Security, privacy'); drop table users; - and forced trust in the information age?

Security, Privacy'); DROP TABLE Users; -- and Forced Trust in the Information Age?

When trusting an information system is not optional and why it matters

By Antti Hakkala, Olli I. Heimo, Sami Hyrynsalmi, and Kai K. Kimppa

In this study, we discuss forced trust in the context of information systems, information society and surveillance. Trust definitions and concepts pertinent to the discussion are examined and portrayed with case examples of forced trust in different situations that make up the information society. As the forced trust appears mostly in the governmental information systems, we reflected the concept from the security and privacy point-of-view that are important for the users of such systems in the current age of information. We portray the trust landscape of critical governmental information systems and discuss forced trust in the context of Internet infrastructure and mass surveillance. We provide a glimpse of an information society that combines security, trust, and privacy, while also providing discussion on what kind of trust dynamics such a utopia would require.

Keywords: trust, information society, information security, surveillance, information systems
Categories: • **Security and privacy~Trust frameworks** • *Security and privacy~Social aspects of security and privacy* • *Social and professional topics~Governmental surveillance* • *Social and professional topics~Governmental regulations* • Social and professional topics~Management of computing and information systems
Corresponding Author: *Antti Hakkala*
Email: *antti.hakkala@utu.fi*

1. Introduction

A famous xkcd comic strip[1] portrays the dialogue between the mother of a school-aged child named *Robert'); Drop TABLE Students;* -- and a school official. This rather individual name – it ends in a SQL-injection[2] – is actually a successful security attack against the school's information system. In the strip, registration of the name caused the loss of all student records. As the official expressed his disapproval, the mother in turn hoped she had succeeded in teaching the school to sanitize their database inputs.

[1] Exploits of a Mom. R. Munroe. xkcd – http://xkcd.com/327/ - Accessed 08/11/2016.
[2] A Classification of SQL-Injection Attacks and Countermeasures. W. G. J. Halfond, J. Viegas, and A. Orso. Proceedings of the 2006 IEEE International Symposium on Secure Software Engineering, Washington, DC, USA, 2006.

While Randall Munroe's xckd comic strip is an amusing small story told in four panels, it is also an illustrative conversation piece about trust in the modern information age. Information and software systems have become the cornerstones of our society. Each system has its producers, operators and users, and these parties are forced to trust each other to some extent. As a concretizing example, the producer of the comic strip's information systems trusted that its operators do not try to hack the system. Similarly, the unlucky operator trusted that users do not try to hack the system – in this case the trust was misplaced. As the infamous mother showed, even one weak link can cause remarkable losses to trust relationships, stored data, and information systems.

This paper addresses the complexity of trust relationships in societies driven by information and software systems. The aim of this paper is to open a discussion in previously omitted topic of *forced trust* and its implications. As we later define in this essay, 'forced trust' refers to a situation where trusting another stakeholder of an information system is not voluntary. The rest of this study is structured as follows. In the following section, we will review relevant literature on trust and mistrust. The third section presents our central contribution, the concept of forced trust, and illustrates it with examples of critical information systems. The last two sections conclude the causerie with reflecting the forced trust in the society and summarizing our findings.

2. Trust

2.1 Defining trust

Trust is an important concept both in personal and societal interactions. Humans have a tendency to trust, and the process of assessing other humans and their trustworthiness is quite intuitive. Sometimes it is formed by stereotypes, in other instances from personal experience. We are also able to differentiate people based on what they can be trusted with. Schneier illustrates this quite concisely[3]: "I trust Alice to return a $ 10 loan but not a $ 10,000 loan, Bob to return a $ 10,000 loan but not to babysit an infant, Carol to babysit but not with my house key, Dave with my house key but not my intimate secrets, and Ellen with my intimate secrets but not to return a $ 10 loan."

Trust and its absence are widely discussed topics in several disciplines; economics, sociology, computing and philosophy all have their own take on the concept of trust. For instance, computer and information system scientists as well as software engineers have been discussing trusted platforms[4], users trust to preservation of digital information[5] and influences of customers' trust to web pages and services[6,7]. Economists have examined both interpersonal and institutional trust. Examples include trust in electronic commerce

[3] Liars and Outliers: Enabling the trust that society needs to thrive. B. Schneier. Wiley, p. 6, 2012.
[4] Reflections on Trusting Trust Revisited. D. Spinellis. Communications of the ACM, 46(6), p. 112, 2003.
[5] Trust in the Preservation of Digital Information. P. E. Hart and Z. Liu. Communications of the ACM, 46(6), pp. 93-97, 2003.
[6] Trust and TAM in online shopping: an integrated model. D. Gefen, E. Karahanna, and D. W. Straub. MIS Quarterly, 27(1), pp. 51-90, 2003.
[7] Dynamics of the Key Elements of Consumer Trust Building Online. E. Patokorpi and K. K. Kimppa. Journal of Information, Communication & Ethics in Society, 4(1), pp 17-26, 2006.

transactions[8] and organizational trust[9]. Schneier examines trust as an essential part of functional society, and provides a framework for modelling trust dynamics and societal pressures in society[10].

Observing the sheer number of definitions and viewpoints on trust, it becomes evident that a single definition of trust is hard to come by. Marsh and Dibben note that as each discipline focuses on their own relevant aspects of trust, trust as a subject is inherently obscured[11]. Thus it is difficult to present all possible aspects and definitions of trust, as it varies according to the lens though which we observe trust. In this work we shall thus not choose a single trust definition over others as definitive, and focus mainly on trust definitions in the realm of information technology.

2.2 Trust and Information Technology

Trust in the discourse of IT and ethics is a widely studied field. A quick search in two main journals reveals this quite handily, as dozens of relevant articles can be found amongst the hundreds that are offered. However, in this context in which we are looking at the topic, the conclusion drawn by Giustiniano & Bolici – that there really is no consensus on what the definition or characteristics of trust are[12] – means that we can figure out what ICT enabled trust requires in specific situations.

Examples of building ICT enabled trust include (but are hardly limited to) for example reputation building and tracking[13,14], trust through using a trusted third party[15], and being reliable and consistent in ones' behavior (be the one behaving either a person, system or a corporation)[16,17]. Often trust in the ICT domain is used to facilitate interactions between hosts, devices, and systems that have no prior knowledge of each other, quite analogously to how humans use trust in interpersonal interactions.

---

[8] Trust metrics, models and protocols for electronic commerce transactions. D. W. Manchala 18th IEEE International Conference on Distributed Computing Systems, Amsterdam, Netherlands, 1998.

[9] An integrative model of organizational trust. R. C. Mayer, J. H. Davis, and F. D. Schoorman. Academy of management review, 20(3), pp. 709-734, 1995.

[10] Liars and Outliers: Enabling the trust that society needs to thrive. B. Schneier. Wiley, 2012.

[11] The role of trust in information science and technology. S. Marsh and M. R. Dibben. Annual Review of Information Science and Technology, 37(1), p. 468, 2003.

[12] Organizational trust in a networked world: analysis of the interplay between social factors and Information and Communication Technology. L. Giustiniano and F. Bolici. Journal of Information, Communication and Ethics in Society 10(3), pp. 187-202, 2012.

[13] How can contributors to open-source communities be trusted? On the assumption, inference, and substitution of trust. P. B. De Laat. Ethics and Information Technology, 12, pp. 327—341, 2010.

[14] From open-source software to Wikipedia: 'Backgrounding' trust by collective monitoring and reputation tracking P. B. De Laat. Ethics and Information Technology, 16, pp. 157—169, 2014.

[15] Dynamics of the Key Elements of Consumer Trust Building Online. E. Patokorpi and K. K. Kimppa. Journal of Information, Communication & Ethics in Society, 4(1), pp 17-26, 2006.

[16] Ibid.

[17] Ethics in the bank internet encounter: an explorative study. J. D. Rendtorff and J. Mattsson. Journal of Information, Communication and Ethics in Society, 10(1), pp. 36—51, 2012.

2.3 Trust and security

When we consider potential adversaries attacking information systems, we can group them into different categories based on their motivation[18]. *Curious non-technical users* are exactly that – curious people with legitimate access rights and a penchant for getting into trouble by looking into places they perhaps should not. Motivated generally by curiosity instead of malice, they explore resources to which they have been given access. *Insiders* are technically capable users who take it as a challenge to break the security of a system. *Financially motivated attackers* range from individuals to organized criminal groups, but all have the same goal of making financial profit. *Espionage*, whether private or state-funded, refers to attackers with a clear motive, extensive training, serious funding and the capability to compromise information systems to achieve whatever goals they have.

When we consider real-world systems, there is no such thing as perfect security[19]. All computer systems have a way for legitimate users to access them, and this can always be exploited by a malicious adversary. The only cryptosystem that actually offers provable perfect security – the one-time pad – is notoriously difficult to implement[20]. We must accept some insecurity in information systems for them to be usable, and if something is usable it can be misused. This leads to organizations having to accept a certain amount of risk with information systems and data. For example, banks accept a certain loss margin with credit card systems. While fraudulent users and technical errors cause a nontrivial financial loss, in the end the benefit (and profit) from using the system far outweigh potential losses due to malicious activity.

The fact that no perfect security exists also means that there is a necessity for some elements of trust in all information systems. The users must trust the administrators not to abuse their greater privileges. The admins in turn have to trust the users to behave, and not to endanger the system. The developer of an information system is trusted to provide a good and secure system with as few errors as possible, and the developer trusts the client that they will indeed keep their end of the agreement, and not to change specifications on the fly or to withdraw from the deal altogether.

2.4 What could go wrong?

Information systems' users are often guardians of information, for they have access over information that should be guarded. Thus, the old question by Socrates is ever more relevant: *Who guards the guardians?* We must place trust in these guardians, at least in matters that are not of utmost importance – such as (electronic) voting, national security, medical records etc. If the systems are built as secure from the inside as from the outside and the users are either heavily restricted or intensively monitored, a lot of resources are lost[21]; resources that could be used either to improve the system or the service or to

---

[18] Modern operating systems. Second Edition. A. S. Tanenbaum. Prentice-Hall, pp. 585—586, 2001.
[19] Beyond Fear – Thinking sensibly about security in an uncertain world. B. Schneier. Copernicus Books, p. 11, 2003.
[20] Communication theory of secrecy systems. C. E. Shannon. Bell system technical journal, 28(4), pp. 656-715, 1949
[21] Parasitic Order Machine. A Sociology and Ontology of Information Securing. J. Vuorinen. PhD dissertation, Annales Universitatis Turkuensis B392, University of Turku, Finland, 2014.

improve the overall security of the system from outside attacks. It must be noted that there must be some security in the system itself – at least against the most basic attacks and malware, but in some areas it is more important to direct scarce resources to the fields that require them the most.

Input sanitation increases the workload, provides an extra layer of complexity in system design, and slows things down – this holds for practically all security measures[22]. If there is no need for added security due to an assumption of trust, we would not necessarily need excessive security measures in place, irrespective of whether the users – should they choose to do restricted actions with the system – could be caught or not.

We must remember however that while not the most common, often the most serious security risk for an organization is an unhappy former employee who misuses this trust[23,24], and thus keep in mind that even if we do trust our workers, fired workers are a different matter all-together.

3. Forced trust in the information age

3.1 May the (forced) trust be with you

We depart from the extant literature, which frequently focuses on voluntary trust relationships built around or enabled by ICT services and products, by focusing on trust relationships that are forced by, e.g., official, superior or governmental stakeholders. This is clearly a case of trust as despair[25], a type of situational trust where the trusting agent has no other choice but to trust the solutions given to them by official parties. Here, on one hand, 'voluntary' refers that a user of an information system or an ICT product is able to decide or not to trust another party.

The forced trust, on the other hand, illustrates a situation where a user is dictated to use and to trust an information system or an ICT product. As we define it, the 'forced trust' concept depict a situation where an entity–whether a customer, an organization or even a governmental agency–does not have a privilege to choose but is instead mandated to use a dictated information system. As their name suggest, the information systems store, retrieve, process and transmit information. Therefore, the entity has interests towards the system, its operators and behaviour regarding his privacy and security. Interesting consequences follow from this setup.

As a user does not have the privilege to choose in the forced trust cases, his or her actions and attitudes are affected by the forced trust. To clarify the consequences, please consider the following simplified example. On one hand, the user of an information system has to use the system but his or her inputs might be partial due to the lack of trust towards either

---

[22] Ibid.

[23] A framework for understanding and predicting insider attacks. E. E. Schultz. Computers & Security, 21(6), pp. 526-531, 2002

[24] Behavioral and policy issues in information systems security: the insider threat. M. Warkentin and R. Willison. European Journal of Information Systems, 18(2), p. 101, 2009.

[25] An integrative model of organizational trust. R. C. Mayer, J. H. Davis, and F. D. Schoorman. Academy of management review, 20(3), pp. 709-734, 1995.

the supplier, operators or administrators of the system. While this might not cause direct harm, it hampers the usefulness of the system. On the other hand, the supplier of the system cannot trust on the benevolence of all forced users and therefore, they are forced to implement security verification for inputs and maintain backup plans. As all security verifications causes costs (in terms of computing power as well as in the price of design, implementation and operation), forcing trust between the entities is also costly.

To make the overall picture even more complex, forced trust appears rarely alone; in all information systems there is, or at least initially was, mutual trust between some of the entities. In addition, there are different forms of trust that are relevant to the discussion on forced trust and information systems. In the following section we will examine three special types of "negative" trust that all have a role in modelling forced trust.

3.2 Mistrust, distrust, and untrust

Marsh and Dibben discuss three trust concepts central to our discussion: mistrust, distrust and untrust[26]. The first, *mistrust,* is, simply put, misplaced trust. It describes a situation where trust is first placed and then abused in some manner, leading to a situation of trust becoming that of mistrust. It is in effect negative trust, a negative characterization of the target of mistrust. It is possible to continue to operate in the zone of mistrust, but probably some other leverage is required than trust to facilitate further cooperation in this case.

The second is *distrust*. It is a subtly complex type of trust, where the expected outcome of trust is *negative*. A trustor with distrust expects the other party to actively act against their interests. It must be noted that it is possible to function in an environment of distrust using external (with regard to trust) control mechanisms to ensure compliance and cooperation. These include rules, regulations, legislation and contracts. Marsh and Dibben give an example on the distinction between mistrust and distrust by comparing them with misinformation and disinformation. The former is factually incorrect but possibly not maliciously, but the latter is purposefully incorrect information.

The third type of trust Marsh and Dibben discuss is *untrust*. It is described as a situation of positive trust, i.e. trust exists, but that trust is insufficient. In a situation of untrust, further action or assurance is required before a state of trust is achieved. Similar mechanisms that can be used for functioning with distrust can be used. The difference between untrust and distrust is that in the former there is some uncertainty towards the trustworthiness of the target of untrust, while in the latter it is clear that the target of distrust is indeed *not* trustworthy.

3.3 An example: Critical government information systems and trust

Next we continue our analysis with an example of ultimate forced trust: information systems that its users are forced to use whether they are willing or not, and with

[26] Trust, untrust, distrust and mistrust–an exploration of the dark (er) side. S. Marsh and M. R. Dibben. International Conference on Trust Management, 2005.

significant negative repercussions on defection – refusal to cooperate with the expected societal norm – instead of cooperation.

Heimo, Koskinen and Kimppa define a *critical governmental information system* (CGIS) as *"an information system developed for governmental needs including data or functionality which is critical in nature to the security or wellbeing of individuals or the society as a whole"*[27]. Classical examples of CGISs include, e.g., e-voting systems, electronic taxation systems and so forth. Such information systems are of particular interest when examining trust, mistrust and distrust as often several public as well as private organizations have a role in production and operation of these kinds of systems.

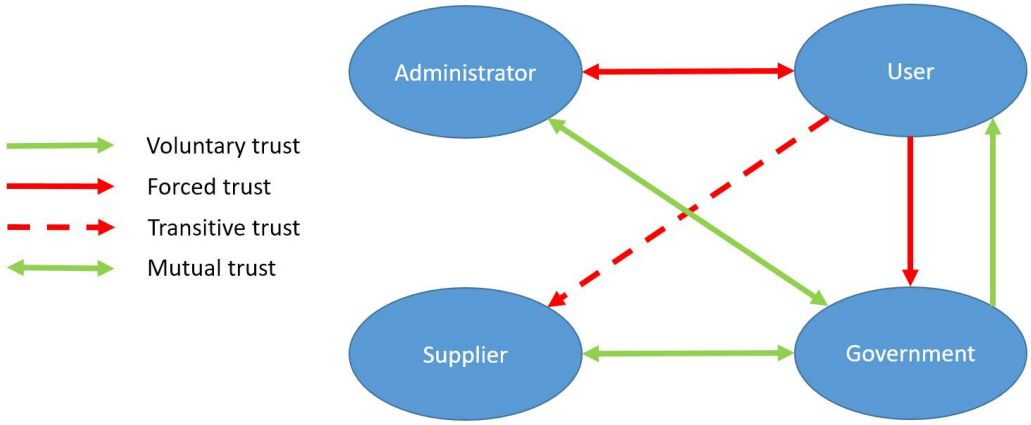

Figure 1. Trust landscape for CGIS

In Figure 1, we have illustrated the trust landscape for a CGIS by using a directed multigraph. Each vertex of the graph represent a category of actors related to the information system. An arrow-headed, i.e. directed, edge between two vertices illustrates trust between two actors and the direction of the arrow depict the direction of trust. In addition, the graph's edges are weighted with the type of trust between the entities.

From the figure, we can clearly identify the forced trust relationships between users, government, system administrators and information system suppliers. The role of the user is particularly unfortunate in the case of user-supplier trust relationship. As the user has actually very little say into which information system supplier will be designing and implementing the CGIS, there is no other option but to trust the supplier to keep their end of their bargain and to provide a secure and usable system. This trust relationship is indeed both transitive and forced; the user must trust the IS supplier because the government trusts the supplier, and the user is in a forced trust relationship with the government. This latter forced trust relationship is very strong. In the case of disagreement, the recourse available to users is either to vote differently and hope for a change in policy, or to move to another jurisdiction with a different government – if possible. Worst case scenarios sadly include violent uprisings.

[27] Responsibility in acquiring critical governmental information systems: Whose fault is failure? O. I. Heimo, J. S. Koskinen, and K. K. Kimppa. Ethicomp 2013 conference, University of Southern Denmark, Kolding, Denmark, 2013.

The government must also trust the supplier, but as an entity with significant advantages over an individual (sovereignty being the foremost), the government has a definite choice on which supplier to select. This decision should obviously be based on trust, but if distrust reigns, control mechanisms must take a major role in the relationship. Of course situations exist where the supplier has the significant upper hand, such as supplier lock-in, where an information system supplier is able make itself irreplaceable and making it impossible or highly impractical for a government to choose another IS supplier. It could be argued that from the point of view of the government this is a clear state of mistrust, but further expanding this aspect of the trust landscape is outside the scope of this paper. We are more interested in the other cases in our example, where forced trust is due to more serious reasons than impracticality.

Users have also no choice but to trust the administrators of the information system. Admins are people with the capability to observe and affect the operation of the information system with the goal of maintaining proper system operation. Their job is to keep an information system running and functioning correctly, but they can also cause significant harm to a system or to an individual user through their actions, whether unintended or deliberate. This trust-based issue can be mitigated by "watching the watchmen": auditing the administrators' actions within the IS and "forcing" the desired behaviour out of the admins by generating panopticon-style control mechanisms for administrators. In most cases the users of an information system do not interact with the admins, unless there is an anomaly that is visible to users and also requires administrative attention.

A major problem with users and information systems is the propensity of users to choose bad passwords[28]. As the password is the main authentication method for the majority of services, the persistent use of bad passwords is a major problem for any IS administrator. It is also a major breach of trust in the case of a successful break-in by criminals using guessed credentials from legitimate users. Password audit tools are common IT administration tools for this reason. In some cases, administrators can choose their customers and users, but in the case of CGISs, this is not generally possible. The administrators simply have to cope with the users behaving in an irresponsible manner – in other words, the admins are in a forced trust relationship with the users. Especially with CGISs that are so important that the right to use them is a legally guaranteed right, it is impossible to ban users from using the system. For example, eVoting systems are in this category; the right to vote is central to democracy, and it would certainly be an interesting discussion whether you could ban people from voting based on irresponsible behaviour. If even the act of killing another person does not revoke your right to vote – at least in civilized jurisdictions – what could possibly justify banning users from this system over bad passwords?

[28] Password strength: an empirical analysis. M. Dell'Amico, P. Michiardi, and Y. Roudier. IEEE INFOCOM 2010 Conference, San Diego, California, USA, 2010.

3.4 Forced trust in Internet infrastructure – mass surveillance on easy mode

We have now examined forced trust in CGISs. Mass surveillance of Internet users is a special case of exploitation of forced trust, and thus deserves to be examined in more detail. The United States National Security Agency (NSA) and other equivalent agencies – including ones like the UK's GCHQ and Sweden's FRA – are engaging in mass surveillance by collecting extensive amounts of data of Internet users. The techniques and methods used to implement this data collection exploit the flaws in the basic infrastructure of the Internet, and further compromise an already insecure communications network. Examples include leveraging the physical layout of the backbone network[29] and compromising the operating system of backbone network routers[30] – methods that make it possible to redirect and intercept Internet communications traffic to desired locations for analysis. An illustrative example of this is how the NSA compromised Google and all the data in their internal network. By taking advantage of network topology and access to routing hardware, the intelligence agency was able to gather data from Google's private cloud networks[31].

The dilemma of forced trust in information systems in general, and CGIS's in particular, thus must be placed in the context of global communication infrastructure; instead of asking whether we can trust an individual information system, we must now question *whether we can trust the underlying infrastructure of the Internet itself*, and also ask *to what extent Internet users are in the desperate position of forced trust?* The Internet in itself is designed to withstand a nuclear conflict, and as a highly decentralized network it is capable of relaying information, barring a complete global destruction of infrastructure. The problem is not resilience; the problem is trust. If users wish to use the Internet, they must also trust it as a platform, and this is forced trust on a global scale.

Our communications infrastructure is based on a massive scientific and engineering effort spanning decades of work. Currently it is being severely undermined by attempts to exploit known flaws and even introduce new, subtle ones that only certain people can exploit – or that is the intention. In reality, there is no such thing as an exploit with a limited user base, a "skeleton key" for security measures. A weakness or flaw can be exploited by anyone who is aware of it, and trusting the security of a system on the obliviousness of the opponent – *security by obscurity* (see e.g.[32,33,34]) – is an information

[29] NSA Surveillance: Exploring the geographies of Internet interception. A. Clement. iConference 2014, 2014.
[30] Photos of an NSA "upgrade" factory show Cisco router getting implant. S. Gallagher. Ars Technica – http://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/ – Accessed 11/9/2016.
[31] NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. B. Gellman and A. Soltani. The Washington Post – https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html?utm_term=.cdb077c223fc – Accessed 30/1/2017.
[32] La Cryptographie Militaire, A. Kerckhoffs, Journal des sciences militaires, 9(January) pp. 5-38; 9(February) pp. 161-191, 1883.
[33] Communication Theory of Secrecy Systems. C. E. Shannon. Bell Systems Technical Journal, 28(4), pp. 656-715, 1949.

security disaster waiting to happen. If this development continues, it will continue to make the Internet less secure for everyone, not just those who are supposed to be targeted by mass surveillance. Ironically, those who are the claimed real targets of these surveillance measures – terrorists and members of major criminal organizations – are often resourceful enough to create their own security solutions. Well-implemented strong encryption is still capable of thwarting all known cryptanalysis methods, and the information required to implement this is freely available – it is impossible to ban the concepts of algebra and number theory from common knowledge.

So far the users have been handed the metaphorical short end of the stick. We will discuss potential user responses in the next section. It might at first seem that the trust issues are non-issues, but societies require a certain base amount of trust to function[35] – without trust it is difficult to ensure even the basest of services in a society. If we consider a society based on distrust, it is a society based on control and constant verification, extending to even the most menial of societal interactions.

3.5 Implications of forced trust

Forcing trust between the actors of the information system has naturally consequences. For each actor, there are roughly three different reaction patterns. Either an actor could *accept* the current situation and decide to trust to the information system, its providers and operators – whether this trust is appropriate or not. There are two major categories belonging into this pattern: First, an actor could either be aware of the implications and, nevertheless, decide to trust the system and continue to use it (e.g. "I know; I do not care" attitude). Second, an actor can be irritated from use of the dictated system but is not worried enough to care (e.g. "I'm annoyed, but *not enough*"). Often these are considered as the desirable outcomes for user reaction patterns from organizational point of view, as these responses make it possible for the information system to perform in its full or at least near to full potential.

Alternatively, an actor could decide to *avoid,* or not to utilize the system to its full capabilities. This for example can mean that an end-user does not give all required information for the system, if he or she uses it at all. For example, please consider the situation where an organization wishes to follow how the employees use their working time in order to ascertain the costs of supporting functions. To do so, the organization launches a time clock system and requires every employee to use it. As the employer is forcing people to trust the information will not be abused, it is likely that due to resistance to change and lack of trust, employees would not give fully correct information. This, in turn, makes this initiative eventually futile or even counterproductive, as the result will be decisions made upon incorrect or incomplete data.

Finally, an actor might decide to take an active stance to *fight against* another stakeholder or the system itself. For example, in the previous example, employees who refuse to use the system and actively use working time to downplay the initiative and the new system

---

[34] Applied Cryptography Second Edition: protocols, algorithms, and source code in C. B. Schneier. John Wiley & Sons, Inc, New York, 1996.
[35] Liars and Outliers: Enabling the trust that society needs to thrive. B. Schneier. Wiley, p. 243, 2012.

are actively fighting against the system. Similarly, administrators of an information system might set needlessly strict information security policies that actively hinder employees in their work due to lack of trust or mistrust between the administrators and the end-users. Indeed, an administrator that has had to previously repair damages caused by an irresponsible user is quite certainly mistrustful of users in the future. Although potentially strict security policies can be justified, there exists a line between helping and hindering.

An alternative stance for the previous analysis is to study the value proposition of a system. Each service and solution has some value that in the best case they could bring to the users and owners of the system. The previously mentioned time clock system would bring value to the employer by revealing the real costs of each functions. Similarly, an employee would be able to follow and report the real working hours required by the different tasks. In the mutual trust situation, the outcome would be the desired one and the information could be useful and help to use resources correctly. In the case of forced trust, the full potential value of the system will not be achieved. As previously discussed, the information can be partial or even incorrect if an employee does not trust the system.

Now let us consider the trust classes described in Section 3.1 in a situation of forced trust in the context of information systems. In this case, it is fruitful to observe the situation when we choose not to cooperate. What are our potential choices in this situation, and how much are they choices in the first place? Examples of information systems dealing with and measuring employee performance leading into negative outcomes such as firings have been previously observed by Zuboff[36], among the first. There is a clear forced trust aspect in such systems, for example, and the user response to forced trust will depend on the type of trust.

In the case of forced untrust, the user response is hard to gauge. As there is positive but insufficient trust, all responses are viable. Some may trust the system and cooperate, some may not trust the system and still cooperate because they are beneath their "bothering" threshold, and some may choose apathy or even adverse actions, but they are probably less common. Forced untrust and CGISs is perhaps the least worrisome situation, as new ISs start out in this state; trust is yet to be established but the expectation is positive. Not having any trusted options can be a disadvantage, for example using a new eVoting system, with no option for paper ballots, is a situation of forced untrust.

Mistrust is more complex, and more prone to non-cooperation. Forced mistrust is a bad situation to be in; we have already trusted the other party, in this case the information system, its admins, or its suppliers, and have been betrayed in some manner. Unfortunately, we are in no position to choose another option, and our expectations of future transactions are probably negatively affected. In the information system context, this can be conceptualized as using an information system that based on previous experience has delivered bad results. Avoidance may be a prevalent user response in this case, with less accepting users and an increase in actively fighting users. A user with a forced mistrust relationship to a CGIS will find their options in society reduced. To

[36] In the age of the smart machine: The future of work and power. S. Zuboff. Basic Books, p. 317, 1988.

continue with the eVoting example, forced mistrust would describe a situation where an eVoting system is used even after negative results, and no other alternative is given.

Distrust is the worst type of trust discussed here, and forced distrust is a very bad situation. In this case, a significant part of the users will probably actively fight against the system, making it a very difficult, even hostile environment to function in. This is the situation where a user is forced to use a system that they are certain will not function properly, will cause detrimental effects to its users, or will in other ways betray any trust and expectations. To continue with the voting example, forced distrust would be using an eVoting system known to be rigged, and being provided no alternatives. In this case, acts of minor disobedience and defection are expected, full-blown sabotage is within the realm of possibility.

4. Discussion

In this study, we have examined the dimensions of forced trust in the context of information society and the information age. To the best of the authors' knowledge, this study is among the first to open discussion on the concept of forced trust between actors in this context. Further understanding of forced trust relationships is clearly needed to facilitate a better information society for us all.

A case in point of forced trust is expressed within the title of this paper. As universities are nowadays funded, e.g., by the volume of published studies, they have implemented different processes, practices and systems to collect all information related to both published and unpublished studies. We, as researchers, are forced to use these systems, and we have little to no power over the way the information we have given is later used. Due to potential dislike, mistrust and distrust among the system's users leading to potential acts of non-cooperation. The information system suppliers and administrations of the universities library system have subsequently had to protect their systems against simple SQL injection attacks – like the one embedded in the title of this paper, for example. Not doing so in the year 2017 is pure folly – thus we are not that terribly sorry for any database tables named "Users" that get lost in the process of dissemination of this paper. Whereas the computing resources needed to process the input information are increased, it is also likely that a librarian is needed to verify that the input given is not from a malicious actor, but rather from scholars with ~~a bad sense of humour~~ an important message.

Most of all it is important to understand where the trust is forced. If the system relies on trust forced upon any of its stakeholders, those stakeholders are subject to use of power by the enforcers of that trust. Moreover, when the trust is forced, the enforcer must have some external power which they can rely upon. If not, the trust is no more – and if so, the perceived power and the likelihood of applying it must be more powerful than the consequence of breaking that trust and the probable gain from this action. Societal pressures describe these forces, and they can be categorized in various ways – Schneier

divides them into moral, reputational and institutional pressures, and security systems[37]. When the enforcer is not a single entity but merely "the system", for which all are more or less working for, most people will not be eager to break the trust – even forced one – but none the less the probability rises whenever the threat of consequences diminishes.

As for the example of CGIS, the requirement for placing any trust is to be able to verify the correctness of any given IS – at least at some level. Without mechanisms of verification, trust turns to belief and the "trusted party" can easily fulfil the needs of the person or organisation in question and not the needs of users – those who are "forced to believe". The key element with trust is that if it is broken, someone *might* figure it out. The main problem amongst secretive CGIS designs, including (but not limited to) mass surveillance, many eVoting platforms, passport systems, or any other system based on security through obscurity, is the lack of openness and thus the possibility to conceal the potential malpractices within the system.

Therefore it is important to understand the difference between responsibility and accountability: a person might be *responsible* for their actions – but are they *accountable* for them? Can there be really trust – even forced – if there are no similarly forced consequences if the trust is seen to be broken? Whatever resources the organisations are given are finite, as are the results they are required to produce, the trust must be 'forced'. Because there are no watchmen (or no one to watch the watchmen?) we must trust others, even if this creates a situation in which a possibility to cheat the system exists. Of course, some members of systems such as these will always cheat; as long as there are not too many such participants, the system still works, however. The key issue is understanding where and when (and how) to dismantle the forced trust.

The forced trust in information systems might be unravelled if we just assigned more resources to watch over each other, a situation that does not have anything in common with trust and only with a more controlled society. But, none the less we seem to choose forced trust quite often. And because we have decided to trust each other rather than to watch each other, could this be a beginning of an end, or the start of a more civilised era?

[37] Liars and Outliers: Enabling the trust that society needs to thrive. B. Schneier. Wiley, p. 69-70, 2012.