. Society had overcome an era of negativity that was triggered by a phenomenon we now know as Fake News. The solution was the creation of an all-encompassing Global Social Sphere in which every human had to be connected.

It was implemented as one large social network in which only positive attitude was allowed. At first it was highly criticized by most policymakers. However, the critical voices became less and finally ceased. The Sphere became the only place in which a citizens was able to purchase, communicate and share experiences. Even though the more intellectual members of society pointed towards the danger of a 1984 like society, most of these thinkers turned a blind eye and saw no harm in using it. After all, it did enforce a positive attitude and sought to eradicate all negative aspects of humanity by mechanically filtering out any content or experience that was not seen as positive. In essence we sought to destroy hate and with it everything that is attached to it, from murder to war. Little did we know that we were feeding a monster. We now call it 'The dark side of the Sphere' and it almost destroyed humanity. We started to marginalise anyone, who was not found to promote positivity at all times and with that fed what we tried to destroy. We trusted machines to make the positivity assessment, which ultimately lead to us losing trust in our own ability to judge good from bad. We became soulless zombies that drifted in a stream of interdependent conformity killing off anything and anyone who was not part of it and eventually crashing down a waterfall and back into reality. It was in the spring of 2081 when we decided to switch off the Sphere. We are now learning to trust ourselves again and each other by allowing each individual to be how nature has intended it. We are setting up a new network, more natural, more organic and based on what humans are more prone to: naturally connecting with their environment. We call it Helios to remind us that it is not the technology, but the human that has to stand in the centre of any real experience.

2 INTRODUCTION

Social Media Application has become an important element in modern day society. They equally serve as communication platform and content distribution platform. Based on their mostly centralized design the social media platform is able to facilitate both aspects in large scale. Two further advantages of this central design are that (1) the user has access to vast amounts of content and (2) access to the overall social graph making it easy to connect with others. The social media platform provider, therefore, can be viewed as a proxy between content and people with a substantial commercial advantage due to being able to distribute premium content in a highly targeted fashion. The underlying principle of content distribution within social networks is based on content engagement, also known as reactions exhibited by users in the form of views, likes, comments and shares. The underlying assumption is that the more engagement a certain piece of content

WWW '18 Companion, April 23–27, 2018, Lyon, France

ACM ISBN 978-1-4503-5640-4/18/04.
https://doi.org/10.1145/3184558.3191608

has, the more interesting it is for the wider community, hence it constitutes a monetizability measure. This means the more users engage on content, the more it can be commercially exploited. This viewpoint is reflected by the use of Greedy-Algorithms [1] that ensure that content indicating increased engagement is distributed quickly and as wide as possible, in the hope to create a viral effect. It can be argued that this focus on content monetization has led to a 'Crisis of Trust'. The three most dominant challenges that are core to this crisis are Filter Bubble [2], Fake News [3,4] and Echo Chambers [5,6]. Filter bubbles are the result of engagement-based content filtering. The underlying principle is to show the user content that relates to the content the user has previously engaged on. The result is a content stream that lacks diversification of topics and opinions. Echo Chambers are a result of content recommendations that are based on interests of friends and peers. This results in a content feed that is strongly biased towards grouped opinion (e.g. Group Think). Finally, fake news and related expressions of the same, such as alternative facts, related to gaming or misusing the underlying greedy algorithm. The result is an increase in the spread of mostly promoted and highly opinionated content. The main approach is to create a viral effect by using fake accounts that increase the engagement resulting in a wider spread of the content [7]. Current algorithms that are responsible for detecting content that is showing high engagement (i.e. is viral) are not able to assess if both the content and the engagement is trustworthy (i.e. not fake). This paper argues that the concept of trust (or the lack of the same) is the driving force behind all three challenges with the first relating to trusting the social media platform managing the distribution of the content (filter bubble). The second challenge relates to trusting friends and peers (echo chamber), and finally the third relates to trusting oneself and ones own judgment (fake news). Based on the centralized concept of most social media platforms, trusting the platform is by far the most common challenge. It can be argued that users simply don't have the control or even leverage to change or understand how content is distributed and what decisions have led to this. Moreover, users are left completely in the dark about what behaviour or engagement has led to content being shown in their content stream. This handover of trust is a critical element for social media applications. In essence it is completely at the discretion of the social network provider how the user's data is used and what content is delivered. However, even though social media platform providers consider the decision over content distribution to be fully theirs, the question of responsibility, in the case of questionable content being spread, is passed on to the content providers and/or users [8]. This argument is based on the claim that social media applications, similar to search indexing engines, only facilitate the distribution and cannot be responsible for the nature of the content itself. This argument, however, is questioned has been questioned by social protection agencies and policymakers leading to the 'Right to be Forgotten' legislation forcing companies to take down content and/or content links [9]. Furthermore, based on the intensity of the public debate around Fake News Social Media Platform providers have introduced questionable countermeasures that include censorship, content monitoring and account banning. The most worrying aspect of applying these measures is that privately held companies are making decisions without reference to any ethical guideline. This can lead to a Black Mirror like scenario in which private corporations or individuals controlling the same, can influence the public debate towards their agenda. Moreover, the current development creates a separate yet connected concern in which individuals (and in this case not content) are assessed and scored for their usefulness. This concern has been highlighted by the US Government in a recent report indicating that Social Scoring can lead to widespread discrimination [10]. Overall, it can be concluded that all challenges introduced above are related to trust and in most cases the lack of the same. To overcome the current 'Trust Crisis' in Social Media Applications this paper introduces a novel social media concept following a 'Trust-by-Design' paradigm. The presented approach (including a draft architecture) seeks to motivate ongoing research in the web community to develop novel approaches that minimize risk to society by Social Media Applications, such as the ones depicted in the TV show Black Mirror.

3 Proposed Solution

The below-introduced solution forms a conceptual base for social network applications to be designed with trust in mind. For this several technological elements are connected to create the overall architecture. This section introduces a use case and all required concepts together with the challenges they address. After this, a preliminary architecture is presented, followed by a discussion of open challenges.

3.1 Background

Social Media Applications are based on the concept of connecting people. This resembles the basic idea of the WWW which in its core was invented to connect information. Recently, the concept of linking information via hyperlink has been extended towards linking knowledge represented by the Semantic Web [11]. Social Media Applications have added a new layer to this core concept of linking by connecting users and distributing content based on the behaviour users emit when consuming content. The main difference however between the WWW and Social Media Applications is that the later follows a centralized architecture which increases the effectiveness of content distribution but also limits control over the same. This shift of control furthermore increases the required trust a user has to have in the distribution mechanisms of the central platform.

This paper introduces a concept that seeks to shift the control and with it the responsibility, back to the individual user. At the centre of this approach lies the ad-hoc creation of social networks based on creating meaningful relationships within the environment of the user that are trusted. To utilize the environment effectively proximity technology is discussed, such as IoT based smart environments. Furthermore, a concept of computational trust is introduced that overlays and the user's social networks. The underlying assumption is that it is easier for an individual to trust people and objects that are proximity. In effect, this means that social media application need to go out into the wild and out of the confined centrally managed box they are sitting at the moment.

3.2 Use Case

Jane likes to make meaningful relationships and currently does not trust any social media applications to do so. To make things worse, she lately thinks that Social Media Applications are not using her personal data to add value to her own experience, but more to add value to the share price. As a stakeholder and not a shareholder, she feels her interest are not reflected appropriately. However, she does understand that she is not paying for the platform but feels the loss of control and trust is a price that is too high for her to pay. But what is the alternative? She does not want to start out fresh in a new platform, simply due to needed to reconnect all connections and in many cases, her friend connections are not on alternative networks. A friend told her about a new platform called HELIOS that is completely decentralized and which connects with people and object in her direct environment and depending on the context it automatically creates and configures each network. Jane decides to check it out. She installs it on her phone. The next morning, she wakes up and notices that HELIOS has set up a network with several IoT enabled devices in her bedroom. The network is labelled 'Bedroom'. In the kitchen, her smart fridge is added to the network, and she can see that it has been relabeled to 'home'. She likes that HELIOS dynamically changes her social networks as she moves through the day and that it also includes objects she engages with. Her neighbour rings the doorbell. She tells her that she is in a hurry and that they can talk later. Looking at the application, she notices that a new social network was established. Her neighbour does not use HELIOS yet. However, her device is broadcasting via Bluetooth allowing HELIOS to add an id to a new network. After a few minutes, she can see that the connection is decaying and that the network disappears completely. She decides to engage more with her neighbors later in the evening to ensure that a 'neighborhood' network gets established. She lives in an apartment block with a high fluctuation of tenants. She hopes that HELIOS can manage this and she won't have to manage the neighborhood network herself. She sets the broadcasting range to maximum and decides that she wants to connect with as many neighbors as possible within that specific network. In work, she attends one meeting after the other. She knows that several of her colleagues have HELIOS installed. She looks at the application and notices that it is very active. Creating new networks, plotting lines, merging, dropping etc. She feels a lot more connected already. At the end of the day, she visualized all her networks within a VR environment. In HELIOS mode she can organize all networks around her in the centre making it look like Galaxy. She notices that the line to her colleague Jack is the strongest. It makes perfect sense, Jack was in almost every meeting, and she trusted him. She was told that HELIOS uses Neuro based algorithms, which assess her direction of speech, body direction etc. Based on this it knows who to trust and who not. She remembers someone telling her that HELIOS builds something like a trust graph that overlays all her social networks. After all, she thinks, the main purpose of this app is to create social networks with trust in mind. By the end of the day, the application has established five different networks. She notices that one node (her colleague Jack) appears in two different networks. One labelled 'Work' and one labelled 'Apartment Purchase'. She remembers that she was standing in front of a real estate agents shop together with Jack who is also looking for an apartment. She likes the way HELIOS can manage Jack existing in two different networks based on his role and the context of the network.

3.3 Key Concepts

The main motivation of HELIOS is to empower trust by creating social networks that are based on environmental parameters of the user and which is completely in the control of the user yet still provides the most powerful features and advantages of current social media applications.

In the following, the different required concepts are introduced followed by a high-level architecture of the concepts.

Open Source

The base concept relies on an open source approach similar to Linux allowing the overall application to be extended towards the needs of different communities. Open Source furthermore ensures a higher level of trust due to users being able to have insight in any algorithms used to assess person data.

Decentralized Architecture and Peer-to-Peer

To ensure the user's data is protected and completely in control of the user, a decentralized architecture is proposed which resembles spontaneous ad-hoc networks [12]. This means that each network in itself is represented by a decentralized network. It has to be noted that due to the dynamics within the environment of the user, including that objects and people are not permanently in the proximity of the user, a hybrid solution is more applicable, which may include a cloud-based storage solution. Each decentralized network follows a Peer-to-Peer (P2P) network architecture [13]. This ensures a high level of privacy and control. Furthermore, P2P ensures that the storage of the data across the different networks is managed effectively. Moreover, the use of Peer-to-Peer architectures ensures a higher level of combination security based on end-to-end encryption and not needed an intermediary control server to facilitate the connection.

Content Monetization

One of the main advantages of current social media applications is the effective and highly targeted distribution of premium content via the central platform. The main drawback is that the central platform takes most of the profits as an acting intermediary. In a decentralized approach, this central 'negotiator' is not needed anymore, and brands can directly pitch content into the networks of users. For example, a social network in the context of a restaurant can allow brands to pitch content directly ensuring that the network owner and members receive all profits and do not have to share them with an intermediate broker. Technically this can be facilitated by adding a premium content distribution node to the social network. This node, which is physically a network endpoint in the proximity of the user, can then broadcast content into the network.

Ego Networks

The type of networks that get established resembles the concept of Ego Networks [14] in which the individual the centre of the social network. This concept fits in with the understanding that each creates social networks within their direct proximity naturally. The user can, if desired, create different more collaborative (non-ego) views however the initial setup always follows an ego viewpoint.

Proximity Networks

A key concept is the usage of the proximity. The underlying thinking here is to model the human brain in how it creates social networks based on assessing objects and people nearby. The technical implementation follows the concept behind Near-field Communication (NFC) and Bluetooth. The user's device constantly broadcasts readiness for connection and connects with other devices that do the same. Different to Bluetooth the connection gets established automatically and resembles a person with high openness for social connections. However, similar to the brain they are not stable networks and only establish permanence if engaged with. By utilizing the environment of the user to create social networks the context and intention of each social network are implicitly given. This ensures automatic labelling and configuration of the created social network.

By using Mixed and Virtual Reality technology, the concept of proximity can be extended towards including objects and people that are not in the direct physical proximity of the individual. For this, the objects and people are virtually 'beamed' into the proximity of the user to enable social network creation.

Finally, large-scale proximity has to be considered, such as sports events in which the proximity is highly overcrowded. The result would be a highly fluctuating network. However, it can be useful to create or be added to large-scale proximity networks to facilitate the broadcasting of messages that are based on the context of the established network. A useful example of this is in a crisis in which receiving or sending information can be lifesaving. A chain reaction function would ensure that the established network can also use the proximity of others network members facilitating a rapid adoption of connections that are in the same context.

Context Detection and Smart Environments

Context detection is vital for the usability of the application. Only by auto-creating and auto-configuring of the networks large-scale adoption and usage is possible. The key to this is the usage of Context facilitated by the environment of the individual. For this smart environment, technology can be used, such as smart homes, smart devices, smart cars etc. Each Internet-of-Things (IoT) device and or Smart Environment broadcasts the context simply by indicating what it is. Therefore, the context is implicit and can be gained based on the behaviour of the user around that context. An example is a lunch in a conference centre at a table with is IoT enabled. The table becomes part of the ad-hoc network that forms around the table. The table itself informs the application that it is a table in a conference centre and can seat four people. This information ensures the correct contextualization of the ad-hoc network, in this case with a label 'Business'.

Trust Graph

The usage of a trust graph ensures each social network follows a 'Trust by Design' principle. The main approach is to establish computational trust by enabling a trust value towards each new element within a social network [15]. This empowers the user to assess what elements to trust. To compute trust, different approaches are envisaged. The main approach relies on Neurotechnology that is used to train Neural Networks trained. The main markers used are speech direction and duration, the tone of speech, neuro activity (e.g. via Neuroimaging) [16]. The result is a trust graph in each social network that overlays each social network. The trust graph informs the social graph about the trustworthiness of each element in the network. Considering that the trust values towards each element can change significantly throughout the lifetime of the network, it is possible that elements are completely deleted or their connections are made close to permanent (for example towards family members within a 'Family' context network).

Social Network Evolution (Strengthen, Decay and Deletion)

Each social network is modelled based on how the human brain creates a social network. Therefore, similar to how neurotransmitters use receptors to connect two neurons and based on the activity either strengthened, weakens or destroys the neuronal connection. Technically this is implemented as a decay factor which after a certain (personal and contextual) threshold deletes the node and the entire network. Similar to highly memorable connections for the human brain, it is possible to set connections to permanent (e.g. for family members). The key concept behind this is the Trust Graph which provides the updated trust value for each connection.

3.4 Design and Architecture

Below, three diagrams are introduced. The first (Figure 1) illustrates the temporal nature of HELIOS as the user moves through space and time. The second (Figure 2) is a high-level illustration of the user's view of the created networks. The third (Figure 3) and final diagram is a high-level architectural overview of the HELIOS.

Temporal User Flow Diagram

The user flow is a high-level illustration of the user moving through the day. Two major aspects have to be considered. The first is that an individual in modern day society plays different roles depending on the time of day and the space the individual is moving in. These roles can include being a husband, a father, a colleague, a friend or team member in the local soccer team etc. It can be argued that an individual holds certain responsibilities and intentions in each role. HELIOS can infer these roles and the corresponding intentions and responsibilities based on what time

and in what space the user currently is. The temporal dimension, therefore, helps support the application to understand where the user currently is (e.g. in work) and therefore reduces the dependency on proximity. The second aspect relates to the space dimension through which the user is moving on a regular base (e.g. the path towards home). Together space and time create 2-dimensional contextual markers that help the assessment of trust by assuming a car used many times is a car that is trusted. Depending on the context the Time and Space viewpoint can be extended towards trusted individuals that enable transactional trust (e.g. I trust the car because my wife uses it every day).

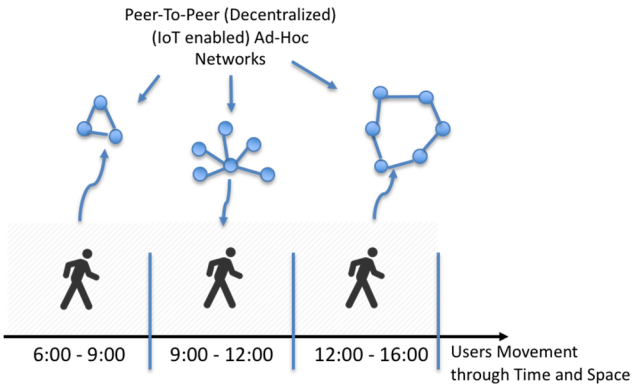

Figure 1 User Flow through Time and Space

User Viewpoint (Helios Mode)

The visualization and management of the user's social networks is a key element of the overall approach. The simplified visualization (Figure 2) illustrates networks that consist of objects and individuals. The thickness of each line between the networks indicates the strength of the connection. In cases in which the trust value drops under a certain threshold, the connection may cap, and the element gets deleted. Overall this approach follows the human brain in its ability to forgets connections if they are not fresh or updated. Content nodes represent a more abstract concept of connecting to content distribution points that enable monetization of premium content within the user's network. An example of where content distribution points are used is in a social context such as a bar or pubs. Here, a beverage brand can pitch premium content and pay the network owner directly (e.g. via Cryptocurrency) without any necessary intermediary.

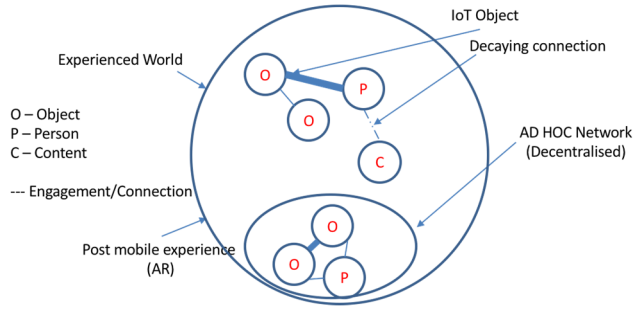

Figure 2 User Network Point o View HELIOS mode

High Level Architectural Overview

The architecture diagram (Figure 3) illustrates the different architectural elements of a decentralized ad-hoc social network. Four layers are introduced. The first layer is the Discovery Layer. It plays a vital role in discovering different elements to connect to (e.g. Objects, People and Content). It is important to note that discoverability is purely based on device based connections. This layer, however, does not specifically care what the device is, as long as it represents something that is useful for a social network. For example, discovery can relate mobile and wearable devices to individuals, objects to locations and content points to brands and organization. This concept resembles Bluetooth, however, does not require explicit pairing. The pairing is performed implicitly via the trust management component within the management layer. The second layer is the Interface Layer. It ensures that the discovered elements are qualified. It, therefore, serves as a quality filter ensuring that elements in the environment that are not valid are not passed on for processing (e.g. introducing fake content endpoints to create a man-in-the-middle attack). To avoid this, the Interface layer can assess context, connection and content based on what type of elements the user tends to trust. The management layer, as the third layer in the architecture, manages the actual creation and management of the ad-hoc networks. A key role for this is played by the trust management component. This component has to be trained based on the individual user's perception of trust. The main task of the trust component is a permanent assessment of all connections over all networks the user has. The network management and configuration component use the trust graph to strengthen or decay connection. In cases in which a predefined threshold is passed the node or network gets deleted. The network configuration component is furthermore responsible for the labelling of networks based on context and unification or splitting of networks. It, therefore, forms a core component that resembles strategies that are used by the human brain to manage social contacts in the individual's environment based on trust assessment. The network management component allows the user to explicitly manage the different networks. Finally, the storage layer ensures that all information is securely stored. This can be purely P2P or via a hybrid cloud approach depending on the user's configuration. This relates to interfacing with external services such as via the web or APIs, or by collaborating with other services (collaboration component) such as to other social networks and Visualization interfaces.

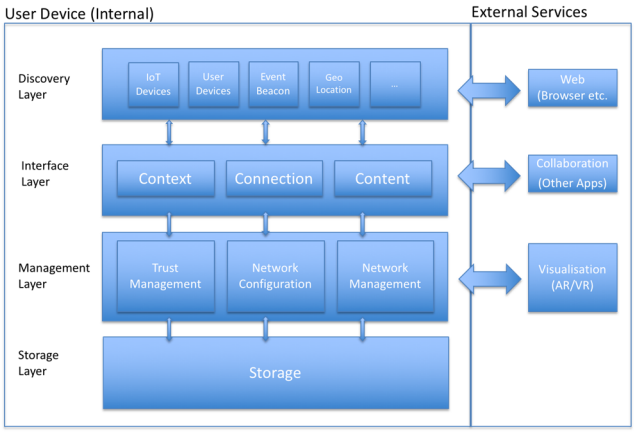

Figure 3 High Level Architecture of HELIOS

3.5 Other Challenges

Establishing a new social network approach is typically prone to many challenges. The most prominent example is Google Circles (i.e. Google Plus) which, despite heavy investment and a focus on user experience has not reached critical adoption. The main concept of Google Plus is to organize the overall social graph of the user into different Circles of Context which resembles the HELIOS approach introduced in this paper. However, Google Plus requires the user to do this configuration and is not based on using smart environment and proximity to auto create and configure the networks. It can be argued that the time and knowledge required to configure and manage social network applications, not only Google Plus but also other social network applications, is one of the reasons of failing to reach mass adoption. The second reason is adoption itself. A new social network tends to be empty which creates the feeling of an empty room. HELIOS seeks to overcome this by focusing on proximity. However, the main challenge lies in the discovery layer. It is yet to be seen how modern devices can provide more open yet controllable discoverability in the direct proximity of the user. This challenge might be overcome throughout the beyond mobile era in which wearable devices, such as mixed reality glasses are seen to become mainstream. Based on visual clues the discovery layer can be simplified significantly. Furthermore, the concept of trust introduced as a computational trust graph needs to be researched further. The main challenge in this context is the highly individual nature of trust, and even with modern day neuro informed technology, it remains questionable if deeper levels of trust can be assessed and utilized (e.g. gut feeling). Finally, P2P facilitating decentralization introduces destabilizing elements into social networks. For example, devices can be switched off or entire areas blocked out of the network.

4 CONCLUSIONS

This paper introduces HELIOS a novel approach to addressing current challenges within the social media application space (e.g. Fake News, Filter Bubbles and Fake News). The current challenges of Social Media Applications are discussed, and HELIOS is presented as a possible solution by introducing a 'Trust By Design' concept to Social Media application development. This includes an architecture that the user can trust, based on deep levels of control and transparency. Furthermore, decentralization via P2P, computation trust and the usage of a smart environment is introduced. Current development such as the 'Right to be Forgotten' legislation [9] and GDPR within the European Union point to an increased desire for increasing the user's influence over the personal data collected by Social Media Applications. By adopting elements of HELIOS, it can be argued that the user gains a significantly higher level of control and freedom yet still has access to powerful features of modern day social media applications (such as direct communication, status updates, sharing photos, content commercialization etc.). A further aspect not discussed in this paper is the notion of authenticity and memory. Both aspects relate to how the individual uses social media applications. In relation to authenticity, the presentation of the user is often staged or dramaturgically orchestrated as a journey or narrative of the user and can tend to misrepresent the actual reality of the user [17]. A trust-based platform, such as HELIOS, limits the ability to create fake or distorted representation of the individual. Based on its 'Trust by Design' principle, it strongly relies on authenticity and disqualifies fake or unauthentic representation. In relation to memory, it has to be noted that many social media networks are used as the album to look back to over time. A strongly decentralized network, such as HELIOS, which can delete nodes and network under certain conditions reduces the memory effect for the user.

In order to avoid a Black Mirror like scenario for Social Media Applications (e.g. Government takeover, social scoring censorship, user blocking etc.), HELIOS introduces a novel decentralization and highly contextual aware approach that is difficult if not impossible to be exploited by third parties and therefore resembles design paradigms followed by the WWW (e.g. decentralization) and Blockchain (e.g. protection and democratization of personal social network data).

5 FUTURE WORK

To validate the usefulness and effectiveness of HELIOS a serious of evaluations are required that are mainly focused on semi-automatic trust assessment. This research, which includes Neurological research and Machine Learning, ensures the creation of a computation trust graph for trust-based social networks. Furthermore, more basic evaluations in the form of surveys, are currently being executed. These surveys focus on the individuals explicitly perceived trust towards other users within their existing social networks. Preliminary results indicate that over 75% of the questioned users would only trust 25% of their existing social network connections with 50 Euros. Finally, it has to be noted, that establishing HELIOS as a widely used approach to Social Networking requires significant investments from state level similar to what was required for the creation of the WWW or the internet.

ACKNOWLEDGMENTS

This work is supported by the ADAPT Centre for Digital Content Technology, which is funded under the Science Foundation Ireland Research Centres Programme (Grant 13/RC/2106) and is co-funded under the European Regional Development Fund.

REFERENCES

[1] Diakopoulos, Nicholas, Mor Naaman, and Funda Kivran-Swaine. "Diamonds in the rough: Social media visual analytics for journalistic inquiry." Visual Analytics Science and Technology (VAST), 2010 IEEE Symposium on . IEEE, 2010.
[2] Pariser, Eli. The filter bubble: What the Internet is hiding from you. Penguin UK, 2011.
[3] Allcott, Hunt, and Matthew Gentzkow. Social media and fake news in the 2016 election. No. w23089. National Bureau of Economic Research, 2017.
[4] Borden, Sandra L., and Chad Tew. "The role of journalist and the performance of journalism: Ethical lessons from "fake" news (seriously)." Journal of Mass Media Ethics 22.4 (2007): 300-314.
[5] Jasny, Lorien, Joseph Waggle, and Dana R. Fisher. "An empirical examination of echo chambers in US climate policy networks." Nature Climate Change 5.8 (2015): 782-786.
[6] Jasny, Lorien, Joseph Waggle, and Dana R. Fisher. "An empirical examination of echo chambers in US climate policy networks." Nature Climate Change 5.8 (2015): 782-786.
[7] Cao, Qiang, et al. "Aiding the detection of fake accounts in large scale social online services." Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation. USENIX Association, 2012.
[8] https://www.theguardian.com/media/2017/sep/30/social-media-companies-fake-news-us-election [last opened 10/02/2018]
[9] Rosen, Jeffrey. "The right to be forgotten." Stan. L. Rev. Online 64 (2011): 88.
[10] https://obamawhitehouse.archives.gov/blog/2015/02/06/economics-big-data-and-differential-pricing [last opened 10/02/2018]
[11] Berners-Lee, Tim, James Hendler, and Ora Lassila. "The semantic web." Scientific american 284.5 (2001): 34-43.]
[12] Wu, Jie, and Ivan Stojmenovic. "Ad hoc networks." Computer 37.2 (2004): 29-31.
[13] Fox, Geoffrey. "Peer-to-peer networks." Computing in Science & Engineering 3.3 (2001): 75-77.
[14] Leskovec, Jure, and Julian J. Mcauley. "Learning to discover social circles in ego networks." Advances in neural information processing systems. 2012.
[15] Sabater, Jordi, and Carles Sierra. "Review on computational trust and reputation models." Artificial intelligence review 24.1 (2005): 33-60
[16] Haynes, John-Dylan, and Geraint Rees. "Neuroimaging: decoding mental states from brain activity in humans." Nature Reviews Neuroscience 7.7 (2006): 523.
[17] Goffman, Erving. "The presentation of self." Life as theater: A dramaturgical sourcebook (2006)]