JeDEM 9(1): 79-96, 2017
ISSN 2075-9517
http://www.jedem.org

Open Government Leads to the Abolition of the Right to the Informational Privacy: An Invitation to Discussion

Tetiana Korshun

for.korshun@gmail.com

Abstract: The central thesis of the article is that informational privacy slows down the progress in many areas of science and social development. Current tendencies to open government lead us to construct an entirely transparent society, and we should be ready to organize our public and private life in the absence of the informational privacy, including the most sensitive areas. This transformation will influence almost every sphere of our social life. Increasing the level of tolerance, more security for private businesses, cost savings for states and individuals, the new wave in the development of the electronic services from governments and corporations, more incentives for law-changing process, the next level of social trust are all at the core of the transparent society after the abolition of the right to the informational privacy. However, many more consequences require further detailed study and research.

Keywords: open government, privacy, big data, democracy, information

1. Introduction

Governments have never been so open and transparent as they are nowadays. Moreover, every year societies all over the world receive tools to control their officials. Open data partnership provides an "international platform for domestic reformers committed to making their governments more open, accountable, and responsive to citizens" (https://www.opengovpartnership.org/).

Participation in this initiative, with the internal will to reform society, leads to rapid changes in the relationship between people and the state. The G20 Anti-Corruption Open Data Principles Assessment (2015) defines open data as: "Open data is the digital data that is made available with the technical and legal characteristics, which are necessary for it to be freely used, reused, and redistributed by anyone, anytime, anywhere" (p.2).

Under the concept of open data, governments are required to publish as much information as possible, and this data can be freely used by any person, including commercial use. The first step for almost every nation is to enforce its government to publish information. However, over time it

turns out that it is not enough to merely open the information. To increase the efficiency of the open data, it is necessary to do much more. In its report, the international organization *Transparency International* summarizes the main problems of open data practices in 5 countries in the context of their fight with corruption. Firstly,

> *"No country released all anti-corruption datasets"*,

for example, the beneficial ownership register. The second point is that much data need to be updated, but it is not. Thirdly, in many countries access is a problem in the absence of the single platform. The fourth point is that data is not always published using open file formats which are machine-readable. Another aspect of this problem is that

> *"lack of standards makes merging and comparing datasets difficult, particularly between countries"*.

The last point is a lack of open data skills (Connecting the dots, 23 February 2017). The tendency of opening more and more data, including personal information about public officials, demands a careful reflection of its consequences. We need to analyse the effects of open data on the social changes.

I use the case study of Ukraine for several reasons. Open government partnership has progressed rapidly over the last two years. The Ukrainian Parliament has adopted new legislation with a strong requirement to make available governmental information free for access. As a result, since March 2017, a governmental portal for open data, which contains more than 12000 datasets, was created. Some data should be digitalized before publishing. In the Global Open Data Index (2017), Ukraine in 2016 was ranked 24th, in 2015 it was 54, and in 2014 it was not ranked at all. The huge amount of information has been opened for a relatively brief period, so the Ukrainian society is still trying to analyse the new possibilities. Another vector of the open data development in Ukraine is the emergence of voluntary projects that are searching for maximization of the availability, usability, accessibility of open data. For example, the IGov project (https://igov.org.ua/) tries to pursue the development of e-services (with some restrictions because of the non-governmental status of this initiative). The ProZorro (https://prozorro.gov.ua/) project won the main award by Open government partnership in 2016 (for shining a spotlight on government procurement and saving taxpayers` millions), and C4F Davos Awards 2017 (in nomination "Trust of the Future"). This project was started as a voluntary initiative but soon became a governmental structure due to solid evidence for public cost-savings. Several hackathons, incubators, challenges, and conferences are held in Ukraine to support innovative applications for visualization of open data. A lot of interesting open data appeared recently. E-vox (http://ukr.e-vox.org/) is a voting system for local councils integrated with e-petitions. Search-analytical platform 007 (http://www.007.org.ua/) provides journalists and the public the opportunity to actively engage the public funds in monitoring through accessible and understandable service, analyse spending of budget funds at all levels, in territorial aspect, in the context of costs and control of public procurement through the integration of tender procurement system Prozorro of transactions that occurred in the State treasury service of Ukraine. Social Inspector (http://civilinspect.com.ua/) is a resource where you can investigate how the local budgets are spent, not only in general but in every school, kindergarten or another municipal

institution. These rapid changes in Ukraine allow comparing the reality with and without open data. Another reason to use the case study of Ukraine is that a strong public discussion on these issues engenders very different thoughts and opinions from all groups of society: scientists, politicians, local and central officials, NGOs, students, working and retired people.

According to the UK Digital Strategy (UK Digital Strategy, 1 March 2017),

> *"data is fundamental to what we do and vast quantities of data are collected, analysed and used every day. Advances in digital technology, cloud-based computing, and data science open up huge opportunities to improve the effectiveness and precision of government policy interventions by using data more effectively. Furthermore, improving the way we collect, manage and share government data has the potential to deliver significant efficiency gains right across the economy".*

The main thesis is that

> *"the true potential of data can only be harnessed if it is open for use by others",*

but

> *"there is a strong tension between open data policy and the privacy of their citizens. A lack of open data standards between (levels of) government organizations has been identified as a barrier for open data usage by citizens and businesses and subsequently to new open data policy". (N. Huijboom, & T.Van den Broek, 2011, p.8)*

N. Huijboom, & T.Van den Broek researched the main drivers and barriers to open government in different countries. They concluded that the main drivers (e.g., citizen pressure, market initiatives, emerging technologies and the ideas of thought leaders) exist in the society, and the main barriers (e.g., the closed culture, limited quality of data, lack of standardisation and existing charging models) exist within government (N. Huijboom, & T.Van den Broek, 2011, p.9). It is interesting to admit that society strives itself to more levels of openness. This leads to the rapid expansion of the circle of people, information about who is of public interest and should be published. For example, in Ukraine, more than 700,000 officials (almost 6% of Ukrainians, including newborns) submit their e-declarations on a single platform (https://public.nazk.gov.ua), and their financial information is available for everyone. This example illustrates the main trend of the growth of the amount and the diversity of the open data.

The purpose of this paper is to set up the thesis that our society will inevitably be fully transparent in future. As I will argue, the informational privacy legislation slows down the development of society and should be abolished. In my view, the open government initiatives are the first step to the transformation of the society as a whole. All the variety of information, including personal, governmental and business should be opened and freely available for everyone. However, the availability of commercial information as well as state secret information is not analysed in this article. The main idea is that in the collision between open society and informational privacy, the priority should be and will be for openness, not to privacy.

The paper is organized as follows. In section 2, I examine the current progress in the opening data processes and the advantages of open data. Section 3 is devoted to the problems of the protection of personal information according to the progress of the big data science. In section 4, I

outline the contours of a fully open society. Then I conclude with a summary of the main points of the paper and list some of the problems associated with the abolition of the right to informational privacy

2. The Advantages of Open Data

The essence of government work is to facilitate information.

> *"Collection and dissemination of information and data are the key tools of government. Governments gather large amounts of data and hold significant national datasets. For being meaningful data must be represented or contextualized in some way – converted into information. In an increasingly digital society where data can be transferred and analyzed using freely accessible platforms and tools, the monopoly government historically had on processing and interpreting data is undermined" (Davies, T., 2010).*

Open government can fuel innovations in society and in government itself. A lot of researchers have explored the advantages of open data and their impact on the development of society (e.g., Davies T., 2010; Landau, S., 2016; Molloy, J. C., 2011.). To illustrate the key points I use the examples from Ukrainian experience because in last two years many cities have approved the idea of "open by default" data.

As it states in the G20 Anti-Corruption Open Data Principles Assessment (2015):

> *"Open data empowers citizens and enables them to hold government institutions into account. Open data can also help them understand, influence and participate directly in the decision-making processes and in the development of public policies in support of public sector integrity. This is paramount to build trust and strengthen collaboration between governments and all sectors of society" (p.6).*

The main advantages of the open government can be grouped into several points. Open data provides new opportunities for building smart cities and smart nations. This offers citizens greater convenience, especially at the local level. For example, MARTA *On the Go* app (http://www.itsmarta.com/marta-on-the-go.aspx) helps passengers to find the bus schedule, train schedule, and bus real-time information throughout Atlanta's Metropolitan Area. The same idea is realized in Ukrainian EasyWay product (https://www.eway.in.ua/). Another example is the CoAXs (http://coaxs.mit.edu/job-map/), where job data for Boston, Massachusetts and Los Angeles, California is reported at block/workplace zone level, then distributed randomly into building footprints within each zone. Locations from administrative records (e.g., the address of a company's headquarters) may not align with actual commuting destinations. Open data allows people to make the optimal choice by providing them with more complete and accurate information at the right time. One of the most fascinating examples is the 3D map visualizing crime trends in New York City (http://coolmaps.esri.com/#14). Visualization makes it clear where most incidents occur, and which areas of the city are the safest. Data is taken from the NYC Open Data portal.

Open data helps to increase the levels of participation in public affairs. Portal «Open City» (http://opencity.in.ua) was created for an interaction of citizens, local authorities, associations, charities, and businesses in the process of problem-solving. More than 10,000 local problems such as pits on roads, homeless dogs, lack of street lighting, emergency buildings have been addressed in 46 cities in Ukraine since the project started. The ChattaData (https://performance.chattanooga.gov/) is focused on the priorities of the residents: safer streets, stronger neighbourhoods, growing economy, smarter students and stronger families and a high-performing government. ChattaData is the performance management tool that tracks, monitors, and makes public the efforts of Chattanooga officials, holding them accountable and helping them achieve their goals. One of the most popular tools in every country is an e-petition service. For 18 months (September 2015 – March 2017) almost 30,000 e-petitions were filed to the President of Ukraine (https://petition.president.gov.ua), and almost 90,000 persons had signed at least one of them. The participatory budgeting in Dnipro, Ukraine (https://adm.dniprorada.gov.ua/) was held in 2017 for the first time. 233 authors proposed 295 projects in different areas. The participatory budget of Kyiv (https://gb.kievcity.gov.ua/) allows 62 projects to be realized in 2017. During the casting, more than 50,000 people gave more than 112,000 votes. In January 2017, the website was visited by 278,000 users. The absolute numbers are not very significant, but we need to consider that for all the participants the task to write an open budget project is much more complicated and demands considerable time and effort from authors. The main point of this statistics is that the simplicity of access to different government information and various public services radically expands the number of their users.

Open data provides much more transparency and public control. Electricity Map (http://www.electricitymap.org/) is a very interesting project, which has a substantial environmental and economic impact. The source of electricity in different European countries and how much CO2 was emitted to produce it is shown in real-time. Also, a visualization of electricity imports and exports exists between countries. The project is open source and runs on open data portal European electricity operators ENTSOE. A website in Ukraine visualizes information from financial declarations of the officials (https://declarations.com.ua). More than 3000 volunteers help to digitalize paper versions of the document as far as e-declarations became obligatory in Ukraine only in 2016. Ukraine is one of the several countries in the world which has a registry of beneficial ownership (information can be found in the dataset https://usr.minjust.gov.ua/). The Ukrainian society and the rest of world were shocked by the wealth of Ukrainian politicians (Sandford Alasdair, 2016; Burridge Tom, 2016). However, despite strong public opinion, only 52 cases have been sent to the court by National Anti-Corruption Bureau of Ukraine (https://nabu.gov.ua/). Moreover, no one official resigned due to public pressure. So, transparency itself is not able to provide the society the necessary effect; we need to have another public instruments and tools to serve politicians to carry a legal or political sentence. The next step is the attempt to build public trust through transparency.

The economy of public costs is one of the leading advantages of the open data. ProZorro helped Ukraine to save more than 500 million US dollars in 2 years. To achieve this result, it was only necessary to publicize information about the future purchases by public authorities. However, the cost-saving is not the only point of open data. UK Digital Strategy (2017) considers that

"data analytics is a fast moving area, and we are committed to keeping the UK at the leading edge of new developments, whilst putting in place the necessary protections to ensure data is kept safe and used appropriately".

As CEBR & SAS (2016) states

"analysis predicts that data will benefit the UK economy by up to £241 billion between 2015 and 2020".

In EU it is forecasted that

"between 2016 and 2020, the market size of Open Data is expected to increase by 36.9%, to a value of 75.7 bn EUR in 2020. The forecasted number of direct Open Data jobs in 2016 is 75,000 jobs. From 2016 to 2020, almost 25,000 extra direct Open Data jobs are created. The forecasted public sector cost savings for the EU in 2020 are 1.7 bn EUR" (Creating Value through Open Data Study on the Impact of Re-use of Public Data Resources 2015).

Open data gives an opportunity to the officials to become more efficient due to more feedback on particular problems. One of the examples is the map of Dnipro city where everyone can add diverse types of objects (http://mapa.dniprorada.gov.ua/?category_id=7). One of the future projects (Znaideno) proposes an online monitoring of illegal deforestation, which is one of the most significant environmental problems in the western part of Ukraine. All these applications give Ukrainian officials better tools to notice a problem and fix it.

In February 2017, the World Government Summit was held in Dubai, and the report Embracing Innovation in Government – Global Trends was published. The critical point is that

"governments are exploring innovative approaches to understanding, predicting and addressing disruptions and complex issues affecting their territory, critical systems, and society. However, the increased use of new tools also brings challenges of its own".

The challenges are quality in information, availability of information, accountability for data-driven decision making, and control over personal data.

However, the main problem with open data is the greatly exaggerated public expectations regarding free access to information. Moreover, these expectations are almost never realized.

"Meanwhile, governments around the world have been publishing large swathes of data in an effort to promote transparency and openness. However, these developments have left the mechanics of our democracy, the basic institutions, processes and structures of governance as well as the relationship between citizens and the state, largely unaffected. Across much of the western world, we still have a system whereby a small political class has a monopoly over the substance and direction of policy with decision-making centralised in national and regional parliaments with little input from citizens" (Simon J., Bass Th., Boelman V. & Mulgan G., 2017, p. 9).

The government has never been open, always remaining accessible exclusively to the elite.

A completely open society is one in which the minimum amount of information is in a closed mode. Citizens do not hide information from the government (including information about taxes,

or do not try to avoid military service); the government does not hide information from citizens (including the real reasons for decision-making), and people do not hide information from each other (with rare exceptions). Based on this consideration, open data alone does not affect the overall state of openness in the country. So, in Ukraine, in fact, corruption has not decreased with the openness of government data in most cases. Rather, it redistributes corruption in that it flows from one sphere to another, and forces officials to change corruption techniques and tools. Partly this is due to the limited data which is already published. Partly this is because of the vast amount of open data, and the inability of society to analyse all the information in a brief time. Moreover, the main reason is the prominent level of tolerance to corruption in a society where almost everyone in one way or another takes part in fraudulent transactions. This ambiguity is noted by H. Yu and D. G. Robinson in their study (2012):

> *"Open government and open data can each exist without the other: a government can be an open government, in the sense of being transparent, even if it does not embrace new technology (the key question is whether stakeholders know what they need to know to keep the system honest). Moreover, a government can provide open data on politically neutral topics even as it remains deeply opaque and unaccountable" (p.181).*

Technology enables the situation to change. Open data can lead to a discussion about the development of understanding the state in principle, a new presentation of the goals and objectives of the government. Tim O'Reilly proposes the idea of government as a platform:

> *"There is a new compact on the horizon: information produced by and on behalf of citizens is the lifeblood of the economy and the nation; the government has a responsibility to treat that information as a national asset. Citizens are connected like never before and have the skill sets and passion for solving problems affecting them locally as well as nationally. Government information and services can be provided to citizens where and when they need them" (O'Reilly, T., 2011, p.14).*

So, the principles of transparency, participation, and collaboration change their meaning due to the development of technology. Despite profound changes in the open data partnership, society demands more efficiency, more transparency, more trust, more accountability, more participation, and more cost-savings. Moreover, the civil society needs more information and more tools to change the core of the citizen-government partnership.

3. The Problems with the Informational Privacy

Both governments and private companies have numerous tools and innovations from a young but rapidly developing big data science to predict the behavior of large masses and every person individually. As Susan Landau (2016) points out,

> *"governments aren't the only organizations collecting massive amounts of data on private individuals. Indeed, it might well be the case that the government's data collection on individuals is dwarfed by the private sector's" (p.3).*

A tremendous shift in informational privacy arose with the integration of the Internet in all areas of life. As A. Crabtree & R. Mortier (2016) put it, "privacy is currently a topic of widespread

societal interest and debate as digital technologies generate and trade in personal data on an unprecedented scale".

Samuel C. Rickless proposes an answer to the modern changes in the informational privacy. He formulates the Barrier Theory to explain the essence of the right to privacy.

> *"The right to privacy is a claim, a claim that concerns not control over access to (or information about) oneself, not accessibility, not the acquisition or dissemination of undocumented personal information, but rather the experiencing or discovery of personal facts about the right-holder via the breaching of barriers used to keep others from experiencing or discovering these sorts of facts. This is the core of the Barrier Theory I have defended as an alternative to the standard accounts" (Samuel C. Rickless, 2007).*

However, even this theory cannot give us the entire perspective of the right of informational privacy in the modern world. The global economy is ineffective with national politics and vice versa. More and more difficulties emerge with the international issues of informational privacy. In principle, it is difficult to control international corporations and even more so the sphere of information. When a company is registered in one country, the servers are situated in another, hosting in the third, the citizen of the fourth country lives on the territory of the fifth, and the beneficiary of information in the sixth country. At the same time, each state has certain requirements for the collection, storage, dissemination, and usage of the same information. All the laws, moreover, can change very often. Thus, the corporation simply cannot initially comply with all legislative requirements. Moreover, it is cheaper to pay a fine or compensation than trying to implement all the laws in their company standards. As M. Xue and others put it, "online privacy laws can potentially have the unintended consequence of reducing individuals' privacy rather than protecting it" (Xue, M., Magno, G., Cunha, E., Almeida, V., & Ross, K. W. 2016, p. 401).

The authors of the article state that even after the execution of court decisions on the removal of personal information from the Internet, this information can be easily found in the vast majority of cases. So, the "right to be forgotten" (e.g., article 17 in EU General Data Protection Regulation, 2016) is controversial because it is very hard to formulate the common rule (when and why we should delete the information), because of the contradiction with freedom of speech, and an actual impossibility of its realization.

Today we can observe the rapid expansion of the circle of people of public interest. Moreover, then it becomes more and more difficult to draw a line, to clearly explain why some people should disclose all information about themselves and why others should not and formulate the common rule. In spring 2017, very controversial laws were issued in Ukraine. These laws compel members of Ukraine's anti-corruption NGOs to release electronic versions of their financial declarations. As Devin Ackles states in his review of this Ukrainian law (2017),

> *"Perhaps the most damaging aspect of law is that it requires any contractors or service providers who work with civil society entities involved in anti-corruption, or receive technical assistance (foreign aid) towards that end, to also file declarations for the public to view. Essentially, this would mean that anyone who engages in any form of business or provides any services — whether it be providing printing services or translations of documents — would also fall under the auspices of this*

legal requirement. This would clearly disincentivise any public organization, private business or individual from wanting to formally work with an NGO whose work may lead to them making public their private individual information".

However, this case shows us a tendency in the open government evolution. We cannot realize in every situation if it is the public or private interest, which we should firstly protect through the law. We all have the public interest in controlling not only officials but all their relatives, friends, counterparts, and even acquaintances because all of them can be accomplices of corruption. In Ukraine, it is widespread practice to make your property or income over to relatives or friends to avoid declaring by signing fictitious contracts. Moreover, open data can help to check the facts and prevent corruption itself. Why should not all workers of state or municipal enterprises publish their financial declarations? In Ukraine, medicine and education are free and guaranteed to all citizens by the Constitution. In fact, education and medicine are traditionally two of the most corrupt industries. Moreover, no one person suggests that educational or medicinal services are free. However, every school or hospital has their specific price, and this practice is legalized as charity. So, there are two independent sources of financing state and municipal institutions and the absence of any transparency at all. People should pay twice, and they have no instruments to control the efficiency of the use of funds. The same goes for employees of state monopolies (the railroad, for example). Moreover, why should society not have access to declarations of all people or companies who somehow receive money from the state budget (including suppliers of various goods and services for the government)? After all, this information is directly related to public interest and should be the subject of public investigation. Moreover, if so, then, including their family members, e-declaration will affect most of the adult population of the country. The next step to the transparency of society is e-declaration for every person in the community. Such a decision is natural and fits into the existing trend. If absolute e-declaration occurs, then the society will have more tools to track illegal financial flows. Such measures significantly contribute to the transparency of the society and the control of officials, reduce corruption risks, and in the case of private corporations reduce the risk of tax fraud.

Society will become fully open in the very near future. Even nowadays the minimal knowledge and skills are required to identify the person and collect an amount of information about his/her professional, family and personal life. We give personal information about ourselves not only in social networks but also in exchange for discount cards, when registering on thousands of sites, at work, with counterparts. Moreover, just one leak (due to the custodian's fault or the result of hacking) is enough to make this info public. Moreover, if something once appears in the public domain, it will remain there permanently.

"Shifting the locus of agency and control to enable users to effectively manage privacy in the emerging digital ecosystem is a grand challenge for contemporary computing in the round and HCI in particular insofar as 'the user' is its core business" (Crabtree, A., & Mortier, R., 2016).

In many countries, there is a requirement to give consent for collecting, storing and using your personal data. However, there are some problems with such consent. The increase in the pace of life and the number of communications leads to the situation when the person makes decisions about the need to transfer personal data to someone several times a day. Each mobile application

requests access to the data; each purchase demands to share some personal information. It is difficult to read each agreement, delving into the conditions for collecting, storing, transmitting information. In addition, if the company uses analytics based on big data, it becomes impossible even to predict what specific data they will be able to obtain about a person and how this personal information will be used. In some cases, it is impossible to renounce the proposed conditions for the provision of information, because users conclude an agreement of accession and have no other suitable alternatives. Thus, the requirement of consent to the processing of personal data significantly increases the cost of the workflow, while the benefits from it are minimal.

A lot of information about people from their birth, including baby photos, is available to different companies. The development of big data science allows predicting many things essential to people's lives such as propensity to crime, mental disorders, and the choice of profession. This will increase the possibilities of social engineering, career guidance, correction of socially harmful behaviour, reduction of unemployment. However, the problem is that today's children do not consent to the publication of this information on the network. Their right to privacy is trying to defend them at the legislative level (Children's online privacy protection act, 1998 in the USA or General Data Protection Regulation, 2016 in EU), but it rarely leads to a marked positive effect (Dey, R., Ding, Y., & Ross, K. W., 2013). However, not only the privacy of children is threatened. There is an inability to protect the privacy of third parties. Every day the billions of photos and videos are published. Many of them also show bystanders. With today's facial recognition technology, it is easy to identify them in almost all cases. Thus, even if the person is very careful, does not spread information about his/her movements, does not publish photos, uses anonymizers and secure connections, AI has more than enough information about his/her life to make rational assumptions about his/her tastes, preferences and strategies of behaviour in different life circumstances. Moreover, any legal restrictions, in this case, are meaningless.

Mobile phone companies, GPS, Wi-fi spots, Web browsers, applications collect a large amount of information on the personal life. Everything is connected to everything. The choice of music, profession and the likes of images "give out" our political views, religious preferences, and most personal habits. As Kosinski, M., Stillwell, D., & Graepel, T. (2013) have shown,

> *"a wide variety of people's personal attributes, ranging from sexual orientation to intelligence, can be automatically and accurately inferred using their Facebook Likes. Similarity between Facebook Likes and other widespread kinds of digital records, such as browsing histories, search queries, or purchase histories suggests that the potential to reveal users' attributes is unlikely to be limited to Likes. Moreover, the wide variety of attributes predicted in this study indicates that, given appropriate training data, it may be possible to reveal other attributes as well" (p.5802)*

They write that is it possible to predict

> *"a range of highly sensitive personal attributes including: sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender" (p.5802).*

Based on the list of purchases, supermarkets can anticipate changes in the marital status (marriage, childbirth, divorce) even before we realize it ourselves. Telephone companies know not

only our real social network, but also the ways of movement, places of residence, and work, based on which they can draw conclusions about sensitive information. Banks collect information not only about financial operations but also about our personal life, communications, and relationships. The Internet giants track our every move not only directly on their websites, but also far beyond their borders. The information arrays that are collected by corporations such as Google or Facebook and the algorithms for processing this information indicate the amazing usefulness of such information both for improving their products and for commercial use. As it is noticed in the Big Data and Privacy: A Technological Perspective Report (2014),

> *"Big data drives big benefits, from innovative businesses to new ways to treat diseases. The challenges to privacy arise because technologies collect so much data (e.g., from sensors in everything from phones to parking lots) and analyze them so efficiently (e.g., through data mining and other kinds of analytics) that it is possible to learn far more than most people had anticipated or can anticipate given continuing progress. These challenges are compounded by limitations on traditional technologies used to protect privacy (such as de-identification). PCAST concludes that technology alone cannot protect privacy, and policy intended to protect privacy needs to reflect what is (and is not) technologically feasible".*

Another controversial problem is what to do with the informational privacy and the artificial intelligence (AI). More power shifts from humans to algorithms. In an increasing number of situations, the algorithms will make decisions that affect our lives. Medical, legal advice, recommendations for training can be already made by the machines. All this advice and these recommendations and decisions are based on the study of our behaviour. For example, in the US, some criminal court judges now use algorithms to guide decisions on bail (Dewan Sh, 2015). This is a relatively new challenge for our society. If the data is used by the machine to make a decision, and this data is not available to any other person, is this a violation of privacy? One aspect is legislation questions; the other is how people perceive it. We need some guarantees and accountability for data-driven decision-making.

Susan Landau (2016) asks "Should we?" use the Big Data information even if it relates to highly sensitive personal information. Moreover, these questions include

> *"is this an application of the data for which a significant percentage of users might hesitate to participate if asked? Is this use of data substantively different in nature from "normal" usage? Might the user feel manipulated or intruded on as a result of this use of the data? If we are using people's private data to inform our results, we have a moral and ethical responsibility to ask such questions. Anything less fails our users" (p.5).*

My answer is "yes, we should". Not only because it can bring tremendous benefits, but because it is already impossible to deny the use of personal information for business or social engineering purposes. Moreover, if the law cannot be observed, its preservation harms the entire legislative system and the state in whole.

4. The Contours of the Fully Transparent Society

Modern society is not ready to remove all barriers to private information; therefore, as the first step, we propose to divide all information into three groups and apply a different mode of access to each of the group. The first group consists of public information such as state or local budgets, statistics and non-personal data. Every person should have free access to such information without any other requirements. The government and corporations should be obliged to share such information in the Internet using formats which are suitable for the machine analysing. The second group contains information about a person, which is in some public interest and may be used for improving different types of services. Anyone can get this information, but only after the reliable identification of the person. Moreover, the addressee can see who have searched data about him/her. The third group is about the most sensitive personal information, which can be provided for everybody, but only for a fee. Moreover, a person is notified that this information about him/her was required by the particular person. If such information is used for the illegal purposes, the person can resort to the court for claiming compensation.

However, I state that all these measures are temporary. We should understand that there is no informational privacy in the modern world. For some people as for some societies, it will be hard to accept this situation, but for collectivist societies, the lack of privacy is a more common thing. The right to information privacy is a creation of the modern era, but in our information age, in the period of development of AI, this right becomes a relic of the past and must be completely abolished. Privacy is a relatively recent invention. Previously, in small communities, everyone knew almost everything about everybody. Moreover, such knowledge and the trust which is based on such knowledge is the basis of modern representative democracy. Law in principle is a substitute for personal trust (which is based on a person's knowledge and ability to predict someone's behaviour). The law makes the behaviour of any unknown person more predictable for us. Opening personal data can make trust less institutional and more personal (depending on the behaviour of a particular person, rather than the law enforcement system as a whole). However, the difference between the past and the future underlies in recording the information forever. Human memory is imperfect; in the era of the Internet, everything is documented. In the modern world, people are gradually getting used to more and more openness. Every mistake, every trivial offence remains in the "public memory" forever, and it can become a significant problem, especially if you have achieved success in life. The consequences can be very different, and this requires additional research from the standpoint of philosophy, sociology, political science, psychology and other social disciplines. On the one hand, such a fixation of all our actions and utterances will lead to the fact that people who are cautious and not prone to risk and impulsive actions will have the advantage. On the other hand, a much more different behaviour will become a social norm and will cease to be condemned. This becomes even more important given that other trends of social development (further automation, robotization, cheaper, labour and resources) will encourage humanity to develop creativity, the ability to take risks and not be afraid to make mistakes to find unexpected solutions. At the same time, the future society, in which personal reputation and social trust (Korczynski, M., 2000) come first, leads to an increase in the psychological pressure of society on the individual. That, in addition to the other factors, can cause

an increase in psychological problems. The specific term "cyberbullying" has appeared to describe this social problem (see for ex. Kiriakidis, S. P., & Kavoura, A., 2010).

The main reasons to limit access to private information are as follows. Personal reasons are related to all the variety of private communications and the difficulties of personal relationships. In the fully open society, people need to build up personal connections with more accuracy and respect to avoid undesirable consequences. Moreover, even after the breaking of relationships, people must learn to explain their reluctance to communicate. The next group of reasons connected with the interference of your private and public life (this is especially important for job-seekers). However, there is an actual tendency to analyse the profiles in social networks and other open sources to find the most prominent worker. So, today this is already a reality for the job-seekers, and for the HR-specialists, and no any separation between your public and private life as far as information about these aspects of life is available. In some cases, it is hard to distinguish if there is some type of discrimination (especially if the information about health, children, and relatives in need of care is considered in the issue of hiring). However, this is the same challenge as it is with another type of discrimination when people cannot hide their peculiarities (their origin, colour of skin, gender). The only way to fight discrimination is to support tolerance and develop a more inclusive society. Partly, the full openness will help to build a more suitable society for all people, because we will see how many our co-workers already have those life circumstances, which we used to think are unuseful to their working capacity. The third group of reasons to hide some information is the person-government relations. Of course, the transparent society increases the detection of crimes. However, we can see this tendency all over the world even now. Governments have considerable information about people and have abundant power to get the information from private corporations to investigate crimes. Perhaps, it will lead to a softening of punishments by increasing the inevitability of these punishments. There are several significant barriers to the abuse of private information. First, it is a tremendous amount of information and the general disinterest of people in each other (with rare exceptions). Secondly, it is a new level of tolerance, which will invariably develop under conditions of full openness of society. Thirdly, no one can deny the importance of legislation and judicial resolution of disputes related to the misuse of information.

The abolition of personal privacy will provide more security, which is associated with the ability to control any process. Security in private business often means more knowledge about your current and possible contractors. For a fee, the YouControl project (https://youcontrol.com.ua) provides notifications to companies when significant changes occur in their business partners. For example, the messages will be sent in the case of court hearings, reorganization, changes of CEO. YouControl takes information exclusively from open sources and open datasets which are available in Ukraine.

Another direction of the evolution of the government is the development of electronic services. Open data and the abolition of anonymity by default will radically expand the participation of various groups in the management of society. This can change all the practices and approaches of public administration in principle. Open information will make it much easier, faster and more efficient to make decisions about more government issues, conduct public opinion polls and

referendums much faster and cheaper than now. If now the example of Switzerland with its dozens of referendums per year is unique, an open vote on thousands of different issues can become a reality all over the world. Moreover, I am convinced that the secret of voting should also be discarded, like the remnants of the past. However, this is a topic for a separate study, and there will not be any development here. Personalization and the absence of anonymity, strong identity of the internet-users will lead to a new level of e-participation. E-petitions, participation budget, more tools to investigate public money frauds and other instruments of direct democracy will help to balance the current political system and give an opportunity to build a radically new model of government. The idea of "liquid democracy" for example (Paulin, A, 2014) is based on the conception of personal engagement in public affairs of the vast majority of the society and the renovation of direct democracy. As Tim O'Reilly (2011) stated,

> *"government is, at bottom, a mechanism for collective action" (p.14).*

The opening of personal information can provide us new possibilities to organize collective actions more effectively.

The transparent society will cause a new wave of lobbyism of laws. In many countries with specific legal traditions, the quality of laws does not affect much the social life. Especially it concerns a society with a low level of public confidence, trust in state institutions. In Ukraine, people mostly share a western tradition of individualism and care much more about their personal benefits than the common ones. Additionally, in many social situations, it is easy enough to break the law. This choice will save your time, financial and mental resources. The person almost always cares about himself more than about society as a whole. It almost never will lead to an official punishment. However, the more information is opened, the harder it becomes to break the law. Moreover, more and more people understand that the only way to change their own lives is to change the law, not to break it. Thus, the announcement of the introduction of the list of persons liable for military service in Ukraine and the reconciliation with this register when going abroad has already caused the intensification of public discussion about the need to switch solely to a contract army. Precisely because earlier it was possible to solve these issues individually, with the introduction of the registry this will become many times more complicated. Thus, many people can support a particular idea in society, while not having enough personal interest to launch a public campaign to support this idea in parliament.

The opening of personal information has enormous potential to influence progress in many social sciences and humanities, such as sociology, economy, political science, jurisprudence, psychology, anthropology, urban studies, design and architecture studies and many others. The development in these areas can bring us many valuable discoveries and provide us solutions for very complicated social problems we have nowadays. Our scientific progress today is depending on the big data studies and the availability of the considerable numbers of different datasets, many of which include some personal information. Of course, people can try to slow down the progress, but the development of the science and the society as a whole is inevitable. (See for ex. Molloy, J. C., 2011). The more the big data will continue to develop, the more expensive personal information will become.

5. Conclusion

Trust is a two-way process. Officials cannot be open in a closed society. In addition, even the most honest and open officials will not lead to increased trust in a society where everyone got accustomed to lying, to hide information from each other and from the state, where the law is repeatedly violated everywhere.

The right of information privacy is under intense pressure from two sides. First, significant economic, scientific, social benefits result by opening up all information. Secondly, the development of technological progress catastrophically reduces the effectiveness of any attempts to protect privacy. Moreover, every year, both these trends will only increase. Therefore, the question is which scenario of cancellation of the right to information privacy is more likely. The first option involves the development of current trends and the gradual erasure of the boundaries between the private and public spheres. First, the existing rules applied to public persons for refusing privacy are beginning to be applied to all citizens. Then the punishments for the dissemination of personal information are gradually relaxed, and, after a while, they will be abolished altogether. Undoubtedly, this process will proceed at different rates in different countries, depending on the conditions of development and historical features of a particular society. However, the advantages of open data, which will be given to countries that have decided on more radical reforms, will become a convincing argument for the rest of the world. The second scenario envisages the existence of a country or group of countries that have decided to create new legislation and open all the data, thus acting as offshore zones for large corporations that do not want to limit themselves in information privacy. As in the case of offshore tax zones, other countries will be forced to weaken their demands for retaining capital. Most likely, such countries can become those in which the tradition of protecting information privacy is not as strong as in the Western countries. However, regardless of the way in which the development of historical progress will go, the abolition of the right to information privacy and the building of a fully open society is our collective, not too distant future.

References

Ackles D. (10 April 2017). A controversial law takes aim at Ukraine's anti-corruption NGOs. Opendemocracy.net, Retrieved April 18, 2017, from: https://www.opendemocracy.net/od-russia/devin-ackles/controversial-law-takes-aim-at-ukraine-s-anti-corruption-ngos

Big Data and Privacy: A Technological Perspective, Executive Office of the White House, President's Council of Advisors on Science and Technology, May 2014; Retrieved March 16, 2017, from: https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf

Burridge Tom (2016) Ukraine politicians' huge cash piles exposed in reform drive. BBC, Retrieved March 23, 2017, from: http://www.bbc.com/news/world-europe-37785741

Children's online privacy protection act of 1998 (1998). Federal Trade Commission.. Retrieved March 10, 2017, from: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

Connecting the dots: building the case for open data to fight corruption (23 February 2017) , Transparency International, Retrieved February 25, 2017, from:http://www.transparency.org/whatwedo/publication/connecting_the_dots_building_the_case_for_open_data_to_fight_corruption

Crabtree, A., & Mortier, R. (2016). Personal Data, Privacy and the Internet of Things: The Shifting Locus of Agency and Control. Retrieved March 10, 2017, from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874312

Creating Value through Open Data Study on the Impact of Re-use of Public Data Resources (2015) European Commission. Luxembourg, Publications Office of the European Union. Retrieved March 10, 2017, from: https://www.europeandataportal.eu/sites/default/files/edp_creating_value_through_open_data_0.pdf

Davies, T. (2010). Open data, democracy and public sector reform. A look at open government data use from data. gov. uk., Retrieved February 15, 2017, from: http://www.opendataimpacts.net/report/wp-content/uploads/2010/08/How-is-open-government-data-being-used-in-practice.pdf

Dewan Sh. Judges Replacing Conjecture With Formula for Bail (June 25, 2015). The New York Times. Retrieved April 20, 2017, from: https://www.nytimes.com/2015/06/27/us/turning-the-granting-of-bail-into-a-science.html?_r=1

Dey, R., Ding, Y., & Ross, K. W. (2013, October). Profiling high-school students with facebook: how online privacy laws can actually increase minors' risk. In Proceedings of the 2013 conference on Internet measurement conference (pp. 405-416). ACM.

G20 Anti-Corruption Open Data Principles Assessment (2015), Report, Retrieved April 11, 2017, from: http://www.g20.utoronto.ca/2015/G20-Anti-Corruption-Open-Data-Principles.pdf

Embracing Innovation in Government - Global Trends (12-14 February 2017), World Government Summit Dubai, United Arab Emirates, Report, Retrieved February 27, 2017, from: http://www.oecd.org/gov/innovative-government/embracing-innovation-in-government.pdf

Huijboom, N., & Van den Broek, T. (2011). Open data: an international comparison of strategies. European journal of ePractice, 12(1), 4-16.

Kiriakidis, S. P., & Kavoura, A. (2010). Cyberbullying: A review of the literature on harassment through the internet and other electronic means. Family & community health, 33(2), 82-93.

Korczynski, M. (2000). The political economy of trust. Journal of Management Studies, 37(1).

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. Proceedings of the National Academy of Sciences, 110(15), 5802-5805.

Landau, S. (2016). Is It Legal? Is It Right? The Can and Should of Use. IEEE Security & Privacy, 14(5), 3-5.

Molloy, J. C. (2011). The open knowledge foundation: open data means better science. PLoS Biol, 9(12), e1001195

Open Government Declaration, Open Government Partnership (September 2011), Retrieved February 14, 2017, from: http://www.opengovpartnership.org/about/open-government-declaration

O'Reilly, T. (2011). Government as a platform. Innovations, 6(1), 13-40. Retrieved February 15, 2017, from: http://www.mitpressjournals.org/doi/pdf/10.1162/INOV_a_00056

Paulin, A. (2014, May). Through liquid democracy to sustainable non-bureaucratic government. In Proc. Int. Conf. for E-Democracy and Open Government (pp. 205-217).

Sandford Alasdair. (2016) Vast wealth declared by Ukraine politicians causes shock and anger. Euronews. Retrieved March 23, 2017, from: http://www.euronews.com/2016/10/31/vast-wealth-declared-by-ukraine-politicians-causes-shock-and-anger

The Global Open Data Index 2016/2017 - Advancing the State of Open Data Through Dialogue (2017). Retrieved May 2, 2017, from: https://index.okfn.org/place/ua/

The Value of Big Data and the Internet of Things to the UK Economy, Feb 2016, CEBR & SAS Retrieved March 8, 2017, from: https://www.sas.com/content/dam/SAS/en_gb/doc/analystreport/cebr-value-of-big-data.pdf

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Retrieved March 2, 2017, from:: http://data.europa.eu/eli/reg/2016/679/oj

Rickless, Samuel C., The Right to Privacy Unveiled (2007). San Diego Law Review, Vol. 44, No. 1, 2007.

Simon J., Bass Th., Boelman V. & Mulgan G. (2017) Digital Democracy: The Tools Transforming Political Engagement, Retrieved March 4, 2017, from: http://www.nesta.org.uk/sites/default/files/digital_democracy.pdf

UK Digital Strategy (1 March 2017), Department for Culture, Media & Sport and The Rt Hon Karen Bradley MP, Retrieved March 2, 2017, from: https://www.gov.uk/government/publications/uk-digital-strategy

Yu, H., & Robinson, D. G. (2012). The new ambiguity of'open government', Retrieved March 1, 2017, from: https://poseidon01.ssrn.com/delivery.php?ID=958073117127104007008097089105113069125005091051065087123098019010087005031119094103030041056026022014118074100085011072092124108051086036081065070120027006116069039018035121093083001127070080078087082104094091113031119123115083092022100105004120092&EXT=pdf

Xue, M., Magno, G., Cunha, E., Almeida, V., & Ross, K. W. (2016). The Right to be Forgotten in the Media: A Data-Driven Study. Proceedings on Privacy Enhancing Technologies, 2016(4), 389-402.

About the Author

Tetiana Korshun

Tetiana Korshun works as an Associate Professor at The Department of Philosophy and Social and Political Sciences at the University of Customs and Finance (Dnipro, Ukraine). After her Master's degree in Law from the National Law University named after Yaroslav The Wise (Kharkiv, Ukraine), she made her postgraduate studies and thesis in philosophy, Oles Honchar Dnipro National University (Dnipro, Ukraine). Awarded a Ph.D., her research interests include human rights, legal philosophy, e-government, online education.

