THE INTERNET: 
A BRIEF HISTORY BASED ON TRUST

Internet: kratka istorija sagledana kroz faktore poverenja

ABSTRACT: In this paper, we use trust as an interpretive lens through which we consider a set of challenges that remain crucial across decades and socio-technical phases of Internet development. Looking through this particular lens highlights several specific factors, which have persisted throughout the history of the Internet and are amplified in today's environment: identity, privacy, and collective online social action. We examine these factors in a diachronic perspective, comparing attitudes dominant in the 1990s with the attitudes dominant today. We argue that the socio-technical environment of the Internet has become so complex that our established ways and resources for making trust decisions are no longer adequate. In such circumstances, trust decisions increasingly become a collaborative effort between the user and a set of outside institutional actors. Yet, assisting users in navigating the progressively complex web of online interactions with human and nonhuman actors can easily turn into a detrimental level of institutional control, with “unsupervised users” perceived as potential victims of untrustworthy Internet sources. Trust thus becomes one of the key driving forces of Internet development and regulation, significantly redefining the relationships between individuals and institutions, and further destabilizing aspects of Internet trust analyzed in this paper.

KEY WORDS: Internet; trust; identity; privacy; collective social action

APSTRAKT: U ovom radu koncept poverenja koristi se kao interpretativna prizma kroz koju se posmatraju tri faktora internet komunikacije koji opstaju kao ključni tokom različitih faza razvoja globalne mreže, i koji su posebno naglašeni u današnjem internet okruženju. Ti faktori su identitet, privatnost, i kolektivna društvena akcija. Uporedjujući primere i pomanja ova tri faktora dominantne tokom 1990s sa onima koja preovladjuju danas, rad pokazuje da je internet

1 smiljana@id.iit.edu
2 gurakl@umn.edu
postao do te mere složeno društveno-tehnološko okruženja da utvrdjeni obrasci za uspostavljanje poverenja više nisu adekvatni. Usled toga, odluke o toke kome i čemu da (ne)veruju na internetu korisnici sve više donose u delimično dobrovoljnoj, a delimično nametnutoj saradnji sa nizom institucija. Takva saradnja, medjutim, lako se pretvara u institucionalnu kontrolu gde su “korisnici bez nadzora” viđeni kao lake žrtve internet aktera koji su označeni kao nepouzdan i opasni. Poverenje tako postaje jedan od ključnih pokretača u razvoju i regulaciji interneta, značajno redefinišući odnose izmedju pojedinaca i institucija, te dodatno destabilizujući faktore internet komunikacije analizirane u ovom radu.

KLJUČNE REČI: Internet; poverenje; identitet; privatnost; kolektivna društvena akcija

Introduction

On September 17, 2019, Edward Snowden's memoir, *Permanent Record*, was published for the first time. Two days later, an electronic copy of the book was already available on Library Genesis. A colleague, let's call him Tom, downloaded it. The permanent record of that download was added to Tom's digital dossier—an impersonally collected personal history that makes Bucky Fuller’s *Dymaxion Chronofile* seem despondently slim.

This simple act of downloading a copy of the electronic book included a set of trust decisions Tom needed to make. First, he decided to follow one of the obscure and constantly changing web links that would take him to Library Genesis. This web source has been on the run through the online wastelands, constantly changing its Top Level Domain (TLD) names and adding numerous proxy and mirror websites, as to enable users to access it despite Internet service providers' (ISP) blocks. Library Genesis found itself in the company of pornographic, pedophile, gambling and similar websites, which are blocked at the ISP level, after two powerful academic publishers, Elsevier and Springer, filed legal suits against it for the infringement of intellectual property (IP) rights.

Second, Tom decided to use a personal computer instead of the work one. His work computer automatically blocked his access to Library Genesis, warning him of security risks. Those risks were portrayed as attackers lurking behind Library Genesis to steal Tom's password and/or credit card information. Capitalized red-letters, as well as prominently placed red exclamation marks, vigorously warned Tom of such risks, although Library Genesis does not ask users to sign in or to buy anything, using a credit card or other payment method. Tom’s computer still warned him about existent and nonexistent risks, telling him to “go back to safety,” and hesitantly offering to allow him to get to Library Genesis only if Tom explicitly selected to “accept the risk” of accessing it.

---

3 Such as https://libgen.unblocked.cab/, http://www.websiteproxy2.com/proxy/libgen, etc.
4 Library Genesis provides “opened access” to millions of copyrighted academic books and journal articles free of charge, so authors like Bodo (2018) observe that “its democratic approach to access is matched by an elitist approach to content” (p. 28).
Next, Tom decided to download a book from the web source sometimes assessed as dangerous just to visit, let alone to use as a source of materials. Those dangers have not been associated with known or suspected cases of malware, but rather with the risk of facing legal consequences for illegal access to copyrighted materials (Himmelstein et al., 2018), which, although theoretically possible, have not been documented with regard to Library Genesis. Public scholarly discussions of risks associated with this Internet source thus primarily swirled around reputational risks—is illegal access to copyrighted materials unethical, and, if so, is a scholar engaged in such acts at risk of reputational damage? Juxtaposed with academic publishers’ exuberantly high profit margins, as well as with both moral appeals and formal requirements for open access to scholarly work (see, for example, the U.S. National Science Foundation’s Public Access Policy), such discussions never got serious traction, but they did increase awareness of leaving “dangerous” digital traces, especially when using library workstations.

This step leads to the final decision Tom needed to make, which brings us full circle back to permanent records. Short of using a Virtual Private Network (VPN), downloading Snowden’s book from Library Genesis left a permanent digital trace of Tom’s illegal access to copyrighted material. Moreover, it put him at specific double reputational jeopardy, serving as a digital testimony of Tom’s interest in controversial material. Written by a person simultaneously hailed as a brave whistleblower and denounced as a cowardly spy, Permanent Record faced legal charges on the first day of publication, when the U.S. Department of Justice filed a civil lawsuit against Snowden for violating the non-disclosure agreement with the CIA and the NSA.

This story illustrates the complex nature of trust and trust relationships between people and the Internet. In specific, this and millions of other online interactions require what Möllering (2001), expanding on work by Simmel, describes as taking a “leap of trust.” Later, we will discuss Möllering’s stages of this process, which provide a helpful framework for viewing the past, present, and future Internet. But for now, suffice it to say that online, we take those leaps regularly, rapidly, and with little to no thought. As we mentioned above, a simple act of downloading an electronic copy of a book requires a leap of trust, that is, an assessment that “the repository can be trusted because it has been deemed an appropriate place ... from which content can be retrieved” (Prieto, 2009, p. 596).

In this paper, we look at trust decisions related to three aspects of Internet trust: identity, privacy, and collective social action. Following the focus of this special issue of Sociologija, we examine these three aspects in a diachronic perspective, comparing attitudes towards identity, privacy, and collective social action dominant in the 1990s with the attitudes dominant today. It is beyond the scope of this paper to examine the complex framework of sociological, psychological, and anthropological theories of trust, or to delve into all of the many details of the rich and multifaceted topic of Internet and trust. Rather, we focus on a few underlying conceptions of trust, using them as an interpretive lens through which we can consider a set of challenges that remain crucial across decades and socio-technical phases of Internet development. We argue that the socio-technical environment of the Internet has become so complex
that our established ways and resources for making trust decisions are no longer adequate. In such circumstances, trust decisions increasingly become a collaborative effort between the user and a set of outside actors. The latest stage of Internet development thus significantly redefines the relationships between individuals and institutions, and trust appears as one of the key driving forces of Internet development and regulation.

**Trust, its functions, and the Internet**

Like the Internet, trust is a broad, deep topic not easy to define quickly or out of context. Perhaps the best general description comes from the sociologist Niklas Luhmann, who reminds us that trust is a central component of our lives. Without trust, we could not function as individuals, and we would not have functioning social and civic systems. As he states in his classic treatise on this topic, “[t]rust, in the broadest sense of confidence in one’s expectations, is a basic fact of social life. . . . a complete absence of trust would prevent [a person] from even getting up in the morning” (Luhmann, 1979: 4). Or, described more closely in relation to trust and human interactions, “[t]he existence of trust is an essential component of all enduring social relationships” (Seligman, 2000: 13). Yet by what means does trust operate?

Trust, as well as mistrust, depends on several factors, but at the most general level trust is established via repeated interactions, during which individuals become increasingly confident in the outcome of similar interactions. Or, as Luhmann states, “to show trust is to anticipate the future. It is to behave as though the future were certain” (Op.cit., p.10). Empirical research confirms this premise, demonstrating that personality traits, such as propensity to trust, have a much stronger impact in unfamiliar than in familiar interactions (Alercon et al., 2016; Freitag and Bauer, 2016). Seligman (Op.cit.) also notes the close relationship between trust and confidence, describing confidence as “[an] intermediate between knowledge and ignorance” which constitutes the very essence of trust (p. 318). In Seligman’s view, the states of complete knowledge, as well as complete ignorance, eliminate the need for trust, which arises exactly at the intersection of the known, the unknown, and the unknowable. Luhmann’s (Op.cit.) understanding of trust as “blending of knowledge and ignorance” (p. 26) is related to this premise, as is Lewis and Weigert’s (1985) interpretation of trust as “a mix of feelings and rational thinking” (p. 972).

Möllering (Op.cit.) develops further this approach to trust in a way that is highly relevant to the Internet. He introduces the concepts of interpretation, suspension, and expectation to form a dynamic model of the trust process. In this model, one’s interpretation is the input and the starting point in the trust process, which, as Möllering notes, cannot begin nowhere or anywhere, but “from one of the places where interpretation leads us but whose suitability cannot be completely certain” (p. 414). (Again, the starting point of the trust process is blending of knowledge and ignorance, as Luhmann puts it.) This blending introduces the need for the second concept in Möllering’s model—suspension—which he considers the key aspect of trust. Suspension refers to the
process of temporarily bracketing out, or suspending, ignorance, uncertainty, and contradictions as to enable the input of interpretation (interpretative knowledge, as Möllering calls it) to become “momentarily certain,” and thus serve as a starting point from which the leap of trust moves to its destination—expectation. Expectation, then, is not the beginning, but the end point, that is, “the state reached at the end of the trust process and which can be either favorable (in the case of trust) or unfavorable (distrust)” (p. 417).

In this regard, trust helps reduce complexity by providing a kind of “confidence reliance” between an “outer threshold of deceit and an inner threshold of confidence reliance” (Frederiksen, 2012: 733). Or, stated differently, the function of trust is to reduce complexity by creating a context in which a certain situation, interaction, or piece of information can be accepted “as if certain rationally possible futures will not occur” (Lewis and Weigert, 1985: 969, cited in Möllering, 2001: 410; emphasis in the original). Furthermore, when a leap of trust must be taken quickly, without the benefit of very much time, we engage in trust transfers, where the burden of establishing trust is transferred to external proof sources, often based on the reputation and trust we have in others (Stewart, 2003). These “others” might be friends, family, institutions, online communities, Web sites, and so forth. This phenomenon is particularly relevant for Internet communication.

Communication, whether face-to-face or mediated by technology, dyadic or in groups, is the basis for how we build trustworthy, durable relationships. For millennia, this communication took place with our bodies: via gestures, facial expressions, sounds, movements, and eventually, through spoken language. Later, writing and its technologies (stone tablets, papyrus scrolls, the printing press, the telegraph, the Internet) supplemented and in some cases supplanted earlier forms, creating new opportunities for trust as well as distrust. In particular, the shift from trust between people to trust in organizations to trust in algorithms requires us to take a more nuanced perspective when considering trust online.

Factors of Internet trust

As described above, trust is a complicated relationship involving many factors, with most factors related in some way to how and why people decide to move forward with the transaction or situation (Möllering’s “suspension” and “leap”). Viewing the history of the Internet through this particular lens brings to light several specific factors, which have persisted throughout the history of the Internet and are amplified in today’s environment. These factors are identity, privacy, and collective online social action.

Identity

Identity has been a key construct in Internet communication since the outset. A discussion of identity naturally leads to discussions of anonymity and pseudonymity as well. As far back as the 1980s (the “pre-web” days), van
Gelder (1985) described a deep betrayal of trust when a male psychiatrist in a CompuServe network forum was caught posing as a disabled woman. The sense of betrayal emerged as particularly strong because users of CompuServe perceived themselves as “a utopian community of the future” whose members are committed to “some new, truer way of relating” (p. 3). In other words, their interpretation of CompuServe as a utopian community led to the expectation that interactions among members of that community would be truthful, despite—or rather thanks to—the ignorance occasioning their “real life” identities.

Such idealized views of online interaction were relatively common throughout the 1990s; trust in online interactions was high, in part because Internet users at that time were a relatively homogeneous group. Yet, as Internet use expanded beyond its initial demographic base, questions about authenticity and the risks of online interactions arose. Two landmark works—Rheingold’s *Virtual Community* (1993) and Dibbell’s “Rape in Cyberspace” (1998)—examined online identity, social interaction, and trust from opposite sides. While Rheingold praised virtual communities as “meetings of the mind” where people can relate to each other in deeper and more authentic ways, Dibbell pointed at examples of deceitful online behavior of individuals misusing technology to trick and victimize users by assuming fake online identities.

In those early cases, and ongoing to this day, we are reminded that “[t]rust, then, is the generalized expectation that the other will handle his . . . potential for diverse action, in keeping with his personality—or, rather, *in keeping with the personality which he has presented and made socially visible*” (Luhmann, 1979: 39; emphasis added). Over time it has become clear that a socially visible Internet personality may have no relation whatsoever to the actual person or organization behind the message. In fact, most recent technological developments, such as social bots, illustrate that a socially visible personality might be unrelated to any human actor, building instead a recognizable online identity based on the input from automated software that mimics the behavior of human Internet users (Larsson and Moe, 2015).

If in the early Internet days users could not be sure whether a person they communicated with was male or a female (as illustrated in the Van Gelder piece), today users cannot be sure whether their online interlocutor is a person at all. Programmed to autonomously create content and interact with humans by emulating human behavior, social bots have become so advanced and sophisticated that the majority of people cannot distinguish them from humans (Wojcik et. al, 2018). In parallel, social bots have come to occupy huge portions of Internet traffic—40% of all online traffic in 2019, which is twice the percentage of bot online activity in 2018. On Twitter alone, 66% of all tweeted links to popular websites were shared by bots rather than humans (Ibid.).

Deepfakes⁵ have also become so sophisticated that the only way to differentiate them from authentic identities and recordings is to retreat to the primordial way of assessing trustworthiness—through the analysis of  

---

⁵ Deepfakes use AI to map one person’s image and voice onto another person, thus creating fake videos that appear genuine.
nonverbal communication. Namely, in dyadic interaction reliance on nonverbal cues increases accuracy in assessing the trustworthiness of another person by whooping 37% (De Steno et al., 2012). Computer analysis of video materials similarly analyses minute nonverbal cues to detect whether a particular recording of a person is authentic or a deepfake (Agarwal et al., 2019). Such examples show that the issues of identity and trust in social interaction assume completely new dimensions in the age of artificial intelligence, bringing a crucial shift to the entire trust process, from establishing certain interpretation as a starting point, over deciding what kind of ignorance to temporarily suspend, to arriving to the positive or negative expectation.

**Privacy**

As the Internet evolved, issues of identity and anonymity brought with them an increasing concern about online privacy. During the late 1980s, a group of computer scientists and programmers, inspired in part by science fiction (cyberpunk) works such as that of Vinge (1981), started the cyberpunk movement, promoting the values of encryption, privacy, and anonymity.6 Their activism became the basis for what many consider the defining motto of the information age, “information wants to be free;” or, in their founding manifesto, “the practical freedom to read and write what one wishes to” (May, 1992). Freedom of speech and free exchange of information were considered among the highest values, and strong encryption was perceived as a trusted way to provide personal privacy and anonymity in an era of increased surveillance.

Yet today, 27 years after May’s Manifesto, mass-scale data collection without users’ explicit consent abounds in what has been characterized as “surveillance capitalism” (Zuboff, 2018). This phenomenon is due not only to algorithms that collect our every click and view on every online site but also, in large part, to users’ conscious decisions to relinquish their privacy in ways unimaginable in the early Internet days. In this regard, privacy is one the factors of Internet trust that shifted most extremely over the past decades. Throughout the 1990s, sharing personal experiences and feelings was mostly contained within virtual communities of trust, where a communal identity of “a thousand aunts with modems” (Weise, 1996) who help newcomers adjust to the city was more important than individual profiles of any of the “aunts.” In these settings, users regularly made leaps of trust about what to say, and to whom, feeling as if the Internet was a safe space populated with others of similar values.

Anonymity and privacy were thus embraced as distinctive qualities of Internet communication considered to enable more sincere and spontaneous social interaction. Fast-forward to 2019, where being unknown online has largely transformed from a cherished value to a feared failure. Today, Internet success is measured as the constantly increasing number of views, followers,

---

6 More than thirty years ago they formulated some of the concepts most relevant in Internet discussions today—cryptocurrency, such as Bitcoin, file sharing via encrypted online dropboxes, such as WikiLeaks, and so on.
likes, comments and similar tokens of value in the economy of online attention. If the method of winning online attention presumes broadcasting oneself on YouTube while sleeping or giving birth, thus entrusting the most intimate and private experiences to millions of random online users interested in watching, so be it (Longhurst, 2009).

Collective online social action

The examples above are closely related to a third factor of Internet trust examined in this paper, namely trust in collective online social action. Today, people share all kinds of personal information via social media apps and gather around “Broadcast Yourself on YouTube” communities to voluntarily breach their own and other users’ privacy. But in the 1990s, concerns about online privacy motivated a group of users to organize and ultimately stop the release of a product called Lotus MarketPlace, in what is now recognized at the first collective online social action. Lotus Corporation (maker of the first spreadsheet software) created a product called “Marketplace Households,” which was supposed to provide (via a CD for purchase) the names, addresses, and spending habits of over 120 million U.S. consumers. When word got out about Marketplace, a group of privacy advocates used the available apps of that time (Usenet news and email) to rally others to the cause. As a result of this online protest, more than 30,000 people contacted Lotus and asked that their names be removed from the database (Gurak, 1997). The speed and reach with which these messages reached the company took management by surprise; the company ended up canceling the product before it was ever released. Trust in the capacity of online social action was clearly exhibited in this case, which took place well before the Web and social media and foreshadowed a trend that exploded with the development of Web 2.0 and apps such as Twitter, Yelp, Facebook, and so forth.

The introduction of Web 2.0 platforms in the early 2000s was hailed as an example of user empowerment, promoting the idea that regular people could control the Information Age. Collective social action exemplified in different forms of participatory knowledge production, from Wikipedia to citizen journalism to folksonomies, was lauded for its potential to democratize knowledge by transforming static knowledge authorities into dynamic and multisided knowledge platforms that engage the public as acknowledged knowledge providers. The role of “Facebook revolution” and citizen journalism in the so-called Arab spring (2010–2012) was seen as a historic example of crowdsourcing in influencing social change and disrupting political regimes. In the domain of cultural heritage, some of the most prestigious museums, such as the Metropolitan Museum of Art and the Guggenheim Museum, created a collaborative platform for social tagging, entrusting “naïve users” to provide descriptions and interpretations of museum collections (Trant, 2009). Wikileaks and Julian Assange were lauded as a new

---

7 Best illustrated in the Time magazine cover from December 2006, which asserted that “You [the Internet user] control the Information Age” (see: http://content.time.com/time/ covers/0,16641,20061225,00.html)
form of trustworthy reporting receiving Amnesty International Media Award in 2009 as “an invaluable resource for anonymous whistleblowers and investigative journalists” (Index on Censorship, 2008).

Fast forward ten years, and Facebook is undergoing a set of U.S. Congressional hearings for “undermining US democracy;” citizen journalism is labeled as “fake news;” Wikileaks’ Chelsea Manning and Julian Assange are imprisoned and facing US Department of Justice indictment for alleged computer intrusion. The change could hardly be more apparent and significant. And while each of these cases could be, and has been, a subject of an entire dedicated analysis, we want to focus here on how crowdsourcing and collective social action reformulated trust decisions in Internet communication. Most significantly, Web 2.0 applications and collective user actions began to rapidly disrupt traditional notions and institutions of expertise, redefining our trust relations with those institutions. From medicine to politics to science, individuals started turning to the Internet, where all information appears to be created equally, and all forms of expertise appear to merit equal consideration. For instance, it is not uncommon for people to dismiss entirely a doctor’s advice based on conflicting advice online; as two examples, consider the anti-vaccination movement (Brownlie & Howson, 2005) as well as the use of crowdsourced medical information sites (Bakke, 2015). A key strategy of this movement is to incite distrust in the traditional medical community through proliferation of personal stories and conspiracy theories, websites devoted to “alternative” interpretations of scientific data, and the promotion of alternative treatments, medications, and educational materials (Hoffman et al., 2019; Yiannakoulias et al., 2019). An accompanying strategy is the (mis)use of crowdsourced review forums, such as Yelp, with coordinated activities of posting negative reviews of doctors and medical institutions assessed as “pro-vaccine.” The influence of online anti-vaccine movement has been so significant that the World Health Organization declared vaccine hesitancy one of the top-ten threats to global health in 2019.

Such success in provoking mistrust towards the official medical community can be seen as part of the broader erosion of trust in official and expert organizations, from government to media. A recent study of the Pew Research Center found that staggering “two-thirds (69%) of Americans say the federal government intentionally withholds important information from the public that it could safely release, and about six-in-ten (61%) say the news media intentionally ignores stories that are important to the public.” (Rainie et al., 2019). This finding demonstrates the increasing insecurity about whom and how to trust.

Returning to Seligman and Luhmann, it is important to remember that trust requires a blend of knowledge and ignorance, of certainty and uncertainty, so that a trust decision could be made either through a direct leap of trust or through a trust transfer. Official and expert organizations commonly serve as outside proof sources to which the burden of establishing trust can be transferred, because they provide a balance between knowledge and ignorance necessary for the trust process. In other words, when we do not have knowledge needed to make
certain trust decisions, we traditionally rely on experts (such as news media or our doctor) to provide us with that knowledge. When the trust we place in such sources erode, supplanted by a shifting sense that anyone can be an expert, the result is diminished capacity to arrive to a destination of the trust process—a reasonably reliable positive (trust) or negative (distrust) expectation.

This phenomenon is particularly visible in the political arena, where “fake news” and deliberate spreading of misinformation online gained such wide traction that entire government and corporate units have been formed to address those issues—from Google’s $300 million News Initiative that asserts to help news organizations debunk misinformation to the European Union’s anti-disinformation action plan ostentatiously titled “Europe that Protects” to the United States Census Bureau’s most recent partnership with Facebook, Twitter, and Google to fight potential misinformation ahead of the U.S. 2020 election. This factor of Internet trust is another parameter that has shifted most dramatically over the past twenty years, creating, in combination with other factors examined here, a set of changes summarized in the next and concluding section of this paper.

Conclusion

Looking at the Internet through the lens of changing attitudes towards trust portrays the early Internet and Internet of today as worlds apart. Yet, it is not a picture of “digital natives” versus “digital immigrants,” such as the one depicted in Palfrey and Gasser’s (2008) study. Such narratives suggest an idea of early Internet days and users as ignorant settlers clumsily trying to navigate an unknown world. This picture is contrasted with a depiction of Internet users in the 21st century as wizards who are skillfully and effortlessly navigating the online world, actively shaping it in the socio-technical environment of their choosing, and letting crowdsourcing sort out truth from fiction. But such a vision is very far removed from the truth. Early Internet users were often computer experts carefully attuned to both the possibilities and risks of digital technologies, capable and willing to initiate changes that they found needed, as we saw in the 1990 case of Lotus Marketplace. The capacity of those early users to identify the most significant risks of Internet development, such as mass surveillance and loss of privacy, shows the maturity of thinking about the digital not always readily found among contemporary users.

One such risk that early online “pioneers” warned about was institutional and governmental control over the Internet. Indeed, while the early Internet days brought redefinitions of the relationship between individuals and communities, primarily based on the wide reach of Internet communication irrespective of geographical distance, the latest stage of Internet development has brought to the forefront redefinitions of the relationships between individuals and institutions. Compare the opening of Barlow’s (1996) “Declaration of the Independence of Cyberspace” with today’s contemporary context. In the Declaration, Barlow addresses governments of the industrial world by saying “you weary giants of
flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.” Yet, in the 21st century, governments and corporations not only hold almost complete sovereignty over the Internet infrastructure, but also have an increasingly tighter control over users’ individual online interactions. Facebook “assists” users to nurture social relations by algorithmically selecting which post from which of her contacts a user should see. Google “assists” users to weed out irrelevant information by deciding which of his search results the user will encounter first. The EU “assists” its citizens from falling victims to manipulation by determining which information sources they should and should not be able to consult.

This storyline suggests a view of individual users as unable to control “threats of technology” and make informed trust decisions, hence the need for a broader social effort of interventions by institutions. And, to some extent, such interventions are indeed needed. As we discussed earlier, technological advancements have so profoundly changed some of the key factors of Internet trust, such as identity, that users admittedly do not have relevant interpretive knowledge on which to draw when taking the leap of trust. The socio-technical environment of Internet communication has become so complex that our established ways and resources for making trust decisions are no longer adequate. In such circumstances, trust transfers are not just shortcuts but key viable methods for making decisions.

However, the genuine need to assist users in navigating an increasingly complex web of Internet sources and interactions can easily turn into a detrimental level of institutional control where “leaving the user alone with the Internet” is considered risky, as we saw in the introduction of this text. Like our colleague Tom, “unsupervised users” are increasingly perceived as potential victims of perilous Internet sources and actors. Therefore, their interaction with such sources needs to be tightly controlled and potentially disabled. In Tom’s example we saw that interaction with one of such sources was made difficult, if at all possible, at several levels—ISPs blocking access to the website, work computer requiring Tom to explicitly acknowledge and accept the risks, and a professional community stressing reputational risks of interacting with such a source. Yet, the only danger to which Tom was exposed when interacting with Library Genesis was to access copyrighted academic material free of charge. Compare this with access to FetLife, the world’s largest social network for the BDSM and fetish communities, that neither ISPs nor Tom’s work computer block.

In contemporary Internet communication, taking leaps of trust is no longer just the user’s decision, but instead a supposedly collaborative effort between the user and a set of outside actors presumably intended to help the user navigate complexities of the unknown. Yet, the comparison between institutionally assisted access to Library Genesis and to FetLife illustrates vividly why people increasingly distrust institutions, and why anti-vaccine networks and fake news flourish. Furthermore, in the context of the Internet and trust, rapidly changing official characterizations of Internet sources and actors such as Facebook or
Wikileaks, dethroned from heroes to criminals in less than a decade, becomes additionally detrimental. Not only are users getting more confused about whom and why to (dis)trust, but “the practical freedom to read and write what one wishes to,” that May articulated in 1994 increasingly becomes an elusive dream. As Electronic Frontier Foundation (2019) warns, this fundamental right of Internet users is increasingly being curtailed, most commonly with the pretense of protecting users from trusting dangerous online sources.

Trust and distrust are thus becoming key driving forces of Internet development and regulation, further destabilizing factors of Internet trust analyzed in this text. In terms of identity, for instance, increasing need to differentiate between human and nonhuman users leads to ever-increasing sets of authentication requirements, from one’s favorite vacation spot to fingerprints and facial images. In return, increasing authentication requirements result in more and more user data, critically undermining users’ privacy and opening the door to surveillance capitalism. Finally, diminished user privacy seriously undermines possibilities of collective social action. Even with the right to be forgotten, digital traces left behind each of our online activities, such as signing an online petition or downloading a book, stay as our permanent record used to determine whether we can enter a foreign country (Brandom, 2017) or get a job (Driver, 2018). So, enjoy your browsing.

References

Agarwal, S. and Farid, H. (2019). “Protecting World Leaders Against Deep Fakes.” CVPR Workshop, Computer Vision Foundation. Retrieved from http://openaccess.thecvf.com/content_CVPRW_2019/papers/Media%20Forensics/Agarwal_Protecting_World_Leaders_Against_Deep_Fakes_CVPRW_2019_paper.pdf

Alarcon, G., Lyons, J.B., Christensen, J.C., Klosterman, S.L., Bowers, M.A., Ryan, T.J., Jessup, S.A., Wynne., K.T. (2017). The effect of propensity to trust and perceptions of trustworthiness on trust behaviors in dyads. Behavior Research Methods, 50(5), 1906–1920.

Bakke, A. (2015). A rhetorical perspective on trust in E-health websites. PhD dissertation. Minneapolis: University of Minnesota.

Barlow, J.P. (1996). A Declaration of Independence of Cyberspace. Retrieved from https://www.eff.org/cyberspace-independence

Bodo, B. (2018). The genesis of library genesis: the birth of a global scholarly shadow sibrary. In J. Karaganis (Ed.), Shadow libraries: access to knowledge in global higher education. (pp. 25–53). Cambridge, MA: MIT Press.

Brandom, R. (2017). Trump’s executive order spurs Facebook and Twitter checks at the border. The Verge, Jan 30, 2017. Retrieved from https://www.theverge.com/2017/1/30/14438280/trump-border-agents-search-social-media-instagram

Brownlie, J. (2005). Leaps of faith and MMR: an empirical study of trust. Sociology, 39(2), 221–239.
Brügger, N., Goggin, G., Milligan, I., & Schafer, V. (2017). Introduction: Internet histories. *Internet histories: Digital Technology, Culture, and Society, 1*(1–2), 1–7.

DeSteno, D. Breazeal, C., Frank, R.H., Pizarro, D., Baumann, J., Dickens, L., and Lee, J.J. (2012). “Detecting the Trustworthiness of Novel Partners in Economic Exchange,” Psychological Science, XX (X),1–8.

Dibble, J. (1998). *My tiny life: Crime and passion in a virtual world.* New York: Holt.

Driver, S. (2018). Keep It Clean: Social Media Screenings Gain in Popularity. Business News Daily, October 7, 2018. Retrieved from https://www.businessnewsdaily.com/2377-social-media-hiring.html

Electronic Frontier Foundation. (2019). *Say No to Online Censorship!* Retrieved from https://www.eff.org/pages/say-no-to-online-censorship

Frederiksen, M. (2012). Dimensions of trust: An empirical revisit to Simmel’s formal sociology of intersubjective trust. *Current Sociology, 60*(6), 733–750.

Gurak, L.J. (1997). *Persuasion and privacy in cyberspace: the online protests over Lotus MarketPlace and the Clipper chip.* New Haven: Yale.

Himmelstein, D. S., Romero, A. R., Levernier, J. G., Munro, T. A., McLaughlin, S. R., Greshake Tzovaras, B., & Greene, C. S. (2018). Sci-Hub provides access to nearly all scholarly literature. *eLife, 7*, e32822. doi:10.7554/eLife.32822

Hoffman, B.L., Felter E.M., Chu K., Shensa A., Hermann C., Wolynn T., Williams D., Primack B.A. (2019). It's not all about autism: The emerging landscape of anti-vaccination sentiment on Facebook.” *Vaccine, (37)*, 2216–2223.

Larsson, A. O., & Moe, H. (2015). Bots or journalists? News sharing on Twitter. *Communications: The European Journal of Communication Research, 40*(3), 361–370.

Licklider, J.C.R. & R. W. Taylor. (1968.) The computer as a communication device. *Science and Technology* (September), 20–41.

Longhurst, R. (2009). Youtube: A New Space for Birth? *Feminist Review. 93* (1), 46–63.

Luhmann, N. (1979). *Trust and Power.* Chichester; New York: John Wiley & Sons Inc.

Markus, F. & Bauer, P.C. (2016). Personality traits and the propensity to trust friends and strangers. *The Social Science Journal, 53*(4), 467–476.

May, T. (1994). Crypto anarchy and virtual communities. *Cypherpunks.* December. Retrieved from http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-virtual-comm.html

Möllering, G. (2001). The Nature of Trust: From Georg Simmel to a Theory of Expectation, Interpretation and Suspension. *Sociology, 35*(2), 403–420.

Palfrey, J. and Gasser, U. (2008). *Born Digital Understanding the First Generation of Digital Natives.* Basic Books, New York.

Prieto, A. G. (2009). From conceptual to perceptual reality: trust in digital repositories. *Library Review 58* (8), pp. 593–606
Rainie, L., Keeter, S., & Perrin, A. (2019). *Trust and distrust in America*. Pew Research Center. 22 July.

Rheingold, H. (1993). *The virtual community: Homesteading on the electronic frontier*. Reading, Mass: Addison-Wesley Pub. Co.

Seligman, A. B. (2000). *The Problem of Trust*. Princeton University Press.

Stewart, K.J. (2003). “Trust Transfer on the World Wide Web.” *Organization Science, 14*(1), 5–17.

Sztompka, P. (2000). *Trust: A Sociological Theory*. Cambridge, UK: Cambridge University Press.

Trant, J. (2009). Tagging, Folksonomy and Art Museums: Early Experiments and Ongoing Research, *Journal of Digital Information, 10* (1), 1–44.

United States National Science Foundation (NSF). 2016. Public access policy. Retrieved from https://www.nsf.gov/pubs/2016/nsf16009/nsf16009.jsp#q1

Van Gelder, L. (1990). The strange case of the electronic lover. In G. Gumpert and S. L. Fish (Eds.), *Talking to Strangers: Mediated Therapeutic Communication* (pp. 128–142). Norwood: Ablex.

Vinge, V. (1981).

Weise, E.R.(1996). A thousand aunts with modems. In L. Cherny and E.R. Weise (Eds.), *Wired Women* (pp. vii-xv). Seattle: Seal

Wojcik, S., Messing, S., Smith, A., Rainie, L., and Hitlin, P. (2018). Bots in the Twittersphere. Pew Research Center, April 9. Retrieved from https://www.pewresearch.org/internet/2018/04/09/bots-in-the-twittersphere/

World Health Organization. (2019). Ten threats to global health in 2019. Retrieved from https://www.who.int/emergencies/ten-threats-to-global-health-in-2019

Yiannakoulias, N., Slavik, C.E., and Chase, M. (2019). Expressions of pro– and anti-vaccine sentiment on YouTube. *Vaccine, 37* (15), 2057–2064.

Zuboff, S. (2019). *The Age of Surveillance Capitalism*. London, UK: Profile Books.