Zsófia Hajnal

The Impossible Trinity of Security, Freedom and Privacy

Abstract

In Economics, the Impossible Trinity of free capital movement, an independent monetary policy and a stable foreign exchange rate is well known. A similar, though less explored trilemma exists in modern governance, operating with more basic concepts: that of security, freedom and privacy. The aim of the study is to clarify this latter trilemma, as well as to offer a theoretical long-term solution. After expounding the general nature of trilemmas and the three main concepts, the impossible trinity of security, freedom and privacy is examined by taking three extreme scenarios, and abandoning one of the mentioned values in each. The scenarios are based on partially hypothetical situations in developed countries, where encryption debates or terrorist attacks took place recently.

The study then turns to the solution of the situation. In order to understand the origin of the problem, it takes a step back to the dilemma of security and freedom. The fourth important concept the study operates with is transparency. The study suggests increasing transparency. A mathematical projection of the above mentioned scenarios is introduced, and the suggested solution is derived in an equation.

Keywords: *Freedom, Security, Privacy, Trilemma, Transparency*

ISSN: 1898-4509 e-ISSN: 2449-7436 online pdf

E-mail contact to the Author: zsofia.m.hajnal@gmail.com

Introduction

The different governments and international organisations have different strategies and tools for combatting terrorism. One of their tools is online surveillance. Surveillance however, is a controversial means in terms of privacy violations. In addition, the statistics of the public's trust in governments are falling. (OECD 2015). One of the arising tensions in society is that between the three concepts of security, freedom and privacy. The tension is triggered by the threat of terrorism, by the security solution of encryption, and by certain governmental strategies. According to this paper, the trilemma can be solved on the long term.

The aim of this study is to clarify the trilemma, as well as to provide a theoretical long-term solution supported by mathematical illustration. On the short term, the aim is to provide the insight which could motivate building stronger ties of trust between the government, the public and technology firms, in order to establish a more transparent system in the future. There is a growing need for public-private collaboration in order to tackle global security challenges (World Economic Forum 2016, pp. 26-27). Terrorism and cybersecurity challenges are no exceptions.

After surveying the three main concepts, the paper builds up the trilemma-model through introducing three scenarios. Thereafter, with a simple mathematical illustration, the growth rate of the impossibility of applying one concept against the other two is calculated. Then the concept of transparency is introduced, and the value of privacy is revisited, in order to determine whether it is indeed a value and a human need on the longer term. Finally, the paper offers the solution to the trilemma through suggesting a privacy lift, accompanied by a further mathematical illustration.

Currently, there clearly are limitations in time and space to this study, as technology firms, terrorism and governments are not present in every country. The paper deals mostly with online and smartphone surveillance, and mostly with scenarios which have emerged in the US and Europe, yet the aim is to make the results applicable on a global level.

Technology's reaches are limited, yet expanding, especially with the spread of access to the Internet and the expansion of the smartphone market. Fortunately, terrorism is not present in or a threat to every country, however, without proper prevention, this cannot be excluded for the future. Stable governments are not present in each country either, the number of fragile states is on the rise (The Fund for Peace 2016).

The paper offers the solution to a problem in (global) governance through mirroring an economic model (the Impossible Trinity), using mathematical tools (simple equations) while touching on legal topics. Related are the fields of philosophy, history and international relations. The present threats are seen through the realists' glasses, the qualitative argument however stands on the liberal approach to international relations. Thus, the future is seen brighter through the solution offered, and despite the challenges introduced, the second half of the paper has a touch of idealism.

The basic concepts

This chapter aims to lay down the basics for understanding the security-freedom-privacy trilemma. Following an introduction to trilemmas in general, security, freedom and privacy are examined one-by-one as concepts for which a definition is sought in the context of this paper.

The nature of trilemmas

A trilemma is similar to a dilemma in that it is a difficult choice, not between two options however, but three. Either it is only possible to choose one out of three, or only two out of three options. This paper deals with a constellation of the latter type, in other words, it applies the model of „pick two" to the concepts of security, freedom and privacy.

In international economics, the Impossible Trinity means that out of three given goals of the economic policy, only two can be realised simultaneously (Benczes *et al.* 2009, p. 236). For example, free capital movement, an independent monetary policy and a stable foreign exchange rate cannot be followed at the same time by the central bank of a small, open economy. This observation is based on the work of the economists Robert Mundell (1932-) and Marcus Fleming (1911-1976).

To explore the trilemma of security, freedom and privacy, we not only have to understand the mechanism of a trilemma, but also define the three concepts, and explore their nature. All three concepts are seen by society as values. Security and freedom even earned the title *global values* in recent literature (Spijkers 2011) of international law.

Security

When writing about security, the paper uses the following definition: „a low probability of damage to acquired values" (Baldwin 1997, p. 13). Throughout human progress, new values are acquired by the possibilities offered through freedom, for keeping these values however, humankind needs security. Thus, security is a „requisite for human society" (McCrie 2014, p. 21). According to neorealism, „security is the most important goal a state can have" (Baldwin 1997, p. 10). In another wording: „The first duty of the community is to protect itself through government and personal initiative" (McCrie 2014, p. 28).

Security is needed on all the levels of the individual, the state and humanity. This paper does not make a difference between them, firstly, because they are interconnected, and secondly because the results are applicable on all levels (however, the focus and emphasis of security in the scenarios is on the level of the state). Security should also be broadly interpreted here in terms of the objects, i.e. the values which need to be secured. The paper deals mostly with physical safety, national security and digital security, but after the solution of the trilemma, positive spillovers from these fields to economic, environmental and other security aspects are not excluded. Eliminating terrorism and similar types of crimes would for example enhance the flow of goods and services.

Freedom

In a broad interpretation, there are two kinds of freedoms present: negative freedom („freedom from") and positive freedom („freedom to"). „Negative liberty concerns the absence of constraints, impediments, or interference. (…) In contrast, positive liberty concerns the power or capacity to do as one chooses, or the power to act autonomously" (Schmidt *et al.* 2010).

Negative freedom and security are concepts close to each other, and the reason they are not unified is the disorder in our concepts about life. Just as many believe or are made to believe that privacy is a value in itself, we cannot clearly distinguish between security and freedom, because of our half-chaotic social structures. If we would define security and freedom based on human needs, we could draw a minimum of rights (the level human rights should reach), which would be well above today's standards. However, this minimum would require a healthier distribution of wealth, and currently, our limited pace of marching towards equality prevents us from reaching that. Still, I will define freedom as opportunities above the security-minimum, i.e. apply the concept in its positive aspect

With progress, humankind has reached (on average) a life more secure and free than our ancestors' was. On the long term, there would not be freedom without security, but we have to cling onto our political and personal freedoms (which are actually rights and should rather be called securities), because they are endangered not only from below, by losing on physical security first, but also from above, from totalitarian-like governmental regulations. One reason I will argue for more transparency is that it eliminates the dangers, more obviously those from above (harmful regimes), but indirectly also those coming from below (terrorism and other crime types).

Privacy

In defining privacy the paper uses Daniel J. Solove's conceptualization of privacy as an „umbrella term" (Solove 2007): „I argued that instead of conceptualizing privacy with the traditional method, we should understand privacy as a set of family resemblances. (…) In other words, privacy is not reducible to a singular essence; it is a plurality of different things that do not share one element in common but that nevertheless bear a resemblance to each other".

Solove mapped out the boundaries of privacy by developing a taxonomy, listing privacy violations. His four main categories (information collection, information processing, information dissemination and invasion) are today's global privacy issue groups. Solove argues against those who see privacy and security as conflicting concepts, because this would mean a separation of the individual rights from community interests, which is simply not true[1].

[1] For a deeper argument about the unity of individual and community, see chapter V. of Hajnal 2016, (*Written and Unwritten Values in the Preamble of the United Nations Charter*).

This paper goes a step further by declaring that privacy is an individual security-freedom combination form (but mainly a form of security, as it has just been stated that negative freedom is security), and the roots of the conflict between the concepts, i.e. the trilemma, lie in the fact that the individual and the community have not ascended to the same level yet (in the individuals' view of their interests). The change requires trust, legal and technological progress, and is explained in more detail in the final main chapter of this paper.

The security-freedom-privacy trilemma in three scenarios

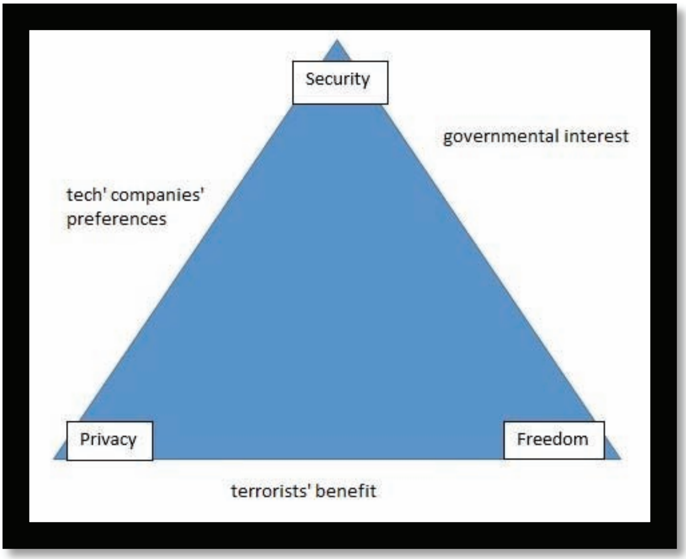

Figure 1. The impossible trinity of security, freedom and privacy

In today's society the three concepts have reached an unstable balance. For now the previous sentence may seem intuitive, and there are indeed limits in the extent of this paper to empiricism, but it is explained below in three scenarios why the current state is not sustainable. In all three scenarios, there is one passive, and there are three active entities. Society is the entity suffering the consequences of abandoning one of the three values in each scenario, while the three active entities (or actors) claim to represent extensive interests. The three entities are: terrorists, the government (in an example

(Yadron et al. 2016) represented by the FBI) and technology firms (in the referred example: Apple Inc.).

First scenario: starting out from less security

Security is the value to give up last, but as some political forces insist on freedoms with a higher emphasis (as do liberal governments) and some market forces insist more on privacy (as do the major technology firms), the paper will first show a scenario where the concepts of freedom and privacy have a stronger representation.

It is understandable if modern governments decide on promoting freedom, as freedom has been a hallmark of the western world's politics for centuries. However, as it is their responsibility as well to keep the people safe, in some cases of emergencies the government will be forced to look to the escape route of surveillance. At this point they face the major technology firms, who in turn face a heavy moral battle. They can give access to information which can help prevent terrorist attacks, but the same access would expose all of their users to the government. This leads the situation to the second scenario.

Second scenario: restricting freedom

If technology firms do not give in, the government cannot sustain preferring freedom to security. They have to tighten security in a degree that it becomes physically noticeable: more police in public areas and increased border control are the signs the public notices first. During the Apple-FBI debate last year, Tim Cook stated that: „While we believe the FBI's intentions are good, it would be wrong for the government to force us to build a backdoor into our products. And ultimately, we fear that this demand would undermine the very freedoms and liberty our government is meant to protect" (Cook 2016*)*, Tech firms should not present themselves as the gatekeepers of freedom, because that is – indirectly – exactly what the government has to take away from the citizens, if the technology firms do not provide the required accesses. And at this point, it is already privacy the concept being at stake.

Third scenario: giving up privacy

Technology companies cannot give in yet, because they see cyber threats. From their argument (Cook 2016) it follows that we would be at least as endangered (probably physically as well) if they provided accesses (a „masterkey" or „backdoor") to the government, as in the case of a world without surveillance. Thus, giving up privacy seems – at this point – equally chaotic to the previous two scenarios.

Mathematics of trilemmas

No mathematical description of trilemmas has been found by the author of this study so far, so this study attempts one.

Let X be the impossibility constant. If A is the possibility of living securely, B that of living free and C that of having privacy in society, then

(1) $X/A=B+C$

(2) $X/B=A+C$

(3) $X/C=A+B$,

Because – as demonstrated in the three scenarios – strengthening two of the concepts in society implies weakening the third.

After simplifying the equations, the following line results:

$$X=2(A)^2$$

The impossibility is exponentially increasing with the trouble of applying one variant against the two others increasing. If X, the impossibility constant is the same in all three cases, i.e. it is equally hard to enforce any third concept beside the other two, then $X=2(A)^2$.

If we let our world become more complex and complicated without making it transparent, it will be increasingly (exponentially) harder to sustain. This is empirically proven, as the increasing size and interconnectivity of the system, in addition to the speed of information (and for example capital-) flows leads to a higher level of vulnerability and more risks (Roy *et al.* 2010, p. 3). The interconnected nature of today's society is also experienced in international economics, more specifically in global value chains: „The increased connectivity brought about by GVCs has made economies more interdependent and increased the likelihood that a local disruption will lead to a system-wide failure. This systemic risk follows directly from the system's linkages and interdependencies, as the failure of a single entity or cluster of entities can cause a domino effect that may affect the entire system" (OECD 2013, p. 47).

Transparency as a solution

At this point it is time to argue for that we let go of one of the three concepts, namely privacy, and use transparency to solve the trilemma.

In its current state, privacy is a value that complements the security for the individual and lends freedom within that security frame. This is needed in the present form of societal systems, because they are based partially on threats, shame and fear. However, if society reaches the full security-freedom coverage on the level of the community, privacy will not be needed. Ancient tribes did not need privacy, and neither would an advanced global community. There may be difficulties however in the shift from the current system to the sustainable form of a transparent society.

The transparency-concept of this paper is based on the following statement: „transparency in essence is about reductions in information asymmetries" (Forssbæck *et al.* 2014). In broad terms, it is openness (disclosure) and accessibility (visibility) of information. Transparency is both about predictability and accountability, as well as it is a „right to know". The provided information has to be trustworthy and precise. (Forssbæck *et al.* 2014) But the transparency-concept the paper operates with goes beyond that. It foreshadows a society where access to any kind of information is equal for all, in all societal dimensions. The practical consequences are again out of the scope of this paper, but the theoretical-philosophical projections are made use of in the given context.

Transparency can solve two of today's society's problems. It can lead us out of the freedom-security cycles and help to get over the present paradigm in cyber-security.

The way out of the security-freedom cycles

There is a battle running through human history between the concepts of security and freedom. Security and freedom on a societal level are influenced by factors such as the availability of resources, the level of technological progress, population numbers and the level of integration. Despite both of them being basic needs, they exist in various constellations in various situations. The most common phenomena of the security-freedom dynamics are giving up a part of positive freedom for security's sake, or increasing security because of increased positive freedom (which has been achieved through integration or new technologies for example) (Hajnal 2016, pp. 29-30).

Through technology diffusion and new technologies, technology's role in security is gaining importance (Mallik 2004). Technological progress usually implies an increase in freedom, which cannot and should not be stopped, as this is how humankind makes progress. However, security has to keep up with freedom, even if „innovation quickly outpaces the capacity for regulatory oversight" (World Economic Forum 2016, p. 28). As McCrie asserts: „A safe society depends upon application of numerous resources (…) Such resources and procedures are likely to continue to evolve as society itself changes" (McCrie 2014, p. 41).

Society attempts to expand in both the directions of security and freedom, while balancing them through new laws. This paper suggests that one day, full security-freedom coverage can be achieved. Just as there is in fact an amount of food produced sufficient for everyone, and just like disaster-prevention would be much more effective if we re-allocated resources there from military budget for example[2], there is a solution at hand for the security-freedom-privacy trilemma, which only collides with interests of a minority. This minority however has a relatively strong bargaining power.

It is possible to live without limits to good intentions, while being completely safe. One of the actual limits to this today is privacy. Thus, the trilemma not only has a solution, but also is its recognition the key to solve the security-freedom dilemma.

The way to get over the present paradigm in cyber-security

If lifting privacy could hack the race between the security specialists and the attackers (Roy *et al.* 2010, p. 1) that would be the way to get over the present cyber-security paradigm (Roy *et al.* 2010, p. 3).

Transparency addresses the issue of attackers from another direction. It would actually prevent the attacks by social and economic suffocation of harmful intentions and

[2] Comments on *The Causes and Effects of Foreign Aid*, Conference Panel, 2016, ISA-CEEISA Conference – The Politics of International Relations (Ljubljana).

obstruction of terrorist groups. Transparency in this context would be a means of self-control and social pressure in the positive sense. The fact that „large-scale damage is possible for small groups and even individuals working from home computers or labs" (World Economic Forum 2016, p. 28) only strengthens the need for transparency.

Why transparency is hard to achieve

One obstacle to transparency on the level of the trilemma discussed is its interconnected nature with national and digital security. Regarding military strategy, encryption and surveillance, there is usually a divide between governmental choices and the choices of the tech world.

If the choice is between transparency and keeping military strategies secret, the governments tend to choose the latter, while the documents sometimes get published on pages such as Wikileaks. However, if the government has a choice between the values of transparency and digital security, it chooses the first one, as seen in the encryption debate. In the same debate, a technology firm stood up for digital security, which is also in tension with national security.

These battles have long not been won yet, and taking into account the current situation, a new approach, and a new level of solution are desirable.

The evolution of transparency

In his 2007 TED talk, „Progress is not a zero-sum game", the journalist and philosopher Robert Wright asserts „that there is a moral dimension to history; there is a moral arrow. We have seen moral progress over time". According to him, we are „on the brink of true global social organization" (Wright 2007).

In the chicken-egg problem of trust and transparency, this paper suggest that trust came first, allowing transparency to be present, which became part of our progress. Humankind has an intrinsic excessive morality that is being held back among others by the barriers to information flows. The next level of trust, i.e. the next moral revolution might be a time for a new type of *social contract* to manifest, laying down the basis for higher transparency levels. The next two chapters will argue that this is not only desirable, but feasible too.

Legal and economic outlook

It is hard to imagine the following, and even harder to create the legal framework, but if the whole system (of humankind) would be transparent, we would have no security issues.

This is not an immediate change – in current situations, there are so-called optimal levels of transparency (Forssbæck *et al.* 2014), because of the controllability of information. These theoretical levels increase with technological progress, and are probably already higher than the real levels of transparency, meaning that we are not at a Pareto optimal state of it.

There is a general legal principle first introduced in the 1789 *Declaration of the Rights of Man and the Citizen*, namely in article IV.: „Liberty consists of doing anything which does not harm others: thus, the exercise of the natural rights of each man has only those borders which assure other members of the society the enjoyment of these same rights. These borders can be determined only by the law". In this principle, we can see the conflict between the freedom of one individual and the security of the other. The principle can be translated into the privacy-transparency conflict: One has the right to know anything, until this knowledge does not harm others. The critical point here is where we draw the line: already at the fact of knowing, or at one's actions harming others.

A society built on fear and shame prefers the former, but that system has less benefits and is less sustainable, than a transparent society – this paper argues. Security of information does not necessarily mean hiding information. It could mean an effective legal system, where information cannot be abused. Thus, the line could be drawn at our actions. It is not our thoughts that have direct legal consequences, but our actions.

In economics, full transparency may be harmful with regard to rivals, but it will also open new arenas of competition, which is beneficial.

Technological outlook – the long-term solution

> „The Internet has opened a new frontier in warfare: everything is networked and anything networked can be hacked. (...) Every future conflict will have a cyber element and some may be fought entirely in cyberspace" (World Economic Forum 2016, p. 28)

Attackers use technology as a tool both for internal communication (planning physical attacks through encrypted networks) and for terror directly (cyberattacks). Thus, the technology has to be both transparent, have backdoors, but also, it has to be stable.

While technology giants do their best to protect our privacy, they also give us the tools for creating a more transparent world community. This is part of the rise of the Internet.

To reach a 100% freedom-security coverage we will need to open our world and our minds to each other. With the help of artificial intelligence solutions it will probably be possible to create the Internet of Minds.

Mathematical projection of the solution

Extrapolating the scenarios described earlier in this paper into the future would lead to deep political crises. And even if we assumed that society manages to get over those crises, they would experience soon that there is no life without security, and no enjoyable life without freedom. Privacy is the only concept that can be omitted from the system, through a smooth and technologically advanced shift. And if there is no privacy, i.e. $C=0$, then $X/C=A+B=\infty$, showing that the impossibility constant turns meaningless, and security and freedom will have no limits.

Conclusion

Transparency is not a universal remedy, however, it is part of the changes and ends humanity ought to get through in order to achieve its goals. All private information should slowly become public information. Individuals should learn from disclosed mistakes and society should learn not to shame individuals. Full transparency provides the highest chances for a perfect information system, which entails its most effective and secure physical state.

References

Baldwin D.A. (1997), *The concept of security*, "Review of International Studies" Vol. 23, http://www.princeton.edu/~dbaldwin/selected%20articles/Baldwin%20(1997)%20The%20Concept%20of%20Security.pdf

Benczes I., Csáki Gy., Szentes T. (2009), *Nemzetközi gazdaságtan (International Economics)*, Akadémiai Kiadó (Academic Publisher), Budapest

Comments on *The Causes and Effects of Foreign Aid*, Conference Panel, 2016, ISA-CEEISA Conference – The Politics of International Relations (Ljubljana)

Cook T. (2016), *A Message to Our Customers*, http://www.apple.com/customer-letter/

Forssbæck J., Oxelheim L. (2014), *The multi-faceted concept of transparency*, Research Institute of Industrial Economics, Stockholm, http://www.ifn.se/wfiles/wp/wp1013.pdf

Hajnal Zs. (2016), *Written and Unwritten Values in the Preamble of the United Nations Charter*, International Studies Association, Conference Paper, Ljubljana, http://web.isanet.org/Web/Conferences/CEEISA-ISA-LBJ2016/Archive/ee4a4645-9e55-4315-8eb3-453134dfce09.pdf

Mallik A. (2004), *Technology and Security in the 21st Century – A Demand-side Perspective*, Oxford University Press, Oxford, https://www.sipri.org/sites/default/files/files/RR/SIPRIRR20.pdf

McCrie R.D. (2014), *A History of Security*, in: *The Handbook of Security*, (ed.)Gill M., Palgrave Macmillan UK, https://he.palgrave.com/resources/Product-Page-Downloads/G/Gill-Handbook-of-Security-2e/0230006809_03_ch02.pdf

OECD (2013), *Interconnected Economies: Benefiting from Global Value Chains*, Paris, https://www.oecd.org/sti/ind/interconnected-economies-GVCs-synthesis.pdf

OECD (2015), *Trust in government*, http://www.oecd.org/gov/trust-in-government.htm

Wright R. (2007), *Progress is not a zero-sum game*, TED talks, https://www.ted.com/talks/robert_wright_on_optimism/transcript?language=en

Roy S., Ellis C., Shiva S., Dasgupta D., Shandilya V., Wu Q. (2010), *A Survey of Game Theory as Applied to Network Security*, University of Memphis, http://ais.cs.memphis.edu/files/papers/Survey.pdf

Schmidt D., Brennan J. (2010), *Conceptions of Freedom*, "Cato Unbound Journal" https://www.cato-unbound.org/2010/03/10/david-schmidtz-jason-brennan/conceptions-freedom

Solove D.J. (2007), *'I've Got Nothing to Hide' and Other Misunderstandings of Privacy*, "San Diego Law Review" Vol. 44GWU Law School Public Law Research Paper No. 289, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565

Spijkers O. (2011), *The United Nations, the Evolution of Global Values and International Law*, Intersentia, Cambridge–Antwerp–Portland

The Fund for Peace (2016), *Fragile State Index*, http://fsi.fundforpeace.org/rankings-2016

World Economic Forum (2016), *The Global Risks Report 2016*, Geneva, http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf

Yadron D., Ackerman S., Thielman S. (2016), *Inside the FBI's encryption battle with Apple*, "The Guardian", http://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple