LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

GESCHWISTER-SCHOLL-INSTITUT
FÜR POLITIKWISSENSCHAFT

Münchener Beiträge zur Politikwissenschaft

herausgegeben vom
Geschwister-Scholl-Institut
für Politikwissenschaft

2018

von Aulock, Raphael

Online Privacy and Public Policy -
Does the Internet freedom status of countries correlate with the frequency and success of their governments engaging in formal user data requests to private companies?

Bachelorarbeit bei
Dr. Xavier Fernández-i-Marín
2018

Is it more gratifying to gain knowledge or to apply it?

I am about to find out.

Contents

Abstract

Governments request data and by doing so attempt to interfere with privacy. Unless they can provide a sufficient legal basis, companies will repel these requests. Companies also disclose who makes requests how often and on how many accounts they request data. More importantly they also publish how often these requests result in the disclosure of user data to governments. But who are these governments and what is their position when it comes to privacy on the internet? To find that out, data from the annual *Freedom on the Net* report is combined with the transparency reports by the most relevant tech companies worldwide to provide an overview and attempt to discover a connection between the Internet Freedom status of countries and their requests to companies about user data. The analysis shows that while countries with a worse Internet freedom score violate user right more often they not necessarily do so through formal requests and probably get their data elsewhere. On the other hand, many governments of freer countries willingly engage in the opportunity to legitimize their interferences with user privacy and are successful in doing so as many of their requests get answered. While the research question can ultimately be affirmed it's answer and the analysis itself give rise to a range of questions on the wider topic of online privacy and public policy.

Introduction

„Anna McDoogles: ‚Hi!'
Mark Bellison: ‚Hi!'
Anna McDoogles: 'You're early. I was just masturbating'
Mark Bellison: 'That makes me think of your vagina. I'm Mark. How are you?'
Anna McDoogles: 'A little frustrated at the moment. Also, equally depressed and pessimistic about our date tonight.'"

(The invention of lying 2009: 2:12-2:48)

This dialogue, of limited finesse, takes place between two characters at the beginning of the 2009 comedy *The Invention of Lying* directed by Ricky Gervais, when they first meet for a date. While the main premise of the movie isn't about not having any privacy but that the people in it are unable to lie, it still helps to bring across a point, essential to any paper about privacy and more so to a paper about privacy online. One might now wonder what bad dates and masturbation habits have to do with a scientific text on online privacy.
The answer is: Countering the "nothing to hide" argument right from the start. Fortunately, this is exactly what Daniel J. Solove must have thought when publishing an article on the topic in 2011, matching the theme of his book "Nothing to Hide" (see: Solove 2011). The notion that "privacy only aids wrongdoers" (Schneier 2015: 92) is used by many people to explain why they

don't care about the privacy of others or their own. Even if the people claiming to be open books have no real secrets, which according to Solove is unlikely, there are still situations where they most likely wouldn't want to share certain information with others. His examples include that many people wouldn't share their credit-card bills or agree to have their naked picture taken and shown to their friends and that many people use curtains (Solove 2011: 2). The latter is probably because the idea of other people, being able to observe oneself at any time and without one's knowledge, is at the very least uncanny.
The quote at the beginning of this introduction shows that a situation can get very awkward if even the most mundane little truths are unwillingly disclosed. Especially so if these truths do not relate to external factors but to one's opinions or beliefs that were rather kept private. In the case of the movie characters the situation is their natural state and therefore they are probably used to it, but to most people the idea of getting in a similar situation, deprived of the possibility to conceal private thoughts and opinions, is most likely more than appalling.

These examples, however, all relate to real life but as this paper has the topic of online privacy it takes things a little further, not only in terms of a provocative start. But what counts as private? Chapter 1 will settle on a definition of privacy and of what information is private. Privacy will be established as a human right that is worth protecting. More importantly it will also be determined that, and under which circumstances the right to privacy can legitimately interfered with by governments.
Dystopian fantasies such as George Orwell's *1984* or Dave Eggers *the Circle* present situations similar but less humorous than the scene from *The Invention of Lying* with the decisive difference being, that in their universes the people's lack of control over their own privacy is not caused by a state of nature but by technology. As technology in our world evolves more and more, seemingly catching up to science fiction with dreams of the past such as self-driving cars and artificial intelligence now becoming available to customers across the world, information collection too has evolved with private information being gathered from seemingly harmless data with sometimes striking accuracy. The second chapter will deal with online privacy and give insight into the technological process of how data is collected and interpreted and why companies and governments have an interest in private user data.
The theoretical part of this paper, consisting of Chapters one and two serves mainly to give an overview as to what privacy is and why it matters. The empirical part draws on the learning from previous chapters and tries to answer to the following research question and generate new insights by combining data Internet freedom by country from the *Freedom on the Net* (FOTN) report with data from different company transparency reports on requests for user data by governments:

Does the Internet freedom status of countries correlate with the frequency and success of their governments engaging in formal user data requests to private companies?

There are different reasons why this question is worth asking:

Firstly, for years a growing number of companies has regularly published data on the requests for user data they have gotten from governments (Accessnow 2017). Still, no systematic analysis of such reports has been done.
Secondly, the yearly FOTN reports evaluate the situation on the internet in different countries and score their Internet freedom according to different categories, one of which primarily deals with privacy (FOTN 2017). While the FOTN reports have drawn on transparency reports in the past they only did so regarding content removal requests but have neglected requests for user data.
Thirdly, the Internet Freedom ratings, that are based on qualitative source material, with quantitative data on user requests can lead to new insights on the motivations of the governments that request user data and whether these motivations determine how successful they are in doing so. The data sets themselves cover a majority of the word population and a majority of typical user online behaviour worldwide, thus possibly allowing the perception of global trends regarding the relationship between companies and governments on the topic of user data disclosure. To answer the research question two hypotheses will be phrased:

H1: *The governments of countries that have a less free internet according to the Freedom on the Net report, request user data from private companies more frequently.*

H2: *The governments of countries that have a freer Internet according to the Freedom on the Net report, get their requests to private companies for user data granted more frequently.*

An affirmation of the research question based on the validation of these hypotheses through the analysis would give rise to a new inquiry. As this paper is limited in its extent the question of causality will be left untouched until further and more detailed research is done.
Before a cross data analysis can take place, the first empirical part of the paper deals with the outlining of the data that is later used. In Chapter 3 the Freedom on the Net report 2016 and its ratings of the Internet freedom in 65 are presented and evaluated. Data from 2016 is used as the companies whose transparency reports are processed in the analysis had not yet published their data for all of 2017 at the time of writing. *Apple, Facebook, Google, Microsoft* and *Twitter* are outlined as the companies that best represent the worldwide average online behaviour and where government request data is available. Another task undertaken in the third chapter, is to harmonize the data of the transparency reports. This is done by combining the data from all five companies allowing for a broader perception of the facts and thus more meaningful conclusions. Methodology as well as some particularities and limits of the data are also addressed in chapter three. The last chapter deals with the hypotheses that are made and based on the information presented in previous chapters. Following the combined analysis and discussion of the data, the learnings, limits and potential benefits from this paper are presented in the conclusion.

Chapter 1: Privacy in Real Life

The following chapter aims to convey an understanding of what the right to privacy is and by exploring different definitions and examples, showing what role, it can play in the lives of people. Furthermore, it is established why privacy cannot be unconditional, how is protected and what exactly can be regarded as private. Finally, a definition to be used for the rest of this paper is settled upon.

Privacy is About control

In ancient Greece the concept of a distinction between private and public life already existed. In their works, both Socrates and Aristotle attributed relevancy to the distinction between the political (public) and the private (Moore 2013: 1). Just as good and bad, darkness and light or old and new, the concept of privacy or private life only works when opposed to publicity or public life, meaning that there can only be private information if public information exists as well.

Evidently all information becomes somewhat public as soon as is it shared with others. Is should be pointed out, that publicity is not an absolute. For example, sharing one's personal phone number with a new acquaintance doesn't mean that the phone number should also be known by advertising company. This follows Parent's Definition of privacy, stating that "privacy is the condition of not having undocumented knowledge about oneself possessed by others" (1983: 269).

The creation of publicity is not always an active process and it can be difficult to keep track of what knowledge about oneself is shared with others. Mundane actions as going for an ice cream in the park, mean that basic elements of identity are automatically shared with everyone one might cross or interact with (Lessig 2006: 39). Unless going through great lengths it is nearly impossible to venture among other people, making the following information about oneself public:

- approximate age
- sex
- skin colour
- height and physique
- health status, if one sneezes for example

Once arrived at the ice cream stand, to get an ice cream, again, one must disclose further information to the people around. This information is now disclosed voluntarily as one expects something in return:

- All the above
- That one is in possession of money
- The location of one's money or credit card

- The flavour of ice cream one likes
- That one is or is not lactose intolerant (unless vegan is an option)
- Whether one is a cup or a cone person
- The sound of one's voice
- One's general mood

The above list is incomplete and there is a plethora of other information that is revealed in such a simple process. Much of the information disclosed in daily life is automatically shared reciprocally, meaning that while a person shares information on their identity, they are also able to collect similar information about others. Thus, a certain balance is created based on the silent agreement that information is shared when venturing among others.

Consciously and unconsciously, people control the information flow towards others, thus creating privacy (Westin 1967: 9). This can be achieved by disclosing or secluding information from others. One might want to keep a controversial hobby from superiors at work, on the other hand, this same person might tell their date about it, to assess whether they both share the same interests. Most information is inherently open to interpretation as well as misinterpretation, which is why people constantly try to influence it (Gross: 1971: 209). A woman wearing makeup and high heels might want to look younger and more attractive than she is, while a man wearing what looks like an expensive watch, might do so to show that he has achieved something and that he can provide for others. They both control what information about them is known to others.

Privacy on a matter can only be achieved by actively keeping certain information from others. Posner sees it as the "right to conceal discreditable facts about oneself" (1981: 46), essentially defining privacy as a right to secrecy. Inness on the other hand, also sees privacy as a form of control, but rather than negative things the focus of her definition lies on the things that matter to the individual on an emotional level (1992: 91), a more neutral definition as emotions can be both negative and positive.

Privacy is not About Control at Any Cost

Like the ancient Greek philosophers, John Stuart Mill also made the distinction between private life and public life. For him "The only purpose for which power can be rightfully exercised over any member of a civilized community, against his will, is to prevent harm to others" (1978: 9). Everything that went beyond this scope could therefore be viewed as an unrightfully exercise of power. A problem clearly occurs with this depiction of legitimate and illegitimate as soon as the point of view is changed. What might be considered as legitimate harm prevention by one, might be considered as an illegitimate cause of harm to another.

Mill further points out, that harm could not only occur by active behaviour, but both by "*doing and allowing*" (Moore 2013: 3). One can do harm or allow harm and one can do good or allow good. This also is true for a governments behaviour towards privacy:

Allowing harm to privacy:
A situation where privacy is or can be violated or violation is facilitated is neglected by the government.

Doing harm to privacy:
A situation where privacy is or can be violated or violation facilitated is created by the government.

Allowing good for privacy:
The government doesn't take steps to strengthen privacy, but it does not prevent efforts by others.

Doing good for privacy:
A situation where privacy is or can be violated or violation facilitated is tackled by the government.

John Locke wanted to secure the rights to property, to life and liberty and to do so, he was ready to subjugate to a set of rules enforced by the government (Locke 1980: 5-30). Like Mill, everything that did not help the protection of those rights, meant that whatever happened behind closed doors not threatening the rights of any individual, would not fall under the jurisdiction of government.

In conclusion, if a government or any other entity would interfere, passively or actively, with said actions behind closed doors without a legitimate reason, such action or inaction could be considered as a violation of privacy. This has been understood by many. So many that the most basic instance of privacy law can be found in Article 12 of the Universal Declaration of Human Rights (UDHR), ratified on December 10th, 1948. It states that:

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to protection of the law against such interference or attacks"

The issue of validity and the issue of justification are two problems the UDHR is facing when it comes to the protection of individual human rights. As its name states, the UDHR demands to be universally valid. It is not, as many people and even whole governments may strongly oppose individual human right claims (GCC 2016: 36). However, the UDHR has since its adoption partially transited into customary international law and has in many countries been adapted into binding national law. In countries or regions where it hasn't it is to be a model (GCC 2016: 34). As the UDHR was not phrased to be a fixed

set of rules but "living document" it is not supposed to settle all the issues but asks for renewed attention as the world changes (GCC 2016: 14).

Drawing from the UDHR two kinds of interference with privacy can be deducted from article 12. The word "arbitrary" suggests that an interference with the right to privacy is only problematic if it takes place without a fixed set of rules, suggesting that any interference with privacy backed by some form of legal framework, might be justified and therefore not viewed as a violation. For countries that have adopted national legislation aiming for the protection of privacy in their national legislation, the phrasing issue should prove to be less problematic as in countries that haven't.

Some interferences with privacy are sure not to be controversial, one being the prosecution of crime. Following a crime, it is imperative for law enforcement to get their hands on Information which can be used to identify the offender, and that to do so a suspect's privacy might be interfered with seems entirely justifiable.

Legally rooted measures

If an individual's privacy is interfered with by another entity this is not a violation of the right to privacy, so long as the reason for the interference is grounded by law in the country where a person is staying. If for instance a citizen of a country with strong privacy laws travelled to a country with very weak ones, the traveller will have to submit to his privacy being interfered with in a way that would not be allowed in his home country. As mentioned above, views differ from country to country, but a government has authority over its territory as well as behaviour taking place within it. Governments limit themselves through law, so if a privacy violation would be in conflict to other superior law the country has submitted to, it could be challenged. This could be the case if privacy is protected in the constitution or if the government has agreed to respect international standards such as the UDHC. In liberal democracies privacy must for instance, be a central part of the political system as the secrecy of the vote is vital to the concept of the leaders being elected according to the peoples will (Moore 2013: 9).

Not legally rooted measures

In accordance with the Art. 12 of the UDHC, any interference with privacy that is not somehow legally rooted can be challenged as a violation (Morinsk 1999: 138-142). While it is safe to say that some concepts such as the assassination of a political figure, child molestation or harmful hacking, can be considered a crime virtually everywhere, on other offences views may once again, strongly differ.

As many different countries with sometimes strongly differing world views will be scrutinized in the upcoming analysis, it would not be proper to deliberate what kind of specific behaviour should be considered as legitimate or illegitimate. Taking the side of privacy as a right worth protecting, but not under every circumstance, the analysis will only focus on looking at whether

steps to interfere with privacy have been taken or not. An assessment of the individual case to determine whether an action was justified or not will not be done.

Personally Identifiable Information as a Means to Make Privacy Tangible

After grasping different definitions and views on privacy the question remains: What counts as private and what counts as public? Moore's definition of privacy, summarizing it as "the right to control access to and uses of personal information and spatial locations" (2013: 5), seems to most fit the concept as it combines the different approaches proposed above. Whereas a differentiation between personal information and spatial location might make more sense in the real space, in the digital world there is only one point of access revealing all that can be revealed, namely the device one uses to access the net. As chapter 2 will show, today this most likely also includes location. The introduction of the concept of personally identifiable information (PII) can help to understand what counts as private and what as public.

There is however no general legal definition as of what Information exactly can be regarded as PII (Schwartz / Solove 2011: 1893). U.S. legislation often follows what is called a reductionist approach, meaning that its privacy regulations mostly focus on PII as enabling already identified individuals to be identified through that information (Schwartz / Solove 2011: 1873).
This neglects the aspect of identifiable information, namely information that does not refer to a person that is already identified but makes an unidentified person potentially identifiable. This so-called expansionist approach can be found in privacy legislation of the European Union (Schwartz / Solove 2011: 1874).
Schwartz and Solove go on to propose a definition of PII that expands on both the reductionist and expansionist approach, calling it PII 2.0. PII 2.0 covers "information [that] can be about an (1) identified, (2) identifiable, or (3) non-identifiable person." (Schwartz / Solove 2011: 1874). Together with an understanding of privacy according to Moore's definition, PII can be understood as information that can facilitate the process of finding out an individual's identity or trace them (Stevens 2012: 6). If this definition seems rather broad that is because it is meant to be. As will be shown in the next chapter almost everything and unlikely data even more can be or become PII and should therefore be seen as private and hence protected.

Learnings of Chapter 1: Privacy in Real Life

Since the ancient times there has been a distinction between public life and private life, a life hidden from the gaze of others. However nearly everything

and even the most mundane actions of daily life produce data that is open to scrutiny and interpretation by others. The right to privacy itself can be understood as the right to have control over personally identifiable information, data that can potentially be used to identify and track one down. Data produced in daily life can be collected, interpreted and potentially be used if people decide to look at it. Following the arguments of Mill and Locke, it can be understood that the right to privacy is worthy of protection but not at any cost. As the rights of others might be harmed from an unconditional right to secrecy the decision as to when one's privacy could be breached was put in the hands of governments. International law requires that interference with privacy can only be legitimized if justified by legislation.

Chapter 2: Privacy on the Internet

This chapter deals with privacy on the Internet and how every movement of a user can be tracked. Showing that technology is now able to accurately guess Information that users haven't actively decided to disclose and sometimes even wanted to keep secret, illustrates why privacy online is just as important as privacy in real life. The second part explores why and how these capabilities can and are used by companies and governments

Same but Different and Why That Matters

While privacy has been established as a relevant topic for the real space it is so in the digital space as well, as the technological ability to intrude in privacy has changed (Moore 2013: 9). The Internet as a global Information Network is changing. Changing from an anarchic space to a more regulable space (Lessig 2006: 200). It has been noted that the sharp rise in surveillance of digital communication asks for new elaborations as not only privacy is being threatened but also puts the freedoms of expression, of association and assembly at risk as well as groups of people such as journalists, activists, minorities and government critics, as their work also takes place in the digital world (CGG 2016: 52). It should be added that as technological progress advances in a seemingly unstoppable fashion more and more Information from real life becomes digitalized. As examples smartphones, cloud storage and more recently the Internet of Things (IoT) come to mind. As the lines between real and digital life get increasingly blurred it can be concluded that privacy laws should be effective in the real space and cyberspace alike. Whether they actually are nationally is not covered by the scope of this paper. Every time a user visits a website or uses an application linked to online services, private information, just like in real life, is disclosed.

"Everything you do on the Net produces data. That data is, in aggregate, extremely valuable, more valuable to commerce than it is to the government. The government (in normal times) really cares only that you obey some select set of laws. But commerce is keen to figure out how you want to spend your money, and data does that. With massive amounts of data about what you do and what you say, it becomes increasingly possible to market to you in a direct and effective way." (Lessig 2006: 216)

Many people believe that they are anonymous on the Internet, if they do not act under their real names. This false assumption has been named the Anonymity Myth, as every device accessing the Internet can be tracked. (Schwartz / Solove 2011: 1837). The first tool to track activity online is the so-called Internet protocol (IP) address. It is a unique number assigned to every device accessing the Internet. As it doesn't identify a person but only a device, companies have tried to argue that the IP does not count as personally identifiable information (Schwartz / Solove 2011: 1838). By the definition of PII used in this paper, it is, because it can be used together with other information to identify one person. The further technical process of how people

can be tracked online is not relevant, it suffices to say that everything people do online leaves traces and can therefore can potentially be tracked for different ends.

Data Collection and Interpretation

To get a better grasp of what can be and is tracked every person using an Internet browser today, be it on a mobile or a desktop device, can find out what data the websites they visit can collect on them. The Application *webkay* (webkay.robinlinus.com) for example, visualizes what data every website can potentially know about its users. The tool works in a very simple way. It is just a website showing all the information it can get about its current visitor. Information presented by this tool is to be viewed as an educated guess, according to the creator, however everyone can check for themselves whether their data is presented accurately. The following information can potentially be collected and used.

- Approximate location (coordinates, address, languages spoken at location, local time)
- Software used (operating system, browser, browser plugins)
- Hardware used (Display resolution, number of CPU cores, GPU model, device battery status)
- Connection (Local- and public IP address, service provider, connection speeds)
- Social media log in status
- Misuse clicks and auto- fill for phishing (the website can potentially exploit social media accounts of the user)
- Gyroscope orientation (only on mobile devices)
- Scan the local network for other devices

Whereas this information still doesn't pinpoint a certain person, implications about the person in front of the screen are made possible, and thus also the target marketing mentioned by Lessig. By the definition used in this paper most if not all of this information is potentially PII.

Depending on the type of service used, information like browsing history, contacts, appearance, for example when granting access to the camera, as well as user provided details, meaning everything the user inputs while using a service, might be collected (Kishore 2012).

Things however go further, with data not only being collected but also analysed and interpreted. The desktop web browser extension *Dataselfie* can be used to visualize that digital user generated data, just as data in real life is prone to interpretation and thus to the disclosure of information the user might not initially agree to disclose. Once installed and linked to a user's Facebook account, the application uses different machine learning algorithms and

application programming interfaces (API's) to predict the user's personality based on their interests in combination with the aforementioned user provided details, namely the users behaviour on the social network (Thi Duc / Flores Mir 2017). The explanation of what Dataselfie does exactly, is best left to the application itself:

"The extension tracks: clicks on likes in your newsfeed, clicks on newsfeed links to external sites, duration spent on different posts and the specifics of those posts (authors, images and text) in your newsfeed, anything you type, and time spent on Facebook overall." (Dataselfie FAQ)

After gathering data from a few days of use, the tracking allows the extension to create a digital output that makes data based assumptions on the following traits of the user:

- Top ten friends
- Top ten interests
- Keyword sentiment analysis
- Entity sentiment analysis
- Personality prediction
- Religious and political orientation
- Political orientation
- Shopping preferences
- Health, activities and other preferences
- Intelligence, life satisfaction, psychological gender and leadership qualities

While this example didn't use PII to identify a person, it self-generated critical PII by linking it to an already identified person. This shows how "Computer scientists are finding ever more inventive ways to combine various pieces of non-PII to make them PII." (Schwartz / Solove 2011: 1841)

The more data is collected the more accurate the results become. Just like in real life interpretation is prone to mistakes. This digital method is too. Still, the accuracy of such Facebook data analysis has already successfully been researched, showing that even sensitive information a user might have decided not to disclose, can be accurately guessed based on their interests (see Kosinski et al. 2013). This means that as opposed to real life that is spatially and sensory limited, on the Internet the user cannot really know and control what data is collected on him and what happens with it. As previously established, any action, and more so the actions online, leave behind information. And as much of this information can be used, misused and is even open to interpretation it becomes increasingly difficult for the individual to control who knows what.

However not all data collection interferes with the right to Privacy. The Internet can be divided into two spaces. The Clear Net or public domain can be

understood as the part of the Internet that is fully accessible to anyone using a search engine (Bergman 2001). Many Blogs (also political), news websites and forums fall under this aspect, while everything that is inherently hidden from the public eye because it is behind a password, such As E-Mails, Private Messages or closed message boards can be seen as private domain or part of the Deep Web (Bergman 2001). To engage in data collection from the private domain companies and governments need legitimization.

Data Processing by Companies

Companies can simply ask the user for permission to collect their data. Online Cookies (see Palmer 2005), that now must be accepted on nearly every first time visit to a website, are one way the user gives his permission for data collection. The Terms and Conditions one must agree to when signing up for new accounts determine what data can be collected by companies and what they can do with it (DeNardis /Hackl 2015: 3-4).

One might now wonder what happens to all the data that can be collected. In short: It helps companies make more money more efficiently just as it was noted in the Lessig quote above (2006: 206). Target advertising allows to generate much higher conversion rates than conventional advertising (Caudill / Murphy 2000: 13-14) and if companies use private data to offer tailor made services, users will be more attracted to the services that fit better to their needs. This seems like a win-win situation as companies can make ever more money and to do so, they invest in providing always better services the user can use seemingly free of charge. As services like google have become ubiquitous in private life and business it becomes increasingly difficult for users to opt out. While using an alternative and arguably worse search engine might still be manageable evading data collection altogether can be hard as an example shall shortly demonstrate.

There is even potential for trouble if data is unintentionally or even incorrect data disclosed by companies. Kosinski et al. gave the example of an unmarried woman whose pregnancy is unwantedly or incorrectly disclosed to her family through targeted ads (2013: 5802). In a culture where this is unacceptable the disclosure of such information might be fatal.
Sociologist Janet Vertesi made exactly that experiment, hiding her pregnancy from the prying eyes of big data. Her decision to limit the information she was giving to Internet companies, is perfectly in line with the notion the right to privacy as a form of control about private information. Later she wrote an article depicting how “opting out [of big data] is not only antisocial, but it can appear criminal” (2014) as she couldn’t talk about the pregnancy anywhere on social media, including private messages, had to withdraw large amounts of cash for the baby shopping and used special software to evade tracking while doing research on names.

Following her own attempts at keeping her data private, journalist Julia Angwing concludes that to evade tracking one must either have vast technological knowledge or be very rich (see 2014). Users today don't seem to really have a choice, other than allow the collection and processing of their private data if they want to stay fully functional in a society that so heavily relies on the services that use private data.

Data Processing by Governments

A State, as defined from a constitutional law perspective by Georg Jellinek (1900: 394-434), consists of three entities, namely: national territory, national population and state authority. The latter is known as government. It is a person or group of people; whose basic task is to rule over the national population living in the national territory the government holds state authority over. More specific tasks and limits of governmental powers can be found in national constitutions. The government derives its executive power from being the only entity of a nation able to make policies as well as enforce them. (Gerching / Kolmar 2014: 2-5). Governments too have increasingly wanted their shay and share of information in the world of online data, arguably to enforce the laws they have sworn to uphold on the Internet as well.

When reports of arrests and repercussions related to online activity surface, in many cases it remains unclear how exactly authorities gained knowledge of the reported actions. Oftentimes the alleged offence was carried out by sharing or publishing information in the public domain, such as on a website, a blog, or by publicly posting or sharing punishable information on public social media that can be viewed without an account (such as Twitter). This behaviour cannot be an interference with privacy as the alleged perpetrators intentionally shared said information in a publicly accessible space. Law enforcement therefore has no need to gain access to a space secluded from the public eye.

If governments do however access information that a user did not intentionally share in public, this must be regarded as an interference with the right to privacy and must therefore be justified. One example are the later analysed government requests. The fact alone that governments ask for the data instead of just looking it up means that it is most likely data that is not easy to access. Their motivations range from "national security, defamation, computer fraud and abuse, child protection, or, in some cases, blatant political oppression such as identifying dissident media sources" (DeNardis / Hackl 2015: 6)

In some cases, it is highly disputable whether a certain space is to be regarded as public or private space, as in in the case of certain social media posts. Publicly posting something on Facebook could be regarded as public speech but depending on individual privacy settings such as the "share only with friends" option it becomes disputable whether an action falls under privacy or

freedom of expression. As one needs an account to see other people's Facebook posts regardless of them being private or public they will herby be defined as private and thus needing justification if breached by governments. It should be noted though, that legislation varies from country to country. India (Hindustan Times 2017) and Germany (Noé 2015) for instance do not differentiate between the privacy settings of social media posts.

To collect data, some governments have instated so called online mass surveillance programs. The best-known ones are probably the programs by the U.S. and U.K. government spy agencies whose practices of mass collecting user data, were blown wide open in 2103 following the revelations of whistle-blower Edward Snowden (Greenwald 2013).

Although the U.S. Government insisted that it was only collecting metadata, consisting of times, duration and location of communications (Stanley / Wizner 2013), instead of contend data. Drawing, yet again, from the previous definition of what is private, such information, when interpreted correctly is sure to make people identifiable, even if the reductionist approach of the U.S. Government doesn't count it as such. That the data collected by these programs is critical regarding the right to privacy is derived from the fact that the governments had bypassed the encryption of service providers (Greenwald 2013)

British researcher Kieran Healy showed how metadata could have been used by the British in the 18th century (see 2013). Using only Information on what societies a set of 254 people were members of, he was able to single out Paul Revere, a US freedom fighter that was considered an enemy of the British Empire. What would have worked with only one set of information almost three hundred years ago shows, that with the help of today's technology, it would be easy to single out a person out of millions with only little more information.

Following the revelations of Edward Snowden, the U.S. National Security Agency (NSA) and the Government Communications Headquarters (GCHQ) of the U.K. were incorporated into the 2014 *Enemies of the Internet* report (Reporters without borders 2014) along with other intelligence agencies engaging in overeager and questionable surveillance across the world. The following countries are home to one or multiple government agencies capable of online mass surveillance (Reporters Without Borders 2014):
Bahrain, Belarus, China, Cuba, Ethiopia, India, North Korea, Russia, Saudi Arabia, Sudan, Syria, United Arab Emirates, United Kingdom, United States, Uzbekistan and Vietnam.

No update of the report was published by *Reporters Without Borders* as a request for the latest issue, in January 2018, has brought to light. Since this report additional countries have engaged or been found to engage in online mass surveillance. Germany recently reformed its Federal Intelligence Service law, regulating the *Bundesnachrichtendienst* (Eng. Federal Intelligence Service), and granting it vast online surveillance competences (Krempl 2016). Australia gained illegal access to user web browsing histories through service providers.

This was publicized in August 2014 (Grubb 2014), a few months after the last "Enemies of the Internet" report was published.

According to privacy protection by international law, all the above governments engaging in mass surveillance should have a sufficient legal basis to justify their behaviour. Whether they do, is not subject of the analysis but that they have the capability to engage in surveillance activities could influence how these governments request information from companies.

Learnings of Chapter 2: Privacy on the Internet

On the Internet, everything one does produce data. The main difference to the real world is that online every action also leaves a trace. A trace that that isn't only created if other individuals take interest but a trace that is constantly created by the storing of information by companies. A trace that is only waiting to be scrutinized and analysed by private companies and government agencies alike. While companies have the goal to make more money, governments can use data to enforce the rule of law on the Internet and real life alike. As the pregnancy example shows, while yet we don't live in a world where we are compelled to tell the truth as everything can be known, for the individual it becomes increasingly difficult and depending on resources maybe even impossible, to evade the look of big brother. The increased connectivity in all life situations means that ever more data is put online, and it becomes more and more impossible, to keep track of who knows what about oneself. With very little data very much can be found out, even if the data used does not relate directly to a person.

Chapter 3: Data and Methodology

The Following Chapter is the first empirical part of the paper and serves for setting stage for the analysis. By presenting the two main data sets, namely the Freedom on the Net report and the aggregate data of relevant transparency reports. The individual analyses explore what the data sets have to offer by carving out all the data that will be used in the combined analysis. Furthermore, some remarkable aspects of the data will be presented aside from the main research question. Methodical aspects and concerns possible as well as possible limits will also be outlined along the way.

The Freedom on the Net Report 2016

First started in 2011, the Freedom on the Net report (FOTN) by U.S. based non-government-organization *Freedom House* has analysed and ranked the political situation regarding the Internet in a growing number of countries around the globe. FOTN report was funded by the following institutions and private interest groups (FOTN 2017):

- U.S. State Department's Bureau of Human Rights and Labor (DRL)
- Google
- Schloss Family Foundation
- Dutch Ministry of Foreign Affairs
- Facebook
- Internet Society
- Yahoo
- Twitter

In 2016, the FOTN report included 65 countries from around the globe. Together they are home to 88% of the global Internet population (FOTN 2016: 32). 65 will also be the baseline of countries analysed. The FOTN reports asks a set of questions and sub-questions in every category. Based on the answers to individual sub questions points are given (FOTN 2016: 1015-1019). In total, these can amount to a score of 100 points with 0 being the best score and 100 the worst. From a score from 0 to 30, countries are regarded as having a "Free" Internet. 31-60 means that a country's Internet is "Partly Free" and everything above that is considered "Not Free" (FOTN 2016: 1013).
Fig. 1 (see: Appendix) discloses the Ranking of all countries from worst to best to give an image of the data being used. As seen in Fig. 1, data will, if possible, be colour coded to disclose the Internet freedom status of countries at a glance. The results show that 35% of the world Internet population lives in countries ranked as "Not Free", followed by 29% in partly "Partly Free" with potentially only a mere 24% of the world's total online population having access to "Free" Internet, as the remaining 12% are not assessed in the report (FOTN 2016: 6)

Countries are ranked in three categories:

Obstacles to Access [Max 25 points]:
“Details infrastructural and economic barriers to access, legal and ownership control over internet service providers, and independence of regulatory bodies” (FOTN 2016: 1013)

Limits on Content [Max. 35 points]:
“Analyzes legal regulations on content, technical filtering and blocking of websites, self-censorship, the vibrancy and diversity of online news media, and the use of digital tools for civic mobilization” (FOTN 2016: 1013)

Violations of User Rights [Max. 40 points]:
“Tackles surveillance, privacy, and repercussions for online speech and activities, such as imprisonment, extralegal harassment, or cyberattacks.” (FOTN 2016: 1013)

The FOTN report has excluded "legislation addressing harmful content" (FOTN 2016: 1018) from the “Violation of User Rights” category giving the examples of child pornography and malicious hacking. As this concerns only a sub question of the “Violations of User Rights” category the effects of this exception on the total score are limited. The implications however are further reaching, as the exclusion is not unconditional but selective.
The examples given in the report suggest that only internationally acceptable legislation has no effect on the score as the example of homosexuality shows. In Tunisia homosexuality is illegal (Code Pénal [Penal Code of Tunisia 2005]: Art. 230) and the ban enforced (FOTN 2016: 824), while in Russia the online distribution of “homosexual propaganda” on social media has been punished (FOTN 2016: 683). In the Netherlands for instance, the exact opposite is the case, the defamation of homosexuality is illegal and can be punished with up to a year in prison (Criminal Code [of the Netherlands] 2012: Art. 137c). No case of prosecution could be found which might be why this legislation is not in the report.
Still, it demonstrates that homosexuality is a disputable topic, as the stance towards it can vary between nations. Although the Officials in Tunisia and Russia were acting in accordance with local law their behaviour has been flagged in the report as it is problematic from a global perspective. Because such disputable cases were not excluded from the report, it becomes apparent that only globally accepted interference with privacy doesn’t influence the final score.

Out of the 65 countries studied on the report 24 have restricted social media over the course of 2016. Some countries have blocked some services temporarily, while others block most of them durably. The services blocked include: Facebook, WhatsApp, Twitter, YouTube, Telegram, Skype and Instagram.
Whether one or more services were blocked temporarily or permanently cannot be taken into consideration, as the exact extent of such blockings is not comprehensible in all cases. People can also use circumvention tools to get

around the barriers and hide their identity online, thus further blurring the validity of the data. As it is evident that if access to services is complicated through blockings, users will have to actively override the restrictions and possibly go against the law, a decision that is presumably not going to be made by 100% of users. Some countries even forbid so called Virtual Private Networks (VPN) and put the use under harsh punishment (FOTN 2016: 7). While it is likely that blocking has a negative effect on the use of the blocked social networks the aforementioned factors limit the potential of social media blocking to provide final explanations. Of the countries that block Social media a majority is "Not Free" while only two "Free" countries have experienced blocking (Fig. 2).

Fig. 2: Countries That Have Had Social Media Applications Blocked in 2016

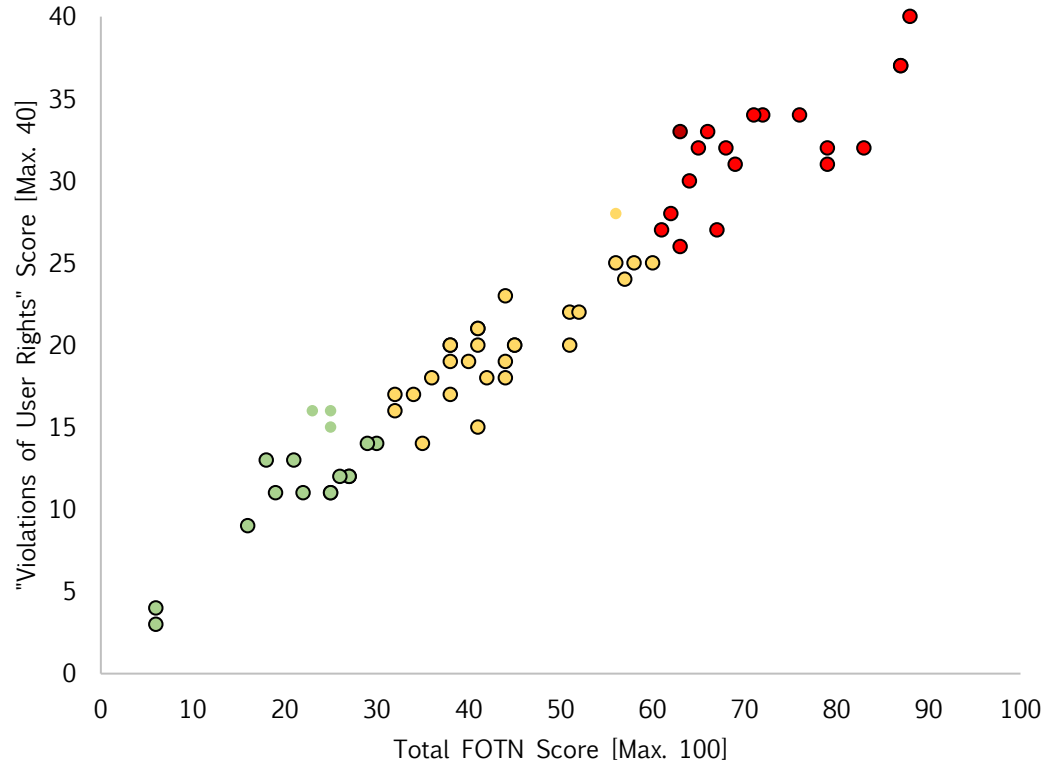
China
Iran
Ethiopia
Uzbekistan
Cuba
Vietnam
Saudi Arabia
Bahrain
Pakistan
United Arab Emirates
Gambia
Kazakhstan
Egypt
Turkey
Bangladesh
Zimbabwe
Jordan
Malaysia
Indonesia
Morocco
Uganda
Brazil
Armenia
Georgia

Background legend:
Free (0-30)
Partly Free (31-60
Not Free (61-100)

While "Obstacles to Access" can be seen as the category disclosing a country's general stance towards Internet use by its people (FOTN 2016: 1015-1016), the "Limitations on Content" category focuses on censorship efforts (FOTN 2016: 1016-1018), thus dealing mainly with freedom of expression. They are

both not central to the questions asked but as part of the total score they help to give a better image of a country's overall position on Internet policy. "Violations of User Rights" essentially deals with privacy violation, as much of the behaviour addressed in the country reports either deals with direct privacy interference (FOTN 2016: 1018), or actions taken by the government that suggest a preceding interference with privacy, such as arrests following online behaviour (FOTN 2016: 1019) for example due to social media posts or private messages. Some of the questions asked in the report also deal with government behaviour that is passively against privacy, such as a lack of adequate protection of the user rights whose violation is addressed in the report (FOTN 2016: 1019).

Figure 3: Countries by "Violation of User Rights" Score in Relation to Total FOTN Score



Legend:

●/●/ = "Free"/"Partly Free" country having a higher Violations of user Rights score than some countries that are a rating category higher

●/●/● = country with "Free"/"Partly Free"/"Not Free" rating

To give a more complete image however, the focus will not lie only on the "Violations of user Rights category but the total score will be used for the comparison with transparency report data. That this is a reasonable approach can be seen in Fig. 3. The number of points in the "Violation of User Rights" score with, a minimum of 0 and a maximum of 40, rises proportionally to the total score, as the linear trend line shows. This leads to the conclusion that countries with a less free Internet are more likely to violate user rights and thus to interfere with privacy. As this paper primarily aims to give a good

overview of global behaviour, the discussion of the data from the combined analysis will be limited to the rating categories rather than individual scores. For the analysis itself the exact total scores will be used. In the discussion "Free" Countries will be expected to be less invasive and "Not Free" ones to be more, while "Partly Free" countries are expected to occupy the space in between the other categories while some deviations will be accepted. Individual "Free" or "Not Free" countries deviating from their expected behaviour will be standing out

Deviation can be understood as being them clearly positioned at the opposite side of the average or median respectively, as compared with most of the countries in the same rating category. A tolerance of 5% will be applied to avoid discussion of countries that are positioned around the average and therefore not overly meaningful.

There are some exceptions however (circled in white) that need to be taken into consideration. While It has been established that the score of the category rises proportionally to the total score, meaning that "Not Free" countries engage more in behaviour interfering with privacy violating behaviour than "Free" countries, while "Partly Free" countries are mostly set in between. Things can look different however look when the "Violation of User Rights" score is looked at in proportion to the total score.

Fig. 4: Countries with the Highest Proportion of Their Total Score Due to User Right Violation

Rank	Country	Overall FOTN Score [Max. 100]	Violations of User Rights Score [Max. 40]	Percentage of Total Score
1	United States	18	13	72%
2	United Kingdom	23	16	70%
3	Iceland	6	4	67%
4	France	25	16	64%
5	Australia	21	13	62%
6	Italy	25	15	60%
7	Thailand	66	33	59%
8	Germany	19	11	58%
9	Canada	16	9	56%
10	Brazil	32	17	53%
...				
19	Japan	22	11	50%
-	*Average*	*46,6*	*21,5*	*48%*
37	China	88	40	45%
...				
65	Malawi	41	15	37%

Background legend:

Free (0-30)

Partly Free (31-60

Not Free (61-100)

(full table in the appendix)

Of the countries with the highest proportion of their total score coming from user right violations 8 out of 10 have been classified as "Free" and of the total 17 "Free" countries covered in the report, ten lie above the general average of 48%. Of these the lowest ranking country is Japan. Still, 50% of its total score comes from user right violations. While it must be mentioned that with a Maximum of 40 points the "Violation of User Rights" category is the strongest of the three, this is equal to all countries and as China demonstrates, ranking at 36th while maxing out on user violation, a below average proportion of the total score stemming from user rights violation is possible with enough points in the other two categories. This leads to conclusion that while "Free" countries overall have more favourable policies and practices regarding the internet Internet, their negative aspects are more likely to be focused on user rights. This doesn't have much impact as the score of these free countries is still lower than the scores of the countries in a worse rating category. The exceptions are the following:

The U.K.	is rated higher than	Malawi, Kyrgyzstan and Colombia
France	is rated higher than	Malawi, Kyrgyzstan and Colombia
Italy	is rated higher than	Malawi and Kyrgyzstan
Bangladesh	is rated higher than	Kazakhstan, Turkey, Gambia and Myanmar

Should unexpected behaviour occur with these countries during the analysis, the higher score of the U.K. France and Bangladesh countries might explain it, however only if anomalies occur in relation to the countries they are higher rated as. As the differences are slight the impact might still be questioned but as the individual country reports only disclose the total score in every category, individual statements in the reports cannot clearly be associated to an individual sub question. Therefore, these slight differences might exactly relate to the points given for behaviour that is relevant to the unexpected outcome.

Transparency Report Selection

Transparency reports have first been released in 2010, with the first one being published by Google. Since then 68 companies worldwide have been disclosing how often they get requests for data disclosure from governments (Accessnow 2017). In transparency reports companies disclose who they have gotten requests from. Therefore, it is safe to assume that the governments of countries that do not show up in the report have not issued any requests.
To best cover the global Internet population as well as use cases in which data is produced, the biggest companies in five categories are devised to accurately mirror average online behaviour. Referring to a 2011 study on the most popular activities online (Purcell 2011: 2) they should be:

- Send or read email
- Use a search engine

- Get news online
- Buy a product online
- Social network sites

As no recent studies are available on online behaviour, a crucial aspect of today's online behaviour has been left out. Internet access through mobile devices has been rising over the past years and globally surpassed Internet usage via desktop in late 2016 (StatCounter 2016). To better mirror these recent developments the "Send or read email" category will be changed "Messaging".
Another issue arises with the category "Get news online" as it has been found that today people of all demographics in the United Kingdom (Kleis Nielsen 2016) and the U.S (Gottfried /Shaerer 2016: 2) get much and sometimes most of their online news from social media. It might be problematic to draw global conclusions from this behaviour but as many of the world's most influential technology companies come from the U.S., the country can be seen as an innovator (2015 :38-39) and thus also a forerunner in the adoption of new behaviour. Furthermore, there don't seem to be media companies big enough as to argue that most of the World gets their online news from them. The "Get news online" category will therefore be changed to "Operating System" as the operating system of a device does not only provide the user with a digital ecosystem but most operating system have a built-in news functions, where the content displayed is controlled by the manufacturer. The five categories are therefore as follows:

- Use a messaging application
- Use a search engine
- Operating system
- Buy a product online
- Social network sites

For each category the two most important companies will be selected. Important means primarily the companies with the highest popularity by number of countries, the most users worldwide or the company with the biggest revenue or political significance.

Use a messaging application:
With the two most popular messaging applications belonging to Facebook, the company becomes the first to be selected in this category. Facebook offers a transparency report since 2013. The third place goes to the Rakuten owned app "Viber" (Schwartz, J. 2016). Unfortunately, Rakuten does not offer a transparency report and the same goes for Tencent with their messaging app "WeChat", that is widely popular in China and beyond.

Use a search engine:
When it comes to search engines Google has been the market leader for some time, steadily holding its global market share above 90% throughout

2016. It is followed by the "Bing" search engine from Microsoft (StatCounter 2016). Both companies regularly publish transparency reports.

Operating system:
At the End of 2016 Microsoft's "Windows" operating System was the most popular worldwide across all platforms with just below 39% of global market share. It was tightly followed by Googles "Android" operating system at 38%. As both Google and Microsoft are already on the list of companies with transparency reports, a look at the third and fourth place reveals that at the end of 2016 Apple had a combined market share of about 18% with its operating systems "iOS" and "OS X" for mobile and desktop respectively (StatCounter 2016). Apple has also been publishing a transparency report.

Buy a product online:
According to Global Power of Retailing 2016 report by advisory firm Deloitte, the list of the Top 50 e-retailers is topped by Amazon and followed by Apple. While Amazon does disclose data about government requests it does so in detail only for the U.S., not offering individual data on other countries (Amazon 2017). The third and fourth spot are held by Walmart and JD.com respectively. They also do not publish transparency reports on government requests.

Social networking:
Facebook is the uncontested king of social media with 86% of global market share at the end of 2016. It is followed by Pinterest at 7% and Twitter at 4% (StatCounter 2016). While Pinterest does offer a transparency report it doesn't receive many requests at all only received 1 foreign request in 2016 and 2015 (Pinterest 2017). It's significance to governments is therefore questionable. On the other hand, Twitter has proven to be a sensible political tool, most notably during the Arab Spring (Huang 2011) and more recently through the Tweets by U.S. President Donald Trump (Apps 2016). It can be argued that the social media site, despite not being in the top spot in terms of market share, is of higher relevancy to this paper.

Fig. 5: Availability of Transparency Reports for 2016

Category:	Messaging	Use a Search Engine	Operating System	Buy a Product Online	Social Networking
Rank 1	Facebook	Google	Microsoft	Amazon	Facebook
Rank 2	Facebook	Microsoft	Google	Apple	Pinterest
Rank 3	Rakuten		Apple	Walmart	Twitter
Rank 4	Tencent			JD.com	

Legend:

Data available
Data unusable
No data

As can be seen in Fig. 5, out of the most important companies in the five categories mirroring average Internet use, not all of them provide usable data about Government requests. Nevertheless, the companies that do, share a

combined 90% of global browser market share, 94% of operating system market share, as well as 90% of global social media market share and most of the Messaging market share across all platforms. The only category falling short of such high coverage is online shopping, as the e-commerce market is globally very diversified and therefore Apple alone cannot be used as a representative of all the other players, despite being the second most important e-commerce company worldwide (Deloitte 2016: 36-37). Still, in the light of this paper focusing on government behaviour rather than potential marketing interests of companies, it seems safe to assume that private messages and social media behaviour are more relevant to governments than shopping patterns in most cases.

Criteria for Data Disclosure

To understand in which cases data is disclosed by companies following a request by governments, their individual criteria should be noted:

Figure 6: Company Requirements for Data Disclosure to Governments

	Apple	Facebook	Google	Microsoft	Twitter
Legal basis required	X	X	X	X	X
Warrant required	X			Sometimes	Sometimes
Company policies relevant			X		
Company opinion relevant	X	X	X		X

The criteria for data disclosure by individual companies (Fig. 6), show that they tend to be on the customer side, by strongly protecting user rights with multiple conditions tied to the disclosure of user data. All require a legal basis and sometimes even a warrant, for instance if content data is requested (Microsoft, Twitter). Requesting a legal basis means that Companies essentially protect their users from misuse of their data by governments (DeNardis / Hackl 2015: 5). The reports themselves do not all distinguish between content and non-content data types of data. That they don't is irrelevant for the analysis because as established in previous chapters already very little PII in combination with today's technology allows for accurate derivation of a lot more than the information that the initial data disclosed. This means that even if very little data is shared, data that might not even qualify as PII depending on legislation, this data can have far reaching implications as it can clearly be attributed to a certain user. The example of Dataselfie showed what can be achieved with seemingly harmless data when it is tied to an already identified individual.

Furthermore, most of the companies grant themselves discretionary powers. While Apple defends its users from potentially hidden intents by rejecting

requests with a questionable scope (Apple 2016 [1]: 1), Twitter, for instance, reserves itself the right to reject data requests "depending on the nature of the underlying crime" (Twitter 2017) and Google states that requests have to comply with their own policies in addition to being based on law (Google 2017).

The high market share of these Internet companies in their respective fields, shows that only a few global players control most of the data flow of typical Internet behaviour. This means, that if a government wants to know what is going on most of the Internet, they must rely on the companies that collect it to give them the data. This becomes increasingly relevant as companies keep governments at bay, not only with administrative but also technical barriers such as encryption (WhatsApp 2017), a growing trend in the tech industry that has already had legal consequences (Mott 2016). If their individual criteria are not met, the companies don't disclose any data essentially saying "no" to governments

These policies are clearly in favour of the user, but this behaviour shows that, in addition to their already vast power in terms of relevancy and market share, private companies now also have the power to decide what is good or bad. As they are all American companies it is safe to assume that they also advocate western values which might be good from a western point of view. Different world views however might be put to a disadvantage if the requests of some governments are being rejected based on a private company's view of what is acceptable and what is not. This potentially undermines one of the central tasks of governments, namely to enforce the rule of law in the country they govern by putting it at the mercy of private companies.

Data Extraction

The analysis is limited in its level of detail and it aims to depict global trends rather than give final answers. Therefore, the amount of government requests is added together across all companies to cover the broadest possible spectrum. A more profound analysis on individual reports would allow for detailed conclusions on individual topics. The Information appearing in the reports varies in detail and content from company to company, but the three following data sets represent the core information of the transparency reports and could be retrieved from all five reports for the whole of 2016.:

Total number of requests by country (see: Appendix Fig. 7):
The total number of requests refers to the amount of individual times each government has requested one or more user data sets from one of the companies. These numbers could simply be added together across all half-yearly reports country by country. The numbers vary strongly between countries ranging from 0 total requests to 95031. The average lies at 4040 requests per country and the median at 15.

Total number of accounts referenced (see: Appendix Fig. 8).:
The total number of accounts referenced refers to the individual people the governments have asked data about. These numbers as well could simply be added together across all half-yearly reports country by country. Here too, the numbers vary strongly between countries ranging from 0 user accounts referenced to 188801. The average lies at 6742 user accounts referenced per country and the median at 20.

Total percentage of requests where some data was produced (see: Appendix Fig. 9):
Some reports disclose the percentage of request that resulted in the disclosure of "some data". From the percentage of positively answered requests the number of positively answered requests could be calculated. Other reports directly disclosed how many requests resulted in data disclosure. By adding them together and dividing the sum of total requests by the sum of requests that where positively answered, the total percentage of requests where some data was produced could be calculated (Fig. 9). The average of positively answered requests is 28%. Twitter points out that some requests get rejected because they refer to inexistent data or because governments didn't reply to further inquiries by the company (2016). As this refers to administrative issues when dealing with requests if this happens with requests to Twitter it most likely also happens with some requests made to other companies. Most likely the amount such administrative rejections does not amount to over two thirds. This would be especially questionable, because as one request can refer to multiple user accounts, if one account doesn't exist, data on other accounts from the same request might still be disclosed making the request count as granted. Again, as the data in the transparency reports is quantitative no definite conclusions can be made as to how often this phenomenon occurs.

Of the 65 countries analysed only 73%, or 48 countries, made any requests at all. countries that didn't make any requests were excluded from the calculation of as a division by zero is impossible. They will therefore also not be included in comparisons involving the data from Fig. 9. Comparisons involving the sums of requests or user accounts referenced can include these countries, as knowing that a country didn't make any requests can also prove to be useful information. For instance, by combining the total amount of requests and user accounts referenced with data on population in every country (Source: Internet Live Stats 2016; World Bank 2016), the number of requests per capita can be calculated. This discloses which countries request the most data from companies relative to their population. Using data on online population (see: Appendix Fig. 10) puts the absolute number of requests in perspective as countries with a very high population might also make more request. Using the number of Internet users in every country instead of general population data additionally adjusts for possible variations of internet penetration between the countries, regardless of it fluctuating due to technology diffusion or because governments make it difficult for users to access the internet:

Government Requests relative to internet population (see: Appendix Fig. 11):
On average 6,20 requests for user data were made per 100.000 Internet users. The Median is 0,13 requests for user data were per 100.000 Internet users.

User accounts referenced relative to internet population (Fig. 12):
On average 12,18 user accounts were referenced per per 100.000 Internet users. The Median is 8,81 requests per 100.000 Internet users.

As individual values vary strongly between countries for most data sets the Median will be more relevant in the upcoming analysis featuring the data from the FOTN report. Still, the average can be used which countries rank significantly higher than others when looking at the whole bandwidth of countries. Only in data sets involving percentages the average can be used as primary value for comparison as values are closer together (Fig. 9)

Learnings of Chapter 3: Data and Methodology

While the FOTN report determines the number of countries that will be looked at during the analysis, the availability of transparency reports determines 2016 as the year being studied. It has been shown that the "Violations if User Rights" score increases proportionally to the overall Internet freedom score and while less free countries also violate user rights more, "Free" countries get a majority of their score from user right violations tied to interference with the right to privacy. This leads to some exceptions in the linearity of proportion between "Violations of user Rights" score and total FOTN score that could be of precise relevance when explaining unexpected outcomes of "Free" and "Partly Free" countries rating higher than some countries of a worse category. A similar but limited relevancy has been attributed to the blocking of social media, mainly engaged in by les free countries.
After establishing the most common actions of Internet behaviour, five relevant companies, namely Apple, Facebook, Google, Microsoft and Twitter, that best represent ordinary global online behaviour, have been selected and the data from their transparency reports combined. Together with data on Internet population the government requests and user accounts referenced per capita could be determined, disclosing which governments use the option to request personal data from Internet companies the most. Companies disclose information only in less than a third of cases worldwide and decide whether they do not only based on a sufficient legal framework but also by applying individual requirements for data disclosure. It has therefore been argued that a governments ability to enforce the law can be undermined by some of these companies as they control and protect significant parts of data flow that could be relevant to national law enforcement.

Chapter 4: Analysis

This chapter combines the data of both sources previously established to attempt an answer to the research question of this paper. The first hypothesis is based on the results of the Freedom on the Net report. It is then falsified by using data from the transparency reports. Following the discussion, a second hypothesis that tries to explain the results of the first analysis is established and investigated. Again, limits are discussed when they are encountered. Finally, the research question is answered in the conclusion of the paper that not only aims to bring the results to terms but also offers ideas for subsequent research.

Analysis and Discussion of the First Hypothesis

Based on the Freedom on the Net report, countries with a higher score in the "User rights Violation section" interfere more with privacy. As user rights violation rises proportionally to the total score, the latter can be used to determine which countries are more likely to interfere with user privacy. Based on the definition of Privacy and of PII in Chapter 1 requests for user data can be asserted to be an attempted interference with privacy. Therefore, countries with a higher FOTN score should be more likely to engage in it.
Based on what was learned about mass surveillance in Chapter 2, it is possible that countries that engage in it might be less depending on company requests. A similar assumption can be made regarding social media censoring as a more difficult accessibility most likely results in less usage of the blocked content. Of the seven applications that have been blocked in 2016, all except for messaging app Telegram, are owned by companies whose transparency report data has flowed into the calculation of user accounts referenced relative to online population data. Less usage of these services could mean less need for requests. It is therefore arguable that the blocking of social media could have some effect on the results. How requests were justified is not disclosed in the reports thus limiting social media blocking as a valid explanation. A tendency might still be identifiable.
Combining FOTN data in the form of country scores and data on who has blocked social media, with the ranking of countries with the most government user accounts referenced per capita and expanded with data on mass surveillance capabilities by country, the examination of a first hypothesis is made possible:

H1: *The governments of countries that have a less free Internet according to the* Freedom on the Net *report, request user data from private companies more frequently.*

Fig 13: Countries by Accounts Referenced per 100.000 Internet Users in Combination with FOTN Report Data and Surveillance Ability Data

Rank	Country	Accounts referenced per 100.000 Internet Users	Mass surveilance	Social media blocked
1	Singapore	87,8447		
2	Germany	72,6830	X	
3	United Kingdom	71,5772	X	
4	United States	65,7975	X	
5	France	60,1787		
6	Turkey	33,5543		X
7	Australia	32,1913	X	
8	Italy	29,2338		
9	Argentinia	17,7702		
10	Estonia	13,3721		
11	Hungary	13,0290		
12	Brazil	12,8351		X
-	*Average*	*8,81*	-	-
...				
49	Syria	0	X	
49	Ethiopia	0	X	X
49	Uzbekistan	0	X	X
49	Cuba	0	X	X
49	Vietnam	0	X	X
49	Gambia	0		X
49	Myanmar	0		
...				
49	Kyrgyzstan	0		

Background legend:

Free (0-30)
Partly Free (31-60
Not Free (61-100)

(full table in the appendix)

The combined data (Fig. 13) shows that unlike expected the ranking is not led by "Not Free" countries as the worst possible offenders but that the higher ranks, meaning above average, are almost exclusively dominated by "Free" countries, with Singapore and Brazil being the only exceptions. As already identified earlier, the scores differ in an extreme manner making the median a more suitable comparison tool. Still, all "Free" countries except Kenya lie above it.

To give an explanation, should the data not mirror the hypothesis, mass surveillance and possibly the blocking of social media have been carved out as factors that could have an influence.

Some countries without any requests (Cuba, Ethiopia, Syria, Uzbekistan, Vientnam) have surveillance capabilities, meaning that they might not need to request data from companies due to them. Countries with surveillance capabilities can also be found among the highest-ranking countries (Australia, Germany, U.K., U.S.), showing that surveillance capabilities don't seem to have a decisive effect on government requests for user data from private companies.

As the data shows, when it comes to the number of per capita requests, "Free" countries, that did not block social media, mostly top the list, while less free countries, that have blocked social media in 2016, often have considerably less or even no requests at all. The idea of social media as a factor of potentially major influence on the frequency of government requests is challenged when looking at countries that neither have surveillance capabilities nor did they block social media. Those countries would arguably have a need for information disclosure by companies as those companies' services are readily available to their populations and they don't seem to the have the technical abilities to get the data on their own.

As could be seen in the case of the recently discovered surveillance programmes by the NSA or the surveillance by the Australian government, government practices, of interfering with the right to privacy, are sometimes hidden. Therefore, it cannot be known which other programs haven't yet been discovered. This means that despite the FOTN report finding that less free countries engage more in privacy violation than others, they don't necessarily do so by requesting user data from exactly these companies. While it is questionable if all countries that did not have any or many requests engage in hidden and undiscovered mass surveillance one possible factor might be that people of interest to those governments use less popular services that are not covered by this analysis.

The lack of any trend has made it obsolete to exactly check the exceptions established based on the "Violations of User Rights" score in Chapter 3. The U.K., Italy and France for instance are all among the highest-ranking countries in terms of User accounts referenced per capita despite them having a low "Violations of User Rights" score.

Summing up it can be said, that governments with a higher FOTN score are not more likely to request data from private companies and that neither surveillance capabilities nor, the blocking of social media can give a sufficient explanation as to why they are not, as no clear trend could be identified. Further analysis of countries that do not follow the trend is therefore not necessary.

Deduction, Analysis and Discussion of the Second Hypothesis.

The question remains as to why many "Free" countries would try to interfere with privacy significantly more than most "Partly Free" and "Not Free" countries.

The following aspects should be taken into consideration when looking for an answer.

Firstly, the significantly higher interference with privacy of many "Free" countries, as opposed to their less free coequals, has only been observed in the case of government requests to the companies whose reports were observed. Other aspects, not covered by this data, have not and cannot be considered in this paper. Still, one should bear in mind that these five companies account for a majority of typical online behaviour, thus a certain relevancy cannot be denied.

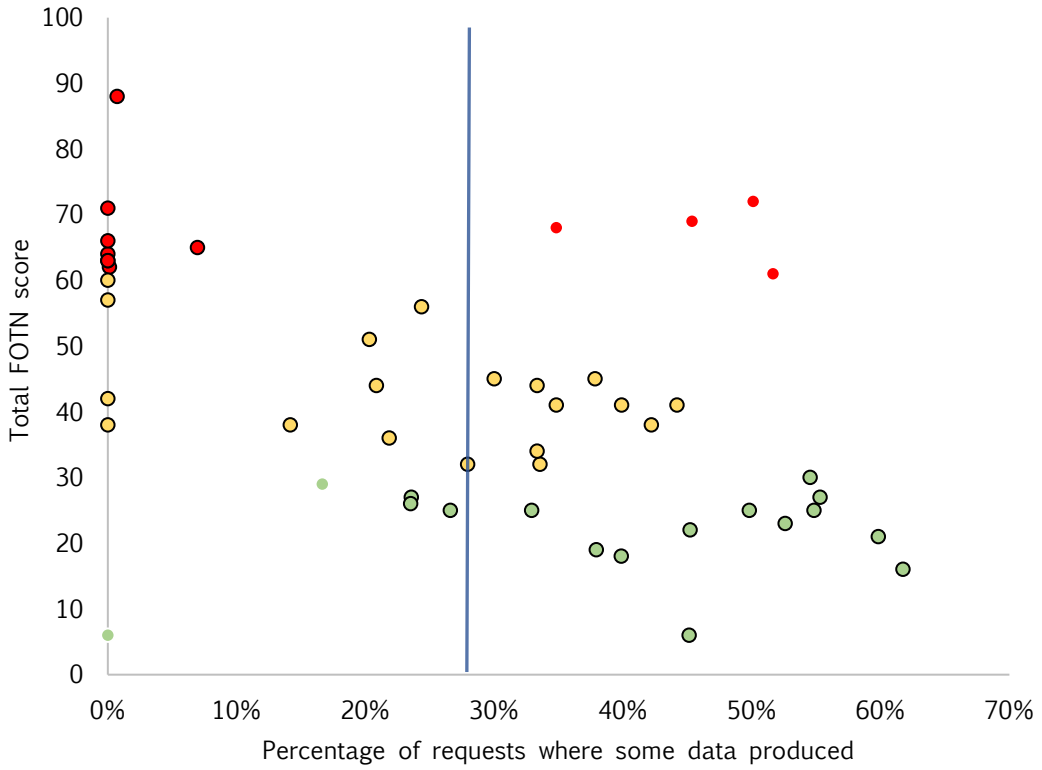
Secondly, the interference with privacy the "Free" countries engage in could be a justified one. As held on in the UDHR, interference with privacy is justifiable if backed by corresponding law. The five companies providing the data for this analysis all require sufficient legal justification to consider disclosing any data. This means that while many "Free" countries engage in interference with privacy by means of user data request more often than many countries with a score that is much worse, they might do so in a legal way.

Thirdly, the FOTN report does not include globally justifiable interference with privacy. The fact that both Freedom House and all companies providing the data used are American, suggests that they are likely to support similar notions of what is good or bad. This common ground of morale becomes evident the moment it is considered that the FOTN report is financially supported by three of the five companies, namely: Google, Facebook and Twitter, as they would not endorse a report that contradicts their own views. That the companies' views matter was shown in their criteria for data disclosure following government requests. This all means, that legislation that is likely to be accepted as legitimate by the companies is also likely to be excluded from the FOTN report and therefore not have an impact on the score.

For governments to profit from all this, their culture wouldn't necessarily have to be rooted in western culture as the correlation of views is a mere possibility. If their policies and practices, follow Freedom House's notion of what is good and bad they should get a lower score on the FOTN report. Then, when making requests for user data based on these policies that are unproblematic, governments of freer countries should het a higher portion of their requests answered positively as opposed to countries that have problematic ones. This leads to the following second hypothesis:

H2: *The governments of countries that have freer Internet according to the Freedom on the Net report, get their requests to private companies for user data granted more frequently.*

Figure 14: Countries by Total FOTN Score in Relation to Positively Answered Requests



Legend:

= Average of requests where "some data produced" (28%)

= "Free" / "Not Free" countries above or below average

= Country

The combined data of FOTN score and positively answered requests (Fig. 14) discloses that the countries group together according to their rating category. "Free" countries tend to have an above average percentage of their requests answered, while "Not Free countries get little to none answered. "Partly Free" countries expectedly occupy the space around the average with only some getting none of their requests answered. There are also some exceptions that fall out of line (circled in white). Four "Not Free" countries (Turkey, Saudi Arabia, Pakistan, United Arab Emirates) are above the five 5% margin of appreciation relative to the average of 28% while the results of two "Free" countries (Iceland, Kenya) lie more than 5% below it. These exceptions are a minority (12%).

Furthermore, almost all "Free" countries, that ranked above the Median (8,81) of user accounts referenced per 100.000 internet users in the first analysis (see: Fig. 13) can be found among the countries with an above average amount of positively answered requests. Hungary is the only exception.

The assumption the hypothesis was based upon, namely that free countries engage more in government requests because their interferences with privacy get legitimized more often, has proven true and therefore the hypothesis itself can be confirmed.

Fig 15: Country Data on Percentage-, Total- and Per Capita Data and on government requests

Rank	Country	Total % of requests where some data produced	Total requests for user data	Requests per 100.000 internet users
1	Canada	62%	2130	6,631
2	Australia	60%	6067	29,338
3	Argentinia	55%	4152	13,676
4	Georgia	55%	86	4,086
5	Armenia	55%	17	1,125
6	United Kingdom	53%	28673	47,572
7	Turkey	52%	12940	28,011
		Majority line (50+%)		
8	Saudi Arabia	50%	154	0,740
9	France	50%	27295	48,863
10	Pakistan	45%	1752	5,102
...				
19	United Arab Emirates	35%	55	0,646
20	India	35%	21760	4,709
21	Colombia	34%	755	2,729
22	Nigeria	33%	11	0,013
23	Sri Lanka	33%	3	0,049
24	Italy	33%	7233	18,446
25	Lebanon	30%	17	0,374
26	Brazil	*Average =* 28%	8111	5,831
...				
29	Bangladesh	24%	68	0,32
29	Hungary	24%	691	8,775
...				
34	Kenya	17%	4	0,019
...				
38	Iceland	0%	1	0,301
...				
38	Tunisia	0%	1	0,018
38	Uganda	0%	1	0,013
38	Kazakhstan	0%	1	0,010
38	Venezuela	0%	1	0,005
38	Egypt	0%	1	0,003

Legend:

Free (0-30)
Partly Free (31-60
Not Free (61-100)

(full table in the appendix)

The low scores of Iceland and Kenya can clearly be attributed to their very low number of overall requests (see: Appendix Fig. 15). One factor strongly limiting the significance of the data is that 38% (or 18 out of 48) countries, including the two exceptions among the "Free" countries, made under twenty requests in total (see: Appendix Fig. 15). In these cases, getting only one request being granted or rejected results in a variation of the score of at least 5%. In the case of six countries (Iceland, Kazakhstan, Venezuela, Uganda, Egypt, Tunisia) that only made one request the difference was instantly 100% to the negative (see: Appendix Fig. 15). These countries, except Iceland, were "Partly Free" or not "Free". The general trend however, remains persistent even if these countries were to be excluded from the account. This is mainly because out of the seven countries that got a majority (above 50%) of their requests granted, six (Canada, Australia, Argentina, Georgia, Armenia, U.K.) were rated as "Free" with Turkey being the only exception. These countries made above 20 requests, meaning that their scores are comparatively stable.

While relatively clear conclusions can be made on "Free" countries, the same cannot be said for the exceptions among "Not Free" countries. The "Not Free" countries that got a higher than expected proportion of requests granted all had relatively strong positions by having made more than 20 requests (see: Appendix Fig. 15). One reason could be that as pointed out in Chapter 3 one request can reference multiple accounts the disclosure of information on only one account would make a request count as "some data produced".
Another explanation could simply be that because a country's FOTN score suggests that it is more likely to engage in unjustifiable interference with privacy, it does not mean that it can't also engage in justified interference. While these countries can still engage in problematic behaviour in other situations, when it comes to requests to companies they have probably learned what works best. To verify this, research combining transparency reports of multiple years with the corresponding FOTN reports could provide the necessary insights even without knowing what laws where applied as justification for individual requests.

Conclusion

The first hypothesis assumed, that countries that are more likely to engage in interference with privacy do so through formal requests for user data to private companies. It had to be negated because no trend confirming this was evident from the available data. Alternative influencing factors that had previously been devised also couldn't offer an explanation. Further research on the topic should be promising is it is arguable that all countries want to get some data from somewhere.

The results of the first analysis showed that "Free" countries use the opportunity to get data from governments more often. The second hypothesis assumed that "Free" countries make so many requests because theirs get granted more often. This could be confirmed but had to be put into perspective as the extreme fluctuation of requests between countries cannot be plausibly explained based on Freedom on the Net data.

In Chapter 2 it was established that government agencies engage in surveillance and that some are even capable of bypass encryption. This hasn't kept "Free" countries with these capabilities to indulge in a disproportionally high amount of user data inquiries as opposed many less free countries with similar capabilities that made no requests at all. As it is arguable that all governments have an interest in governing cyberspace to some extent the question remains as to where the countries that did not make any requests nor had surveillance capabilities get their data from.

The guidelines for data disclosure showed that adequate legislation is possibly not the only requirement to get access to user data from companies. Combined the they only granted 28% of requests whereas it is unlikely, that so many requests simply failed due to administrative complications. While things might look different from company to company their global market power and their ability to say "no" to governments gives rise to many implications ranging from internet governance by companies to the crippling of a governments ability to act.

This paper, while lacking to give any final answers due to the limitations by data and because of the global approach to the topic, has given impulses for a range of further research topics and was ultimately able to confirm its research question, determining that there is in fact some interaction between the Internet freedom status and how governments engage in user data requests.

Bibliography

Reports

Apple (2016) [1]: Report on Government Information Requests: January 1 – June 30, 2016.
[online] https://images.apple.com/legal/privacy/transparency/requests-2016-H1-en.pdf [last visited on January 8th, 2018]

Apple (2016) [2]: Report on Government and Private Party Requests for Customer Information: July 1-December 31, 2016.
[online] https://images.apple.com/legal/privacy/transparency/requests-2016-H2-en.pdf [last visited on January 8th, 2018]

Amazon (2015): Amazon information Request Report.
[online] http://d0.awsstatic.com/certifications/Information_Request_Report.pdf [last visited on January 8th, 2018]

Deloitte (2016): Global Powers of Retailing 2016. Navigating the new digital divide.
[online]https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Consumer-Business/gx-cb-global-powers-of-retailing-2016.pdf [last visited on January 8th, 2018]

Facebook (2016): Government Requests Report.
[online] https://govtrequests.facebook.com [last visited on January 8th, 2018]

Freedom House (2016): Freedom on the Net 2016 [online]
https://freedomhouse.org/sites/default/files/FOTN_2016_Full_Report.pdf [last visited on January 8th, 2018]

Google (2017): Transparency Report.
[online] https://transparencyreport.google.com/user-data/overview [last visited on January 8th, 2018]

Pinterest (2017): Transparency Report.
[online] https://help.pinterest.com/en/articles/transparency-report [last visited on January 8th, 2018]

Reporters Without Borders (2014): Enemies of the Internet 2014. [online]
https://rsf.org/sites/default/files/2014-rsf-rapport-enemies-of-the-internet.pdf [last visited on January 8th, 2018]

Twitter (2016): Transparency Report [online]
https://transparency.twitter.com/en/information-requests.html [last visited on January 8th, 2018]

References

Angwin, Julia (2014) *Dreagnet Nation*. New York: Times Books.

Caudill, Eve M. (Murphy, Patrick E. (2000): Consumer Online Privacy: Legal and Ethical Issues, in Journal of Public Policy & Marketing, vol. 19, no. 1, pp. 7-19.

DeNardis, L. / Hackl. A. M. (2015) Internet governance *by* social media platforms, in: Telecommunications Policy, vol. 39, no. 9, pp 761-770.

Gerching, Kristofel R. / Kolmar, Martin (2014): The States's Enforcment Monopoly and the Private protection of Property, in: Journal of Institutional and Theoretical Economics, vol. 170, no. 1 pp. 5-23.

Gross, H. (1971): Privacy and Autonomy, in Roland Pennock / John W. Chapman (eds.), *Privacy: Nomos XIII*. New York: Atherton, pp. 169–81.

Innes, Julie C. (1992): *Privacy, Intimacy and Isolation*. Oxford: Oxford University Press.

Jellinek, Georg 1900 [1914]: *Allgemeine Staatslehre*, 3rd Edition. Berlin: Verlag von O. Häring.

Kosinski, Michael / Stillwell, David / Graepel, Thore (2013): Private traits and attributes are predictable from digital records of human behaviour, in: *Proceedings of the National Academy of Sciences*, vol. 110, no. 15, pp. 5802 – 5805.

Lessig, Lawrence (2006): *Code version 2.0*. New York: Basic Books.

Locke, J. 1980 [1690]. *The Second Treatise of Government*, ed. C. B. Macpherson. Indianapolis: Hackett.

Mill, J. S. 1978 [1859]. *On Liberty*, ed. E. Rapaport. Indianapolis: Hackett.

Moore, Adam D. (2013): Privacy, in Ed. Hugh LaFolette *The International Encyclopedia of Ethics*, Hoboken (NJ): Blackwell Publishing Ltd., pp. 4099-4110.

Morinsk, Johannes (1999): *The Universal Declaration of Human Rights: Origins, Drafting, and Intent*. Philadelphia: University of Pennsylvania Press.

Palmer, Daniel E. (2005): Pop-Ups, Cookies, and Spam: Toward a Deeper Analysis of the Ethical Significance of Internet Marketing Practices, in: *Journal of Business Ethics,* vol. 58, no. 1-3, pp. 271-280.
Parent, W. A. (1983): Privacy, Morality and the Law, in: *Philosophy and Public Affairs*, vol. 12, no, 4, pp 269-288.

Pick, James B. / Sarkar Avijit (2015): *The Global Digital Divides: Explaining Change*. Berlin: Springer-Verlag.

Posner, Richard (1981): *The Economics of Justice*. Cambridge: Harvard University Press.

Rosen, Jeffrey (2000): *The Unwanted Gaze: The Destruction of Privacy* in America. New York: Random House.

Schneier, Bruce (2015): Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York: Norton & Company.

Schwartz, Paul M. / Solove, Daniel J. (2011) The PII Problem: Privacy and a NEW Concept of Personally Identifiable Information, in: *New York University Law Review*, vol. 86, pp. 1814 – 1984.

The Global Citizenship Commission [GCC] (2016): The Universal Declaration of Human Rights in the 21st Century. A Living Document in a Changing World. New York, *Global Institute for Advanced Study* NYU.

Westin, Alan F. (1967): *Privacy and Freedom*. New York: Atheneum.

Online Sources

Accesnow (2017): Transparency Reporting Index.
[online] https://www.accessnow.org/transparency-reporting-index/ [last visited on January 8th, 2018]

Apps, Peter (2016): Commentary: Trump's brave new world of Twitter Diplomacy, in: Reuters.
[online] https://www.reuters.com/article/us-apps-twitter-commentary/commentary-trumps-brave-new-world-of-twitter-diplomacy-idUSKBN13U2VX [last visited on January 8th, 2018]

Bergman, Michael K (2001): White Paper: The Deep Web: Surfacing Hidden Value, in: Journal of Electronic Publishing, vol. 7, no. 1
[online] https://quod.lib.umich.edu/j/jep/3336451.0007.104?view=text;rgn=main [last visited on January 8th, 2018]

Facebook (2017): About government Requests.
[online] https://transparency.facebook.com/government/about/ [last visited on January 8th, 2018]

Freedom House (2017): About Freedom on the Net.
[online] https://freedomhouse.org/report-types/freedom-net [last visited on January 8th, 2018]

Gottfried, Jeffrey / Shaerer, Elisa (2016): New Use Across Social Media Platforms 2016, in: Pew Research Center.
[online] http://www.journalism.org/2016/05/26/news-use-across-social-media-platforms-2016/ [last visited on January 8th, 2018]

Greenwald, Glenn (2013): Revealed: how US and UK spy agencies defeat internet privacy and security, in The Guardian.
[online] https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security [last visited on January 8th, 2018]

Grubb, Ben (2014): Telstra found divulging web browsing histories to law enforcement agencies without a warrant, in: The Sydney Morning Herald.
[online] http://www.smh.com.au/digital-life/digital-life-news/telstra-found-divulging-web-browsing-histories-to-lawenforcement-agencies-without-a-warrant-20140819-106112 [last visited on January 8th, 2018]

Healy, Kieran (2013): Using Metadata to find Paul Revere.
[online] https://kieranhealy.org/blog/archives/2013/06/09/using-metadata-to-find-paul-revere/ [last visited on January 8th, 2018]

Hindustan times 2017: Offensive posts against SC/ST on social media a punishable offence: Delhi HC. [online] http://www.hindustantimes.com/cities/offensive-posts-against-sc-st-on-social-media-a-punishable-offence-delhi-hc/story-gwGvoHuMuazlimTDEFjh2H.html [last visited on January 8th, 2018]

Huang, Carol (2011): Facebook and Twitter key to Arab Spring uprisings: report, in: The National. [online] http://www.l2f.inesc-id.pt/~fmmb/wiki/uploads/Work/misnis.ref01.pdf [last visited on January 8th, 2018]

Internet Live Stats (2016): Internet Users by Country (2016).
[online] http://www.internetlivestats.com/internet-users-by-country/ [last visited on January 8th, 2018]

Kishore, Aseem (2012): What Type of Data do Websites Collect About You, in online-tech-tips.
[online] https://www.online-tech-tips.com/computer-tips/what-type-of-data-do-websites-collect-about-you/ [last visited on January 8th, 2018]

Kleis Nielsen, Rasmus (2016): Where do people get their news?, in: Medium.
[online] https://medium.com/oxford-university/where-do-people-get-their-news-8e850a0dea03 [last visited on January 8th, 2018]

Krempl, Stefan (2016): BND-Reform: Bundestag beschließt Internetüberwachung a la NSA, in: Heise.
[online] https://www.heise.de/newsticker/meldung/BND-Reform-Bundestag-beschliesst-Internetueberwachung-a-la-NSA-3356543.html [last visited on January 8th, 2018]

Ministère de la Justice de la République tunisienne (2005): Code Pénal.
[online] http://www.e-justice.tn/fileadmin/fichiers_site_francais/codes_juridiques/Code_penal_12_07_2010_fr.pdf [last visited on January 8th, 2018]

Mott, Nathaniel (2016): Take that, FBI: Apple goes all in on encryption, in: The Guardian.
[online] https://www.theguardian.com/technology/2016/jun/15/apple-fbi-file-encryption-wwdc [last visited on January 8th, 2018]

Noé, Isabell (2015): Hetzen, Pöbeln, Lästern: Was darf man auf Facebook?, in: n-tv.
[online] https://www.n-tv.de/ratgeber/Was-darf-man-auf-Facebook-article15886256.html [last visited on January 8th, 2018]

Purcell, Kristen (2011): Search and E-Mail still top the list of most popular online activities. Two activities nearly universal among internet users, in: Pew Internet Project.
[online] http://www.pnrc.net/wp-content/uploads/2011/02/Search-and-email-still-yop-the-list-of-most-popular-online-activities.pdf [last visited on January 8th, 2018]

Schwartz, Joseph (2016): The Most Popular Messaging App in Every Country, in The Market Intelligence Blog.
[online] https://www.similarweb.com/blog/worldwide-messaging-apps [last visited on January 8th, 2018]

Solove, Daniel J (2011) Why Privacy Matters Even if You have 'Nothing to Hide', in: The Chronicle of Higher education.
[online] https://www.chronicle.com/article/Why-Privacy-Matters-Even-if/127461 [last visited on January 8th, 2018]

Stanley, Jay / Wizner, Ben (2013): Why the government wants your metadata, in Reuters.
[online] http://blogs.reuters.com/great-debate/2013/06/06/why-the-government-wants-your-metadata/ [last visited on January 8th, 2018]

StatCounter (2016): Global Stats.
[online] http://gs.statcounter.com/press/mobile-and-tablet-internet-usage-exceeds-desktop-for-first-time-worldwide [last visited on January 8th, 2018]

Stevens, Gina (2012): Congressional Research Service. Data Security Breach Notification Laws, in: Federation of American Scientists, File no. R42475.

[online] https://fas.org/sgp/crs/misc/R42475.pdf [last visited on January 8th, 2018]

Thi Duc, Hang Do / Flores Mir, Regina (2017): Dataselfie. [online] http://dataselfie.it/#/about [last visited on January 8th, 2018]

Universal declaration of Human rights (1948).
[online] http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf [last visited on January 8th, 2018]

Vertesi, Janet (2014): My Experiment Opting Out of Big Data Made Me Look Like a Criminal, in: Time. [online] http://time.com/83200/privacy-internet-big-data-opt-out/ [last visited on January 8th, 2018]

WhatsApp (2017): Android Security and Privacy: End-to-End Encryption.
[online] https://faq.whatsapp.com/en/android/28030015/?category=5245250 [last visited on January 8th, 2018]

Wike, Richard et al. (2017): Manny unhappy with current political system, in: pew global.
[online] http://www.pewglobal.org/2017/10/16/many-unhappy-with-current-political-system/ [last visited on January 8th, 2018]

Willem III, King of the Netherlands (2012): Wetboek van Strafrecht. Criminal Code of the Netherlands. English Version.
[online] http://www.ejtn.eu/PageFiles/6533/2014%20seminars/Omsenie/WetboekvanStrafrecht_ENG_PV.pdf [last visited on January 8th, 2018]

Worldbank (2016): Population 2016.
[online] http://databank.worldbank.org/data/download/POP.pdf [last visited on January 8th, 2018]

Illustration Directory

Sources:
Internet Live Stats (2016): Internet Users by Country (2016).
[online] http://www.internetlivestats.com/internet-users-by-country/ [last visited on January 8th, 2018]

World Bank (2016): Population 2016.
[online] http://databank.worldbank.org/data/download/POP.pdf [last visited on January 8th, 2018]

Figure 11: Combined Amount of Government Requests for user data per 100.000 Internet users
Own diagram depicting information based on the transparency by Apple, Facebook, Google, Microsoft and Twitter and data by Internet Live Stats
Sources:
See: Bibliography > Reports

Internet Live Stats (2016): Internet Users by Country (2016).
[online] http://www.internetlivestats.com/internet-users-by-country/ [last visited on January 8th, 2018]

Figure 12: Combined Amount of User Accounts Referenced by Governments per 100.000 Internet Users
Own diagram depicting information based on the transparency by Apple, Facebook, Google, Microsoft and Twitter and data by Internet Live Stats
Sources:
See: Bibliography > Reports

Internet Live Stats (2016): Internet Users by Country (2016).
[online] http://www.internetlivestats.com/internet-users-by-country/ [last visited on January 8th, 2018]

Figure 13: Countries by Accounts Referenced per 100.000 Internet Users in Combination with FOTN report Data and Surveillance Ability Data
Own table listing information from the Freedom on the Net 2016 report, information from Figure 11 and from Reporters Without Borders as well as different news articles.
Sources:
See: Appendix > Figure 11

Freedom House (2016): Freedom on the Net 2016 [online]
https://freedomhouse.org/sites/default/files/FOTN_2016_Full_Report.pdf [last visited on January 8th, 2018]

Grubb, Ben (2014): Telstra found divulging web browsing histories to law enforcement agencies without a warrant, in: The Sydney Morning Herald.
[online] http://www.smh.com.au/digital-life/digital-life-news/telstra-found-divulging-web-browsing-histories-to-lawenforcement-agencies-without-a-warrant-20140819-106112 [last visited on January 8th, 2018]

Krempl, Stefan (2016): BND-Reform: Bundestag beschließt Internetüberwachung a la NSA, in: Heise.
[online] https://www.heise.de/newsticker/meldung/BND-Reform-Bundestag-beschliesst-Internetueberwachung-a-la-NSA-3356543.html [last visited on January 8th, 2018]

Reporters Without Borders (2014): Enemies of the Internet 2014. [online]
https://rsf.org/sites/default/files/2014-rsf-rapport-enemies-of-the-internet.pdf [last visited on January 8th, 2018

Figure 14: Countries by total FOTN score in relation to positively answered requests
Own diagram depicting information based on Figure 1 and Figure 9
Sources:
See: Illustration Directory > Figure 1; Figure 9

Figure 15: Country data on percentage-, total- and per capita data and on government requests
Own Table listing information Based on Figure 7, Figure 9 and Figure 11
Sources:
See: Appendix > Figure 7; Figure 9; Figure 11

Appendix

Due to the large number of countries being compared some figures were to large to be displayed or entirely displayed in the continuous text. They can be found here. The sources are disclosed in the Illustration directory.

Figure 1: Freedom on the Net 2016 Total Scores

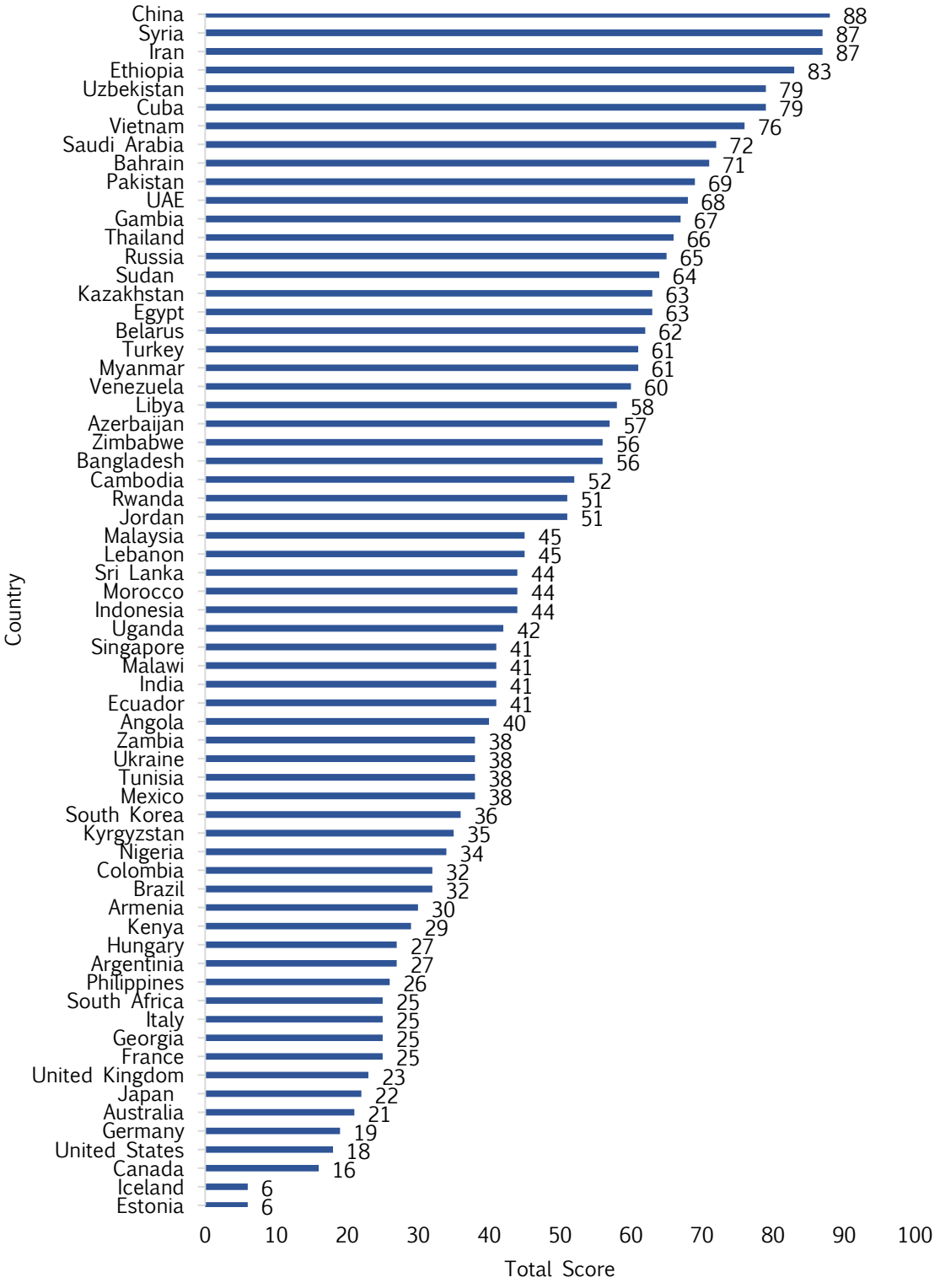


Figure 4: Countries with the Highest Proportion of Their Total Score due to user Right Violation

Rank	Country	Overall FOTN Score [Max. 100]	Violations of User Rights Score [Max. 40]	Percentage of Total Score
1	United States	18	13	72%
2	United Kingdom	23	16	70%
3	Iceland	6	4	67%
4	France	25	16	64%
5	Australia	21	13	62%
6	Italy	25	15	60%
7	Thailand	66	33	59%
8	Germany	19	11	58%
9	Canada	16	9	56%
10	Brazil	32	17	53%
11	Mexico	38	20	53%
12	Tunisia	38	20	53%
13	Morocco	44	23	52%
14	Egypt	63	33	52%
15	Singapore	41	21	51%
16	Ecuador	41	21	51%
17	Bangladesh	56	28	50%
18	Estonia	6	3	50%
19	Japan	22	11	50%
20	Colombia	32	16	50%
21	Nigeria	34	17	50%
22	South Korea	36	18	50%
23	Ukraine	38	19	50%
24	India	41	20	49%
25	Russia	65	32	49%
26	Bahrain	71	34	48%
27	Kenya	29	14	48%
28	Angola	40	19	48%
29	Armenia	30	14	47%
30	United Arab Emirates	68	32	47%
31	Saudi Arabia	72	34	47%
32	Sudan	64	30	47%
33	Philippines	26	12	46%
34	Zimbabwe	56	25	45%
35	Pakistan	69	31	45%
36	Vietnam	76	34	45%
37	China	88	40	45%
38	Zambia	38	17	45%
39	Belarus	62	28	45%

40	Georgia	25	11	44%
41	Malaysia	45	20	44%
42	Turkey	61	27	44%
43	South Africa	25	11	44%
44	Argentinia	27	12	44%
45	Hungary	27	12	44%
46	Lebanon	45	20	44%
47	Myanmar	61	27	44%
48	Uganda	42	18	43%
49	Indonesia	44	19	43%
50	Jordan	51	22	43%
51	Iran	87	37	43%
52	Libya	58	25	43%
53	Syria	87	37	43%
54	Cambodia	52	22	42%
55	Azerbaijan	57	24	42%
56	Venezuela	60	25	42%
57	Kazakhstan	63	26	41%
58	Cuba	79	32	41%
59	Sri Lanka	44	18	41%
60	Gambia	67	27	40%
61	Kyrgyzstan	35	14	40%
62	Uzbekistan	79	31	39%
63	Ethiopia	83	32	39%
64	Rwanda	51	20	39%
65	Malawi	41	15	37%

Background legend:

Free (0-30)
Partly Free (31-60
Not Free (61-100)

Figure 7: Total Requests for User Data

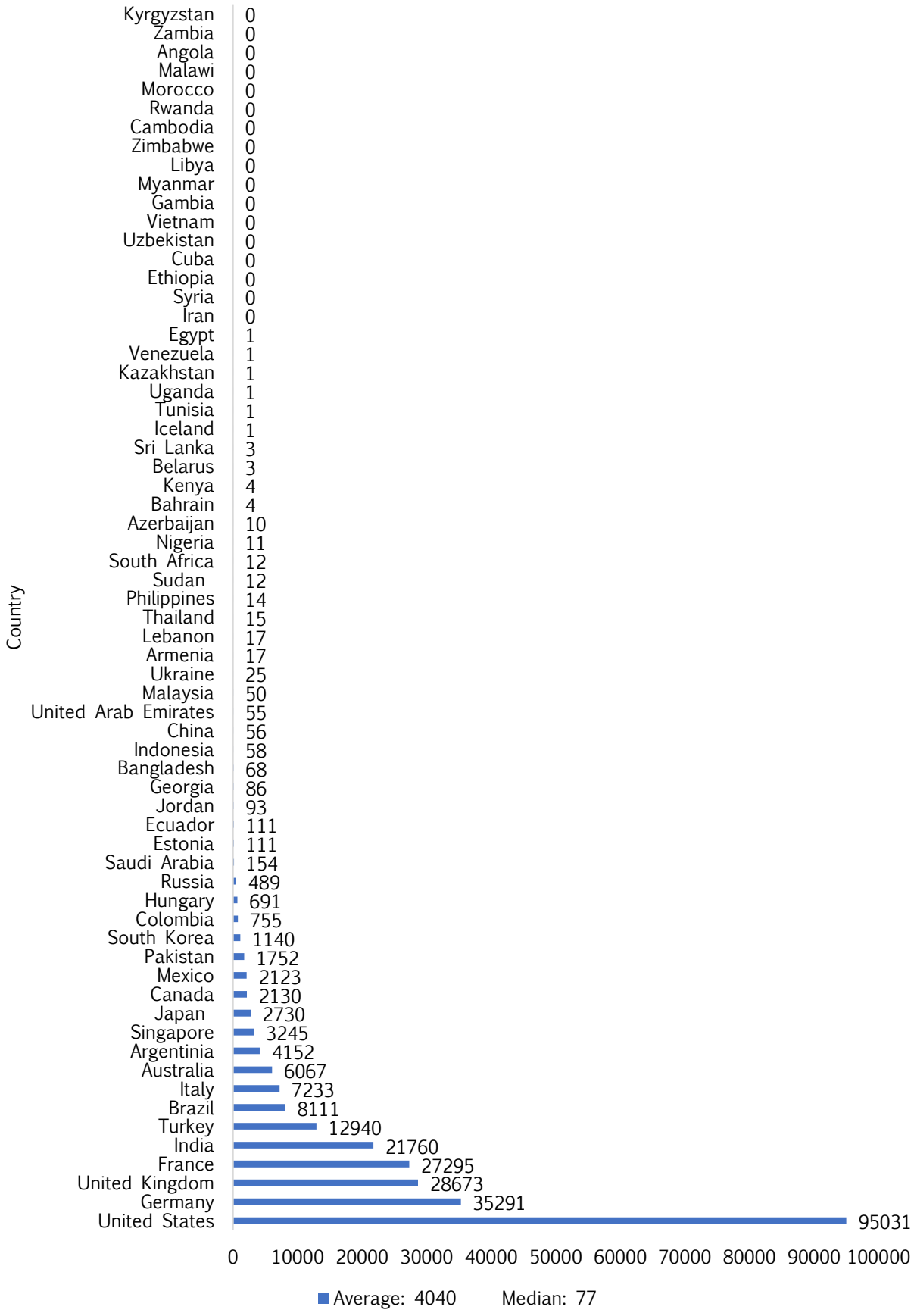


Figure 8: Total User Accounts Referenced

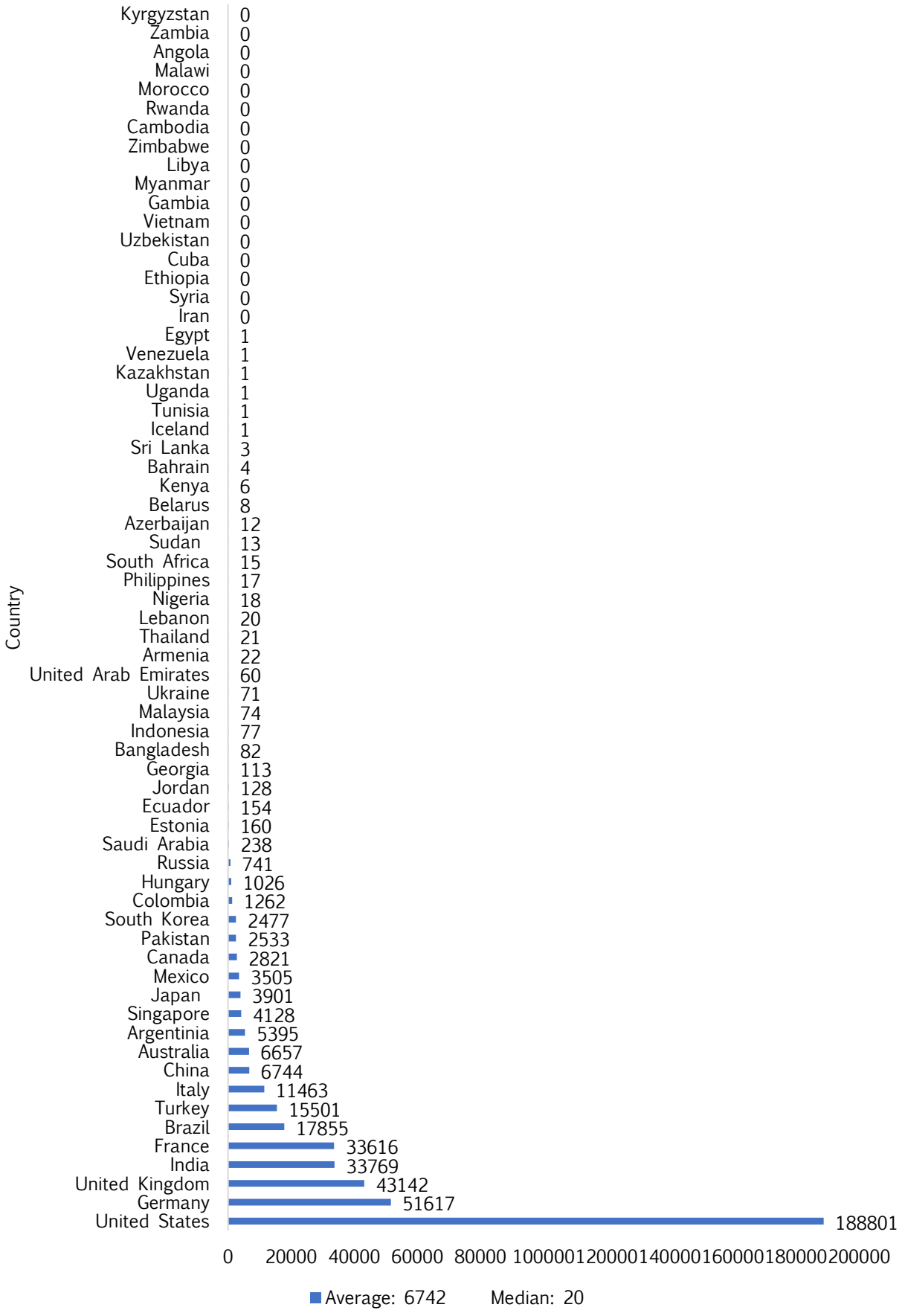


Figure 9: Total Percentage of Requests Where Some Data Produced

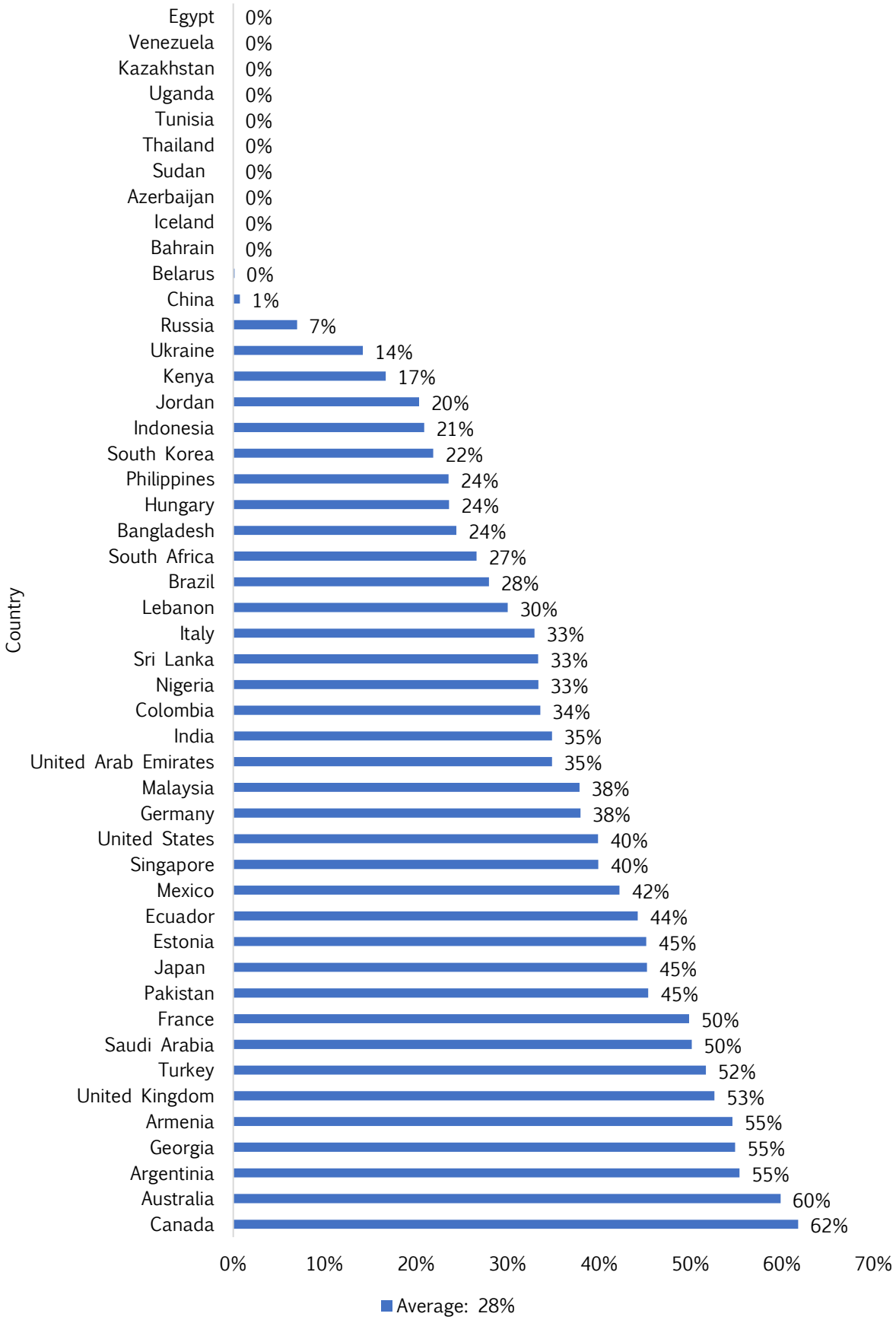


Figure 10: Country Data on Population, Online Population and Internet Penetration 2016

Country	General Population (1000 rounded)	Online population	% of Internet penetration
Angola	28.813.000	5.951.453	23%
Argentinia	43.847.000	30.359.855	69%
Armenia	2.925.000	1.510.906	50%
Australia	24.127.000	20.679.490	85%
Azerbaijan	9.762.000	6.027.647	61%
Bahrain	1.425.000	1.278.752	92%
Bangladesh	162.952.000	21.439.070	13%
Belarus	9.507.000	5.786.572	61%
Brazil	207.653.000	139.111.185	66%
Cambodia	15.762.000	1.756.824	11%
Canada	36.286.000	32.120.519	89%
China	1.378.665.000	721.434.547	52%
Colombia	48.653.000	27.664.747	57%
Cuba	11.476.000	3.696.765	32%
Ecuador	16.385.000	7.055.575	43%
Egypt	95.689.000	30.835.256	33%
Estonia	1.316.000	1.196.521	91%
Ethiopia	102.403.000	4.288.023	4%
France	66.896.000	55.860.330	86%
Gambia	2.039.000	346.471	17%
Georgia	3.719.000	2.104.906	53%
Germany	82.668.000	71.016.605	88%
Hungary	9.818.000	7.874.733	80%
Iceland	334.000	331.778	100%
India	1.324.171.000	462.124.989	35%
Indonesia	261.115.000	53.236.719	20%
Iran	80.277.000	39.149.103	49%
Italy	60.601.000	39.211.518	66%
Japan	126.995.000	115.111.595	91%
Jordan	9.456.000	3.536.871	46%
Kazakhstan	17.797.000	9.961.519	56%
Kenya	48.462.000	21.248.977	45%
Kyrgyzstan	6.083.000	2.076.200	34%
Lebanon	6.007.000	4.545.007	76%
Libya	6.293.000	1.335.705	21%
Malawi	18.092.000	1.160.839	7%
Malaysia	31.817.000	21.090.777	69%
Mexico	127.540.000	58.016.997	45%
Morocco	36.286.000	2.068.556	58%

Myanmar	52.885.000	1.353.649	3%
Nigeria	185.990.000	86.213.365	46%
Pakistan	193.203.000	34.342.400	18%
Philippines	103.320.000	44.478.808	44%
Russia	144.342.000	102.258.256	71%
Rwanda	11.918.000	1.478.216	12%
Saudi Arabia	32.276.000	20.813.695	65%
Singapore	5.607.000	4.699.204	83%
South Africa	55.909.000	28.580.290	52%
South Korea	51.246.000	43.274.132	86%
Sri Lanka	21.203.000	6.087.164	30%
Sudan	39.579.000	10.886.813	26%
Syria	18.430.000	5.502.250	30%
Thailand	66.864.000	29.078.158	43%
Tunisia	11.403.000	5.472.618	48%
Turkey	79.512.000	46.196.720	58%
Uganda	41.488.000	7.645.197	19%
Ukraine	45.005.000	19.678.089	44%
United Arab Emirates	9.270.000	8.515.420	92%
United Kingdom	65.637.000	60.273.385	93%
United States	323.128.000	286.942.362	89%
Uzbekistan	31.848.000	15.453.227	51%
Venezuela	31.568.000	18.254.349	58%
Vietnam	31.568.000	49.063.762	52%
Zambia	16.591.000	3.167.934	19%
Zimbabwe	16.150.000	3.356.223	21%
Average	-	-	51%

Figure 11: Combined Amount of Government Requests for User Data per 100.000 Internet users

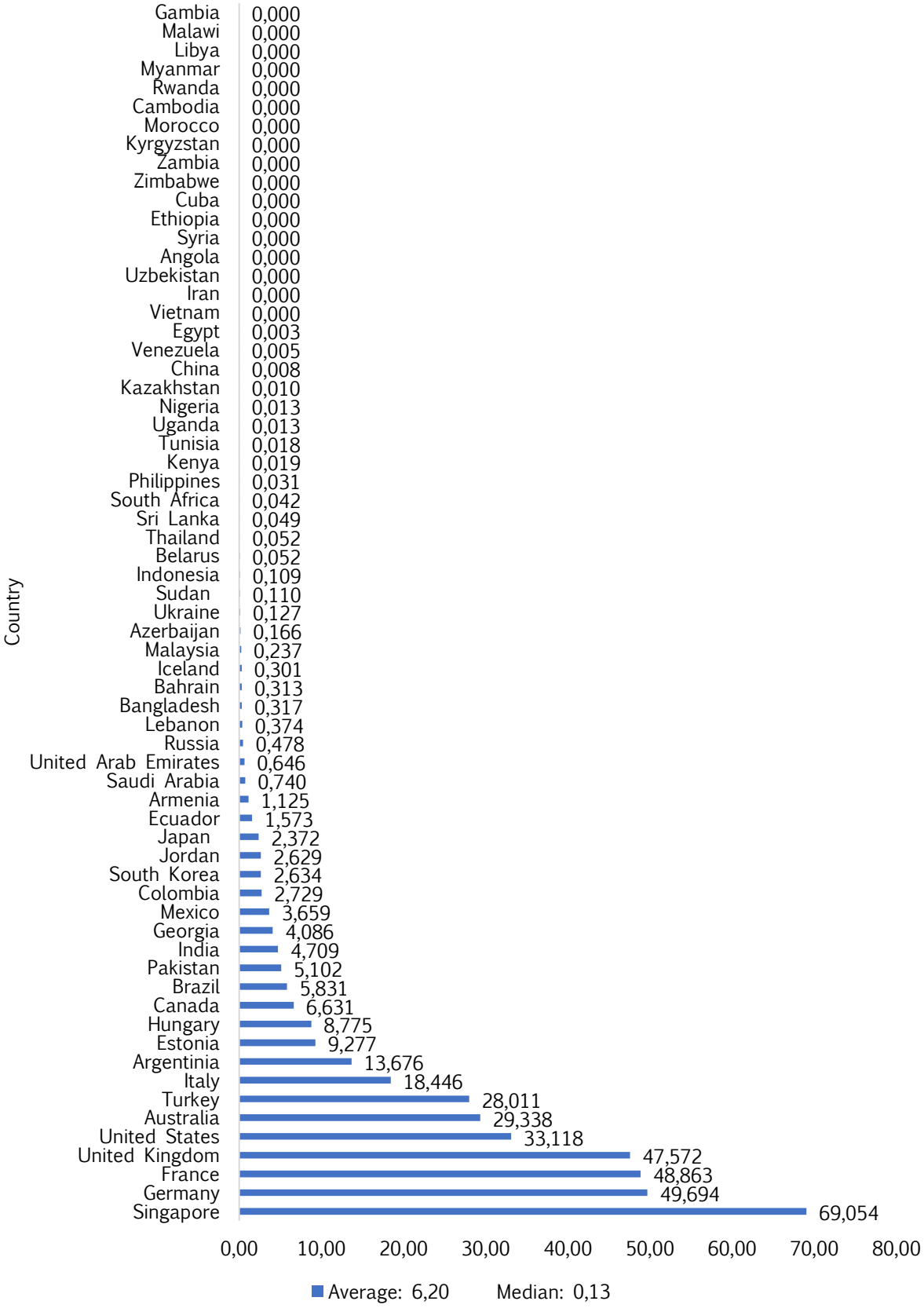


Figure 12: Combined amount of User accounts Referenced by Governments per 100.000 Internet Users

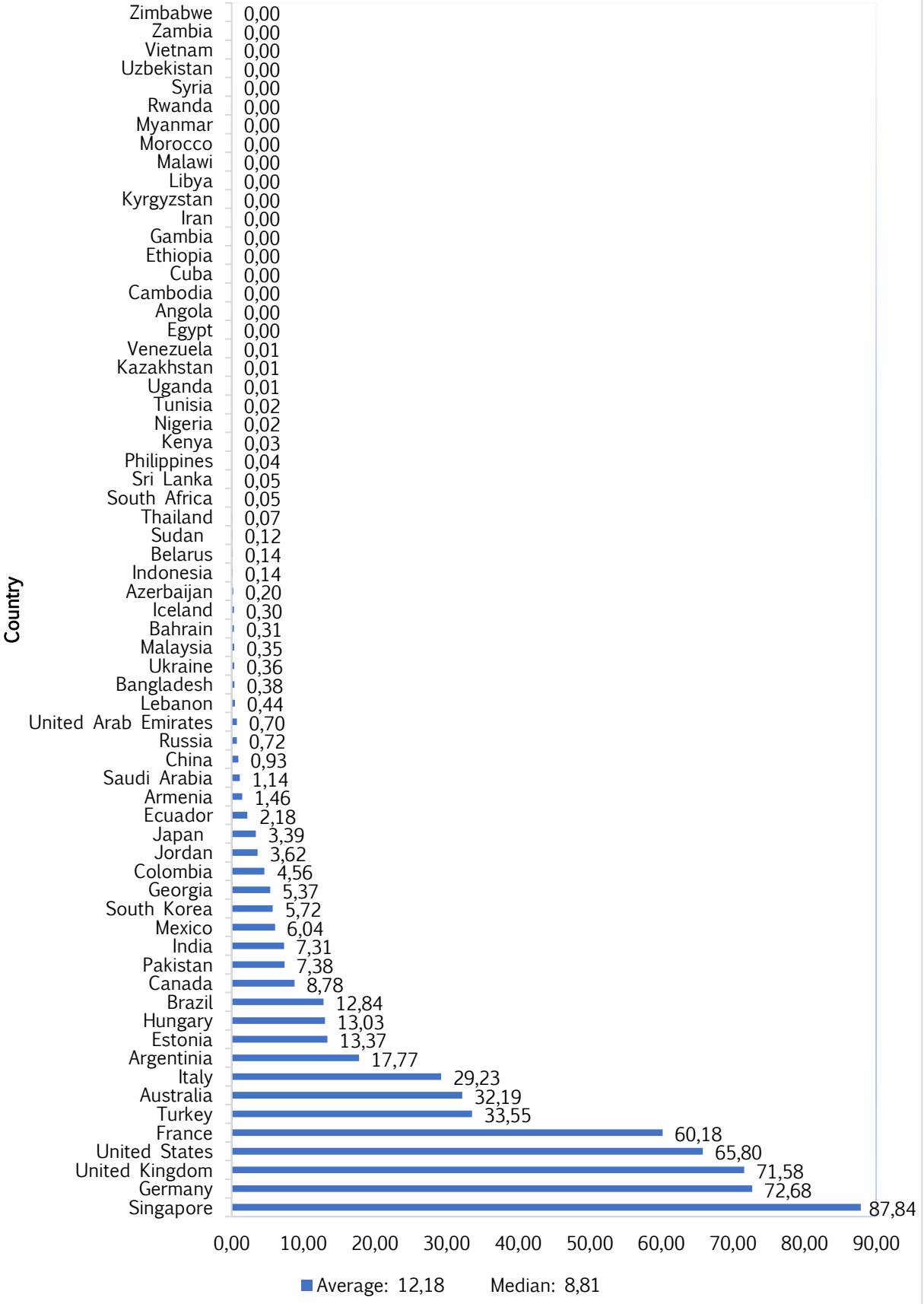


Fig 13: Countries by Accounts Referenced per 100.000 Internet Users in Combination with FOTN Report Data and Surveillance Ability Data

Rank	Country	Accounts Referenced per 100.000 Internet Users	Mass surveilance	Social media blocked
1	Singapore	87,8447		
2	Germany	72,6830	X	
3	United Kingdom	71,5772	X	
4	United States	65,7975	X	
5	France	60,1787		
6	Turkey	33,5543		X
7	Australia	32,1913	X	
8	Italy	29,2338		
9	Argentinia	17,7702		
10	Estonia	13,3721		
11	Hungary	13,0290		
12	Brazil	12,8351		X
-	*Average*	*8,81*	-	-
13	Canada	8,7825		
14	Pakistan	7,3757		X
15	India	7,3073	X	
16	Mexico	6,0413		
17	South Korea	5,7240		
18	Georgia	5,3684		X
19	Colombia	4,5618		
20	Jordan	3,6190		X
21	Japan	3,3889		
22	Ecuador	2,1827		
23	Armenia	1,4561		X
24	Saudi Arabia	1,1435	X	X
-		*1 Request per 100.000 Internet Users*		
25	China	0,9348	X	X
26	Russia	0,7246	X	
27	United Arab Emirates	0,7046	X	X
28	Lebanon	0,4400		
29	Bangladesh	0,3825	X	X
30	Ukraine	0,3608		
31	Malaysia	0,3509		X
32	Bahrain	0,3128	X	X
33	Iceland	0,3014		
34	Azerbaijan	0,1991		
35	Indonesia	0,1446		X
36	Belarus	0,1383	X	

37	Sudan	0,1194	X	
38	Thailand	0,0722		
39	South Africa	0,0525		
40	Sri Lanka	0,0493		
41	Philippines	0,0382		
-	*Median*	0,3	-	-
42	Kenya	0,0282		
43	Nigeria	0,0209		
44	Tunisia	0,0183		
45	Uganda	0,0131		X
46	Kazakhstan	0,0100		X
47	Venezuela	0,0055		
48	Egypt	0,0032		X
49	Iran	0		X
49	Syria	0	X	
49	Ethiopia	0	X	X
49	Uzbekistan	0	X	X
49	Cuba	0	X	X
49	Vietnam	0	X	X
49	Gambia	0		X
49	Myanmar	0		
49	Libya	0		
49	Zimbabwe	0		X
49	Cambodia	0		
49	Rwanda	0		
49	Morocco	0		X
49	Malawi	0		
49	Angola	0		
49	Zambia	0		
49	Kyrgyzstan	0		

Background legend:

Free (0-30)
Partly Free (31-60
Not Free (61-100)

Fig. 6

Fig 15: Country Data on Percentage-, Total- and Per Capita Data and on Government Requests

Rank	Country	Total % of Requests Where Some Data Produced	Total Requests for User Data	Requests per 100.000 Internet Users
1	Canada	62%	2130	6,631
2	Australia	60%	6067	29,338
3	Argentinia	55%	4152	13,676
4	Georgia	55%	86	4,086
5	Armenia	55%	17	1,125
6	United Kingdom	53%	28673	47,572
7	Turkey	52%	12940	28,011
		Majority line (50+%)		
8	Saudi Arabia	50%	154	0,740
9	France	50%	27295	48,863
10	Pakistan	45%	1752	5,102
11	Japan	45%	2730	2,372
12	Estonia	45%	111	9,277
13	Ecuador	44%	111	1,573
14	Mexico	42%	2123	3,659
15	Singapore	40%	3245	69,054
16	United States	40%	95031	33,118
17	Germany	38%	35291	49,694
18	Malaysia	38%	50	0,237
19	United Arab Emirates	35%	55	0,646
20	India	35%	21760	4,709
21	Colombia	34%	755	2,729
22	Nigeria	33%	11	0,013
23	Sri Lanka	33%	3	0,049
24	Italy	33%	7233	18,446
25	Lebanon	30%	17	0,374
26	Brazil *Average =*	28%	8111	5,831
27	South Africa	27%	12	0,042
28	Bangladesh	24%	68	0,317
29	Hungary	24%	691	8,775
30	Philippines	24%	14	0,031
31	South Korea	22%	1140	2,634
32	Indonesia	21%	58	0,109
33	Jordan	20%	93	2,629
34	Kenya	17%	4	0,019
35	Ukraine	14%	25	0,127
36	Russia	7%	489	0,478
37	China	1%	56	0,008
38	Belarus	0%	3	0,052

38	Bahrain	0%	4	0,313
38	Iceland	0%	1	0,301
38	Azerbaijan	0%	10	0,166
38	Sudan	0%	12	0,110
38	Thailand	0%	15	0,052
38	Tunisia	0%	1	0,018
38	Uganda	0%	1	0,013
38	Kazakhstan	0%	1	0,010
38	Venezuela	0%	1	0,005
38	Egypt	0%	1	0,003
	Morocco		0	0,000
	Angola		0	0,000
	Zimbabwe		0	0,000
	Vietnam		0	0,000
	Zambia		0	0,000
	Myanmar		0	0,000
	Iran		0	0,000
	Libya		0	0,000
	Syria		0	0,000
	Cambodia		0	0,000
	Cuba		0	0,000
	Gambia		0	0,000
	Kyrgyzstan		0	0,000
	Uzbekistan		0	0,000
	Ethiopia		0	0,000
	Rwanda		0	0,000
	Malawi		0	0,000
	Average	*28%*	*4040*	*6,2*
	Median	-	*77*	*0,13*

Legend:

Free (0-30)
Partly Free (31-60
Not Free (61-100)

Declaration of Authorship [in German]:

Ich versichere, dass ich die vorgelegte Bachelorarbeit eigenständig und ohne fremde Hilfe verfasst, keine anderen als die angegebenen Quellen verwendet und die den benutzten Quellen entnommenen Passagen als solche kenntlich gemacht habe. Diese Bachelorarbeit ist in dieser oder einer ähnlichen Form in keinem anderen Kurs vorgelegt worden.

Name, Vorname: _____

München, den _____

Unterschrift: _____