D.6.4
ELSI guidance on ICT tools design

WP6 – Ethics

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 822337.

Populism and Civic Engagement

1.0 About this document

Work Package 6 Lead: Trilateral Research
Task Lead: The Democratic Society
Contributors: Trilateral Research, Citizen Foundation, TU Dresden
Due Date of Deliverable: 31 October 2019

This document outlines the potential Ethical, Legal and Social Issues (ELSI) that could be raised by the ICT tools created as part of the PaCE project and provides recommendations for their development. These recommendations can also serve as guidance for other consortia or organisations designing similar tools. This document is the official ELSI report for the PaCE project, under work package 6 'Ethics', deliverable D6.4.

Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

A brief summary of revisions will be recorded in the table below:

HISTORY OF CHANGES			
VERSION	**DATE**	**KEY CHANGES**	**AUTHOR**
0.1	06/09/2019	Initial version	The Democratic Society and Trilateral Research
0.2	07/10/2019	Insertion of revisions by technical partner Citizen Foundation	The Democratic Society and Trilateral Research
0.3	22/10/2019	Insertion of revisions following consortium review	The Democratic Society and Trilateral Research
1.0	31/10/2019	Final version submitted to the EC	The Democratic Society and Trilateral Research

The working language of this document will be English (EN), as required for reporting purposes by article 20.7 of the Grant Agreement.

TABLE OF CONTENTS

1.1 About PaCE

Across Europe there is a rise of political movements that claim to challenge liberal elites and speak for the 'ordinary person' - movements that can be loosely categorised as 'populist'. Many of these movements have undesirable tendencies. The Populism and Civic Engagement project (PaCE), with others, aims to better understand and respond to the negative tendencies of populist movements, to build upon the lessons of positive examples (such as Reykjavik), and hence play a part in constructing a firmer democratic and institutional foundation for the citizens of Europe.

PaCE will analyse, in detail, the type, growth and consequences of such movements in terms of their particular characteristics and context. From this, it will analyse the causes of these movements and their specific challenges to liberal democracy. In particular, it will focus on transitions in these movements (especially changes in leadership) as well as how they relate to other kinds of movements and the liberal reaction. PaCE will propose responses to these challenges, developing risk-analyses for each kind of response, movement and transition. To this end, it will employ the agent-based simulation of political processes and attitudes to allow for thorough risk analyses to be made. Throughout the project, it will engage with citizens and policy actors, especially groups under-represented in public affairs, face-to-face and via new forms of democratic participation appropriate to our digital age to help guide the project and to comment on its outputs.

The project will develop new tools, based on machine-learning algorithms, to both identify and track populist narratives and aid online consultation. It will result in specific interventions aimed at the public, politicians, activists and educators. It will look further into the future, developing new visions concerning how different actors could respond to populism and it will warn about longer-term trends.

1.2 Consortium

#	PARTICIPATING ORGANISATION	CODE	COUNTRY
1	Manchester Metropolitan University (**coordinator**)	MMU	UK
2	City of Reykjavik	RVK	Iceland
3	The Centre for Liberal Strategies Foundation	CLS	Bulgaria
4	The Paris-Lodron University	PLUS	Austria
5	The Technical University of Dresden	TUD	Germany
6	The Democratic Society	DEM	Belgium
7	Trilateral Research	TRI	Ireland
8	University of Helsinki	UH	Finland
9	Citizens Foundation	CF	Iceland

Table 1 Consortium Partners

2.0 Introduction Ethical, Legal, Social Issues (ELSI) Guidance

2.1 Goal of report

The PaCE project aims to develop **Information and Communications Technology (ICT) tools** under the Work Package (WP) 3 *Narrative Analysis and ICT Tools*. WP 3 will produce the following three deliverables:

- **D3.1: Definitions and operationalisations of populism:** Report containing definitions and operationalisations of populist narratives and counter-narratives; empirical types of populist narratives and counter-narratives; occurrences of populist narratives and counter-narratives in the public media.

- **D3.2 : Tool to identify populist narratives:** Publicly available tool (algorithm or application software) allowing policy actors and citizens to identify populist narratives and counter-narratives in the media and allowing policy actors and citizens to assess their individual exposure to public populist narratives and policy actors and citizens to adequately react to populist public narratives.

- **D3.3: Results of online experiments:** Report containing analysis of the effects of populist narratives in online experiments, analysis of the properties of counter-narratives in online experiments, policy recommendations on how to react to populist narratives

The consortium sees the benefit of using ICT tools to inform the research of the PaCE project, and to highlight grievances taking the shape of populist (or related) narratives publicly voiced online by people across Europe and globally. This will provide the consortium partners with an opportunity to draw the attention of citizens, policymakers, and researchers to those grievances by clustering them into different categories, and the manner in which these ebb and flow over time. In doing so, policy-makers will be able to distinguish between different types of narratives and better understand the voices of voters, whilst citizens will be able to reflect on these narratives and their evolution. The output of this activity will also contribute to the academic research on populism by providing a resource to researchers on this subject matter to better understand public discourse online taking the shape of populist rhetoric (or related).

There are, however, potential drawbacks to using technology to study a social phenomenon - technology may invade privacy, be used to undertake surveillance, compromise the rights of the individual or harm the society at large. These negative impacts can be regarded within the categories of ethical, legal and social issues (ELSI). The goal of this report PaCE deliverable 6.4 is therefore to present the analysis of potential risks that the use of the project's ICT tools poses for individuals and communities and recommend ways in which these can be mitigated. It also

highlights the process that has taken place in Task 6.4 in order to identify the potential ethical, legal and social issues raised by these tools and to address these issues with the partners responsible for developing the tools (CF) and the consortium as a whole in order to mitigate the risks. Further ethical, legal and social considerations will continue to be made after the finalisation of this report and as the tools develop. This ethical support will be provided as part of T6.2 (Ethical monitoring) and T6.5 (Guidance on public engagement).

The analysis conducted here draws from research ethics but extends beyond this sphere since the ICT tools developed will be used not only by researchers in the PaCE project and beyond, but potentially also by policy-makers, representatives of the civil society, and the general public. Furthermore, as it is largely recognised in the literature on internet research ethics, research on the internet deeply challenges classic research ethics concepts and processes (such as consent or human subject). Sugiura, et al. argue that, "although online research appears to be accountable to established ethical 'rules', current ethical guidelines are confusing and not fit for purpose"[1]. They add that ethical standards should be updated to accommodate the new modes of data collection. The massive use of the internet is generating a large amount of data that is of particular interest to social scientists to understand society today. However, traditional ethical guidance and practice struggle to keep up with these new ways of collecting data. This is why an ELSI analysis was found to be a more appropriate means of identifying potential ethical, legal and social issues that may emerge within the development of the PaCE ICT tools and to mitigate these.

At present, there is no internationally agreed-upon method for carrying out an ELSI assessment. Nonetheless, the variety of approaches obtained from a review of the current literature are largely concerned with the identification of risks and the means of overcoming those risks. The present ELSI study draws from the methodology of the Data Protection Impact Assessment (DPIA) – an essential requirement of the General Data Protection Regulation (GDPR) of the European Union. The report analyses the potential risks of PaCE's ICT tools and implements the required mitigation measures, as part of Task 6.4. In addition to providing support for the development of PaCE's technological tools, the present report also offers recommendations to ensure ethical, legal and social considerations are taken into account for similar ICT tools-related projects.

Guiding principles

Core guiding principles for the development of PaCE ICT tools are based on Article 34 of the PaCE Grant Agreement and can also be found in the PaCE Ethics Handbook. With regards to research integrity, the Grant agreement refers to the European Code of Conduct for Research Integrity by the ALLEA[2]. This implies compliance with the following fundamental principles:

- **reliability** in ensuring the quality of research reflected in the design, the methodology, the analysis and the use of resources;

[1] Sugiura, Lisa, Rosemary Wiles, and Catherine Pope. "Ethical Challenges in Online Research: Public/Private Perceptions." *Research Ethics,* Vol. 13, No. 3–4, July 2017, pp. 185–186, doi:10.1177/1747016116650720.
[2] ALLEA, European Code of Conduct for Research Integrity, March 2017. https://allea.org/code-of-conduct/

- **honesty** in developing, undertaking, reviewing, reporting and communicating research in a transparent, fair and unbiased way;
- **respect** for colleagues, research participants, society, ecosystems, cultural heritage and the environment;
- **accountability** for the research from idea to publication, for its management and organisation, for training, supervision and mentoring, and for its wider impacts and means that beneficiaries must ensure that persons carrying out research tasks follow the good research practices and refrain from the research integrity violations described in the Code.

Furthermore, from the proposal stage of the project, the consortium's partners committed to taking into account **the social responsibility principle** as developed in the SATORI project that defines it as the "responsibility to consider the societal impacts of research and innovation and for taking steps to minimise anticipated harm and maximise benefits"[3]. This is a key element of this ELSI analysis and is especially important considering the highly polarised context the PaCE research project engages with.

The PaCE consortium has voluntarily adopted the following principles, agreed at its kick-off meeting (February 2019). These principles are compatible with, and supportive of, the above legal, contractual and institutional requirements. The consortium aims to:

- Adhere to the highest standards of legal compliance, integrity, ethics, fairness and openness;
- Seek to do research of the highest possible rigour, significance and usefulness;
- Actively engage with, and listen to, outside voices (other academics, citizens, stakeholders, etc.);
- Sensitively address any cultural issues (gender, minorities, citizens' rights, etc.);
- Actively promote the careers of early stage researchers working on the project;
- Use all project resources carefully and appropriately, getting the greatest value for money.

The PaCE Ethics Handbook can be consulted for more details about the guiding principles.

2.2 Methodology

The report was developed through a literature review of the current debate in the field of internet research and ethics and through several discussions with the developers of the ICT tools (two conference calls were held between DS, TRI and CF and several exchanges over email and Slack) and other partners in the PaCE project. Furthermore, the findings of this report are based on a meeting with consortium partners held on October 4th, 2019 to discuss the development of the ICT tools and its potential implications. Finally, the report went through a review process. CF was first invited to review and comment on an earlier version of this deliverable which was then revised by DS and TRI. The report was then sent to all consortium partners for comments and review.

[3] SATORI, "Report on standardizing operating procedures in ethics assessment", July 2017. http://satoriproject.eu/media/D7.1_Standardizing_ethics_assessment.pdf

The ELSI guidance report has been developed simultaneously with the ICT tools themselves in order to influence the creation of said tools. Given that the ELSI guidance report is due before the finalisation of the ICT tools and the task (T6.4) within which DS and TRI have been providing ethical support for the ICT tools development, the present deliverable reports on the ELSI process that has taken place so far, highlights the potential ethical, legal, and social issues that have been identified, and ways to mitigate them. Whereas some mitigating measures have already been implemented as part of T6.4 and in discussion with the technical lead (CF), other measures that could not yet be implemented considering the timing of the tools development have been identified and will be explored at a preliminary stage. This includes in particular the framing and language that will be used for the public website. As part of the ethical monitoring TRI is conducting throughout the PaCE project (Task T6.2), TRI will ensure that these and additional concerns are addressed even after the finalisation of the ELSI guidance report. Furthermore, as part of T6.5 on public engagement, TRI and DS will provide further advice to the technical lead (CF), especially in relation to the public platform that is being developed.

2.3 Audience

The main audiences for the ELSI guidance on ICT tools report are the PaCE partners themselves and similar projects that aim to include ICT tools as part of their research activities. As a public report, it also aims to inform any interested parties, whether researchers, policy-makers, or the general public, on the potential ethical, legal, and social issues raised by the ICT tools developed in PaCE and the measures put in place to mitigate them.

2.4 Information and Communication Technology (ICT) tools considered

Specifically, three ICT tools are being developed for the PaCE project in the realm of Deliverable 3.2:

- **Search tool**: Keyword search tool to search for keywords in the Common Crawl and, potentially, Twitter public datasets (at the time of the writing of this deliverable, the use of Twitter data was still to be confirmed).
- **AI Training tool**: Artificial Intelligence (AI) training app that will be used to recognise different types of populist narratives. It will be trained on the data from the search tool.
- **Web Application**: Web app giving public access to the results of the content that has been collected with the search tool and filtered with the AI tool.

3.0 Information and Communication Technology (ICT) Tools

3.1 Description

Under Work Package 3 'Narrative Analysis & ICT Tools' of the PaCE project, the consortium aims to develop and use ICT tools to identify and analyse populist narratives online.

> *T3.2 Employing Hermeneutic Computational Narrative Analysis (HCNA) to identify populist narratives and counter-narratives, as well as to locate these narratives in the public media.*[4]

Citizen Foundation (CF) is developing search tools to gather data online towards the above goal. It is using Common Crawl data scraped from the web from 2014 onwards that is publicly available as an Amazon S3[5] Public Dataset. Common crawl is a non-profit 501(c)(3) organization based in San Francisco, USA, crawling the web each month and providing a dataset of publicly available data to civil society and researchers[6]. The PaCE project will focus on the Common Crawl data from publishing sites, such as blogs and general media sites. In addition, the social networking service Twitter has been contacted by the PaCE partners to allow access to their publicly available data via the same keyword search that is used on Common Crawl data. However, at the time of the writing of this deliverable, the process is still ongoing, and no decision has been reached by Twitter to make the dataset available to the PaCE consortium during the finalisation of this report. Twitter specifically notes that "crawling the Services is permissible if done in accordance with the provisions of the robots.txt file, however, scraping the Services without the prior consent of Twitter is expressly prohibited"[7].

The Common Crawl dataset contains petabytes of data collected over years of web crawling. The dataset contains raw web page data, metadata extracts and text extracts. Common Crawl data is stored on Amazon Web Services' public dataset and on multiple academic cloud platforms across the world, making the dataset accessible for researchers and civil society organizations.

For the PaCE ICT tools, only the top pages based upon the PageRank[8] are being considered for the narrative search, entailing the data from the top four million websites. The dataset is being searched for open source narratives in text form through the use of selected keywords. Relevant narratives between 200-1500 characters are stored. The tool is trained to exclude any personal data such as email addresses, phone numbers or Twitter handles. It does not contain pictures. The narrative search seeks to highlight discussions of the general public online.

---

[4] According to the PaCE Grant Agreement
[5] Common Crawl. http://commoncrawl.org/the-data/
[6] Amazon, "Amazon S3".. https://aws.amazon.com/s3/
[7] Twitter. "Twitter Terms of Service". Last modified May 25, 2018. https://twitter.com/en/tos#intlTerms
[8] PageRank is the process used by Google to determine the importance of a web page. A link to a page is effectively a "vote", weighted by how important the linking page is itself.

3.2 Search using keywords

The PaCE consortium has developed a list of **keywords** in different languages to search the dataset for narratives framed in populist and related political rhetoric. The same keywords will be used for the Common Crawl search activities and the Twitter search alike, in case Twitter data is used. The development of the list of keywords was led by Technische Universität Dresden (TUD), with the support of the whole consortium. Four sets of keywords were developed to identify four types of narratives referring to four different types of political rhetoric: *populism, anti-democratic, nativism*, and *liberal democratic*, based on the typology developed in WP 1. At the time of the writing of this deliverable, all the different types of narratives to be searched and their labelling was still to be confirmed.

The keyword search is planned to involve two different strategies in order to be as efficient as possible. The first entails high **precision**, enabling the confident identification of a good number of actual narratives, but also potentially missing out a large number of relevant ones. The second entails high **recall**, enabling the identification of a large number of relevant narratives but also narratives that actually do not fit within the identified categories (i.e., large amount of false positive).[9]

The following links to the Website Github provide an overview of the keywords issued for the web scraping activity:

- https://github.com/CitizensFoundation/ac-keyword-scanner/blob/master/exampleKeywords/additionalKeywords.txt; and
- https://github.com/CitizensFoundation/ac-keyword-scanner/blob/master/exampleKeywords/essentialKeywords.txt

The search is carried out in several different languages and will ultimately be made available to a wider audience in English. The following languages are currently being considered for the ICT tool and will be finalised during tool development stage:

- English (UK),
- English (US),
- Icelandic,
- Norwegian,
- Swedish,
- Danish,
- Finnish,
- German,
- Dutch,
- French,

[9] Keywords and search strategy presented by TUD at the consortium meeting in Brussels on June 25-26th, 2019.

- Spanish,
- Italian,
- Greek,
- Polish,
- Hungarian,
- Turkish,
- Bulgarian,
- Czech

3.3 Intended use

The aim of the ICT tools developed in PaCE is, as specified in the PaCE Grant Agreement, to produce "*a publicly available tool (algorithm or application software) allowing policy actors and citizens to identify populist narratives and counter-narratives in the media and allowing policy actors and citizens to assess their individual exposure to public populist narratives and policy actors and citizens to adequately react to populist public narrative*."[10]

The objective is to identify populist and related (anti-democratic, nativist) narratives, as well as possibly liberal narratives online in order to gain an overview that may be as comprehensive and precise as possible on these discourses. Ultimately, this overview will help to better understand the social reality, ideas, and discourses that are generated and expresses dissatisfaction with those that are identified as the "elite" as opposed to the "ordinary person", i.e., populism, and that fuels votes for populist parties.

Another objective of the task is to highlight that populist narratives do not only entail negative tendencies. These narratives may actually raise legitimate claims that should be taken seriously by elected officials. As the populism expert Kirk Hawkins suggests in an article published in *The Guardian*, "instead of trying to silence populist voices, we should understand their concerns and engage with them"[11]. The ICT tools aim to highlight these narratives so that they may be heard.

Similarities between narratives will be quantified and highlighted, showing trends and shifts in perspectives around an issue and the way it is framed by relying on classic populist rhetoric or related types of political rhetoric. More specifically, the narratives that are being shared more widely will be aggregated via a percentage marking their dominance. In doing so, the developed ICT tools will allow both policy actors and citizens alike to identify the dominant narratives. It remains to be decided whether the ICT tool should include the location of where the narratives are being discussed. This would be especially helpful to policymakers to provide them with a national perspective on the issues discussed.

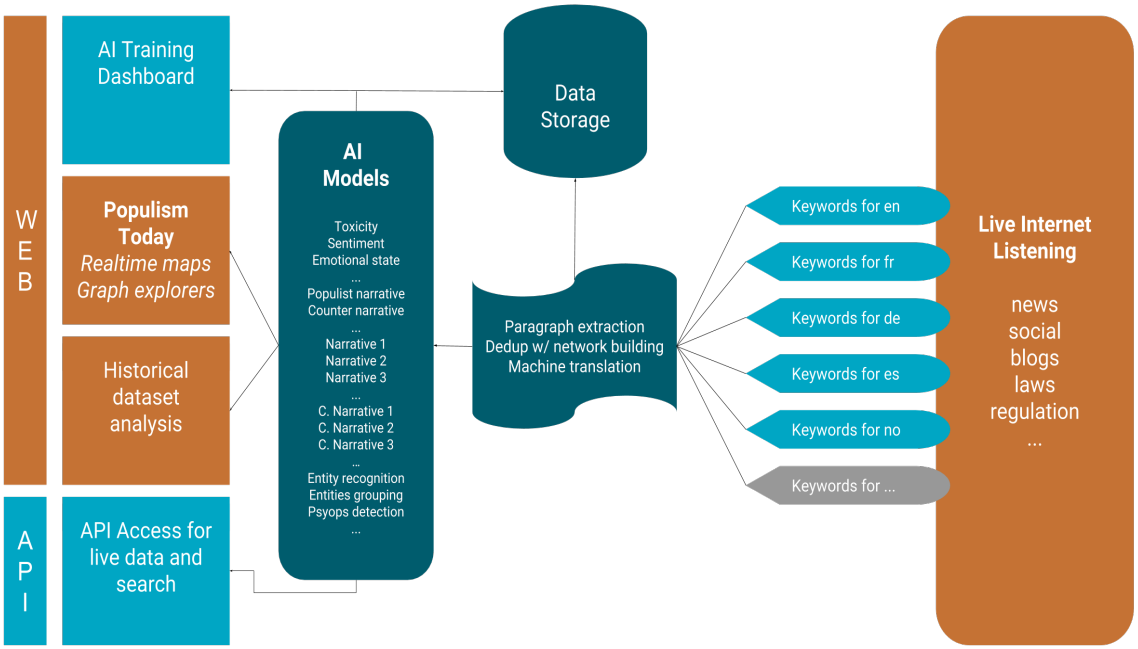
[10] According to PaCE Grant Agreement.
[11] Hawkins, Kirk. "Don't try to silence populists - listen to them", *The Guardian*, 9 March 2019. https://www.theguardian.com/world/commentisfree/2019/mar/09/dont-try-to-silence-populists-listen-to-them

3.4 Intended users

The potential and intended users of the ICT tools developed for the PaCE project depends on the type of tool. The tools will be accessible by any interested party via the repository Github. The publicly accessible Website will provide policy-makers, researchers, the general public and media representatives the opportunity to review the narratives of the general public online.

3.5 Data flows

The following chart developed by the PaCE project visualizes the data and information flows between the above-mentioned ICT tools developed for the Deliverable 3.2 of the PaCE project.



Source: Graphic representation of the ICT tools presented by Robert Bjarnason (CF) at the Kick-off meeting of the project in Manchester, February 6-7th, 2019.

Common Crawl

The servers of the Common Crawl datasets are stored in California (USA) on the Amazon Simple Storage Service. PaCE project partners query the open source dataset of Common Crawl. The dataset is crawled using keywords and then filtered with an AI trained model that will be publicly available to identify narratives published online by the general public. The list of keywords has been developed by the partners of the PaCE consortium and are made public on Github. The data repository of the PaCE project is located at the TU Dresden, in line with any GDPR considerations within the European Union.

Twitter

Depending on the availability of the Twitter dataset, it will also be searched for the selected publicly available keywords. The selected narratives will be downloaded and stored on the same data repository system provided by TU Dresden. As part of live listening, the AI-trained app will scrape the Web for narratives that are currently being published online.

Licences and deletion of data

The software developed by Citizen Foundation is published under the General Public License v3.0 (GNU) open source license, and the developed code is available on the public repository Github. More information about the licenses can be found here: https://github.com/CitizensFoundation/your-priorities-app/blob/master/LICENSE.md.

At the end of the project, the data will either be manually deleted by the Citizens Foundation from the database – if there is no general interest in archiving the web application for a historical review of narratives within the time period of the PaCE project – or the data will be archived and retained in pseudonymised form for historical and research purposes, in keeping with GDPR requirements. No live web scraping will be carried out after the end of the project.

While the partners are taking utmost care to safeguard individual privacy, both during and after the end of the project, the consortium remains open to deleting individual data under the right to be forgotten if individuals or organizations approach the PaCE partners.

Personal data

The ICT tools will be designed to filter data in such a way as to minimize the accidental display of personal information from the Common Crawl archive as well as any potential Twitter data. This will primarily be done through the following processes:

- We will only process data from Common Crawl from the top 10% ranked internet sites based on popularity. Considering the popularity of these websites, we may expect that personal data has been removed from them already.
- We will use filters to remove:
    - phone numbers
    - email addresses
    - GPS coordinates
    - physical addresses
- We will also train AI models to filter out all irrelevant data from our keyword searches including any accidentally disclosed personal data.

4.0 Current debates around the use of ICT tools

In essence, the ICT tools developed for the PaCE project will rely on web scraping and crawling. Web scraping, or the automatic extraction of data from the Web, is becoming an increasingly common practice for industry and academic research projects. Landers et al. explain that web crawling involves developing and running a script that automatically browses the web and retrieves the needed data[12]. These crawling applications (or scripts) are conventionally developed using such programming languages as R and Python. Once the required data is parsed from the selected Web repository, it needs to be cleaned, pre-processed, and organized in a way that enables further analysis of this data[13].

The very notion of data refers to any information that has been converted into binary or digital form. The vast volumes of data available online provide a real-time representation of numerous processes, relationships and interactions that take place online, thereby presenting academic researchers with the opportunity to answer new and old research questions with new rigour and precision[14], including those around contemporary populism and civic engagement. It must be noted, however, that the harnessing of such volumes of data can potentially pose legal, societal, and ethical risks, which will be discussed in this section.

Smart Information Systems (SIS) - driven by AI and big data analytics - are a subset of ICT, and many of the ethical issues applicable to ICT are also applicable to SIS. In a review of 809 papers discussing ethics in ICT, Wright and Stahl found that 177 addressed the issue of privacy and data protection, which makes this the most prominent issue[15]. However, numerous other issues are also frequently discussed. These include autonomy of users, their agency, trust, consent, identity, inclusion and digital divides, security, harm, misuse, and deception, to name just a few.

Despite its growing use, the legislation behind web scraping, and the development of ICT tools in general, still remains an ongoing debate, largely guided by legal theories and concepts, such as copyright infringement, terms of use, the EU 's General Data Protection Regulation (GDPR), etc.

Wright and Raab caution that some issues and impacts can be categorised in different ways[16]. For example, autonomy and dignity may be classified as privacy issues, but they may also be regarded as ethical issues. Moreover, some scholars argue that, in the context of internet-based research,

[12] Landers, Richard, Brusso Robbie, Cavanaugh Katelyn & Collmus Andrew. "A Primer on Theory-Driven Web Scraping: Automatic Extraction of Big Data From the Internet for Use in Psychological Research". *Psychological Methods.* Vol. 21, No. 4, May 2016, pp. 475-492. doi:10.1037/met0000081.
[13] Krotov, Vlad and Leiser, Silva. "Legality and Ethics of Web Scraping".*Proceedings of the Twenty-fourth Americas Conference on Information Systems*), New Orleans, September 2018.
[14] Ibid
[15] Stahl, Carsten Bernd and Wright, David. "Ethics and Privacy in AI and Big Data: Implementing Responsible Research and Innovation". *IEEE Security and Privacy*. Vol 16, No. 3, May/June 2018, p. 27, doi: 10.1109/MSP.2018.2701164
[16] Wright, David and Raab, Charles D. "Constructing a surveillance impact assessment". *Computer Law and Security Review*. Vol. 28, Issue 6, December 2012, p. 617, https://doi.org/10.1016/j.clsr.2012.09.003

privacy is in itself inherently social, relational and socio-technical and should not be addressed in the traditional individualist sense[17].

This document is structured around the key issues and potential consequences for the individual and society in general. It introduces the current requirements and ongoing debates around the legal, ethical and social aspects of ICT tools. The document begins with the legal requirements as spelt out in the GDPR (4.1), followed by debates in research ethics (4.2) and intellectual property online, (4.3) potential risks in terms of surveillance and related individual and societal impacts (4.4), and ends with individual and social harms (4.5) As such, it provides a framework to engage with the specific ELSI raised by the tools developed in PaCE whose analysis is presented in section 5 of this document.

4.1 General Data Protection Regulation (GDPR)

A key document regulating ICT is the General Data Protection Regulation (GDPR)[18] introduced by the EU in 2016 with the aim of regulating the processing by an individual, a company or an organisation of personal data relating to individuals in the EU. It replaces the apparently outdated 1995 Data Protection Directive. Member States had to ensure that it was fully implementable in their countries by May 2018.

The GDPR is based on the approach of privacy as a fundamental human right. The GDPR regulation has a wide impact beyond the European Union due to its wider territorial scope and its definition of personal data.[19]

The GDPR is structured around six key principles:

- Fairness and lawfulness;
- Purpose limitation;
- Data minimisation;
- Accuracy;
- Storage limitation; and
- Integrity and confidentiality.

To ensure the operationalisation of these principles, a proactive design, also known as privacy by design, and conceptualisation of privacy as the default for any data collection activity is needed. Furthermore, it is the responsibility of data controllers to adopt the necessary transparency and accountability measures to protect individual privacy[20].

[17] Zimmer, Michael and Kinder-Kurlanda, Katharina (eds.). *Internet Research Ethics for the Social Age: New Challenges, Cases, and Contexts*. Peter Lang, New York, 2017, p. xxiii.
[18] European Parliament and The Council. Regulation 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://data.europa.eu/eli/reg/2016/679/2016-05-04
[19] Goddard, Michelle. "The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact". *International Journal of Market Research*, Vol. 59. No. 6, November 2017, pp. 703–705. https://doi.org/10.2501/IJMR-2017-050
[20] Ibid

The GDPR creates the same playing field for data collectors within the European Union, ensuring the privacy of individuals. The European Union Agency for Network and Information Security (ENISA) argues that if "privacy principles are not respected, big data will fail to meet individuals' needs; if privacy enforcement ignores the potential of big data, individuals will not be adequately protected. Therefore, all involved stakeholders should work together in addressing the new challenges and highlighting privacy as a core value of big data. Technology, instead of being a rival in this attempt, should be the main weapon and support tool."[21] Standards similar to those set by the GDPR have been applied in many other countries and states, such as Brazil or California.

Personal information and the processing of personal data

Web scraping in the EU should comply with the GDPR according to which personal data should not be processed unless one has a lawful basis to do so. Personal data is defined in Art. 4 as "information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can

be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[22]

Personal data includes (but is not limited to):

- Name
- Physical Address
- Email Address
- Phone Number
- Credit Card Details
- Bank Details
- IP Address
- Date of Birth
- Employment Info
- Social Security Number
- Medical Information
- Video/Audio Recording

In addition, according to Art 9, in the absence of specific exemptions the GDPR generally prohibits the processing of "special categories of personal data", i.e., "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"[23]. Where these data are to be processed, special protections are required.

[21] The European Union Agency for Network and Information Security). "Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics." December 2015. https://arxiv.org/pdf/1512.06000.pdf
[22] European Parliament and The Council. Regulation 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://data.europa.eu/eli/reg/2016/679/2016-05-04
[23] Ibid

It must be noted that personal identities can also inadvertently be revealed when different sources are matched. Sugiura et al. point out that this is problematic as some Web users may not want to remain anonymous, for example writers of blogs, and that in such cases using these blogs without citation would infringe upon copyright or intellectual property[24]. However, it is not definitive that all bloggers should automatically be viewed as authors. In such cases, some scholars argue that researchers should acknowledge the user's authorship and cite their texts as they would more traditional media, but they should be aware that this may compromise anonymity: "Removing identifying data alone will not guarantee anonymity as verbatim quotes can often be traced back via search engines to the original website and thence to the forum member who made them"[25]. More on copyright and intellectual property is covered in sub-section 4.3.

Some privacy regimes around the world, particularly in the United States, work on a fundamental distinction between public and private data. This in turn distinguishes between data which is private, and has particular protections, and data which is in the public domain, and has fewer protections in law. This operates as a legal operates as a legal framework for many web-crawling operations, where the fact that an item of data has been published on a website makes it fair game for collection and use by others, as noted by several scholars[26]. This does not, however, remove any ethical considerations around the re-use of public data for research purposes. This is nonetheless not the legal regime in place in the EU under the GDPR. Personal data that is "public" or "publicly available" is still considered personal data, and therefore all the protections for the data subject, and all the obligations on the data controller or processor, remain. The processing of publicly available personal data is permitted under the GDPR, providing that certain requirements are met, namely the identification of legal grounds for the processing of personal data (these are defined in section 5 in relation to the PaCE project in particular). That personal data is publicly available, and that data subjects may anticipate its processing can influence certain balancing tests and risk assessments within the GDPR.

4.2 Research ethics

Ethics can be described as "a set of concepts and principles that guide us in determining what behaviour helps or harms sentient creatures"[27]. Ethics is not merely a procedural element of ethics applications. In keeping with Markham et al.'s recommendations, ethics should be embedded in research methods; it must be an ongoing concern during data collection, analysis, and dissemination[28]. **This is also an important consideration for our consortium as well as the broader PaCE project.**

---

[24] Sugiura, Lisa, Rosemary Wiles, and Catherine Pope. "Ethical Challenges in Online Research: Public/Private Perceptions", *Research Ethics,* Vol. 13, No. 3–4, July 2017, p. 194. doi:10.1177/1747016116650720.

[25] Ibid

[26] Zimmer, Michael. "Addressing Conceptual Gaps in Big Data research Ethics: An Application of Contextual Integrity", *Social Media + Society,* Vol. April-June 2018, pp. 1-11.https://doi.org/10.1177/2056305118768300; Ravn, Signe, Barnwell Ashley, & Barbosa Neves Barbara. "What is "Publicly Available Data"? Exploring Blurred Public-Private Boundaries and Ethical Practices Through a Case Study on Instagram", *Journal of Empirical Research on Human Research Ethics*, 2019. https://doi.org/10.1177/1556264619850736

[27] Paul, Richard and Elder, Linda. "Miniature guide to Ethical Reasoning", *Critical Reasoning*, 2005. http://www.criticalthinking.org/files/SAM-EthicalReasoning2005.pdf

[28] Markham, A N, Tiidenberg Katrin and Herman Andrew. "Ethics as Methods: Doing Ethics in the Era of Big Data Research", *Social Media + Society*, Vol. July-September, 2018. https://doi.org/10.1177/2056305118784502

There is little doubt that preserving privacy and maintaining anonymity is central to ethical research. Nonetheless, the very features of the internet - searchability and replicability - make it difficult to remove all traces from data that can be linked back to the individual[29]. Robson finds that these features also present an interesting conundrum to researchers due to the rich source of qualitative data that online posting and interactions present on the one hand and the possibility to trace direct quotations back to the original source on the other[30]. He states that there are a number of ways in which online researchers have attempted to overcome these challenges, with the most common being presenting data in a narrative form; fictionalising aspects of the research; creating composite accounts in the form of vignettes; and amalgamating specific examples into generic forms. Paraphrasing, in particular, is an often-used strategy whereby paraphrased quotations can be run through various search engines to test whether the original source can be traced. Robson, however, cautions that none of these precautions are foolproof and can fully take into account the different real-world complexities involved in this type of research - a point that is echoed in research ethics scholarship.

Beyond the legal requirements as set in the GDPR, social scientists and research ethicists have also pointed to the significance of privacy from a social and ethical point of view. For instance, in relation to the analysis of data received from social media and phone records, Boyd and Crawford point to big data as being akin to a troubling manifestation of a 'Big Brother regime' wherein individuals have little or no idea what data is being collected or shared with third parties, thereby threatening their liberty and fundamental rights[31]. This is why Wright and Raab emphasise that those assessing the impact of data analytics should primarily ask: **Does the project or technology have potential social, legal, and ethical consequences other than the purpose for which it is being deployed?**[32]

A key issue in this debate on social media data is whether this data is public or not, and therefore, whether consent is required to process it. Ravn, Barnbell, and Barbosa Neves find that, despite the emerging debate on the ethics of social media research, scholars still tend to rely on traditional understandings of "publicly available data" when doing research on social media platforms[33]. The underlying assumption is that social media users have knowingly published the content in the public domain, thereby waiving off their consent and paving the way for the scraping and analysis of online content as empirical data. This is why the authors assert that **relying on a simple understanding of "publicly available" data is not sufficient for social media research to be ethical**.

---

[29] Zimmer, Michael. "But the data is already public: on ethics of research in Facebook", *Ethics and Information Technology,* Vol. 12, 2010 pp. 313-325.
[30] Robson, James. "Participant Anonymity and Participant Observations", In Zimmer, Michael and Kinder-Kurlanda, Katharina (eds.). *Internet Research Ethics for the Social Age: New Challenges, Cases, and Contexts.* New York, Peter Lang, 2017, pp. 195-196.
[31] Boyd, Danah and Crawford, Kate. "Critical Questions for Big Data", *Information, Communication, & Society,* Vol. 15, No. 5, 2012, p. 664. https://doi.org/10.1080/1369118X.2012.67887
[32] Wright, David and Raab, Charles D. "Constructing a surveillance impact assessment". *Computer Law and Security Review.* Vol. 28, Issue 6, December 2012, p. 617. https://doi.org/10.1016/j.clsr.2012.09.003
[33] Ravn, Signe, Barnwell Ashley, & Barbosa Neves Barbara. "What is "Publicly Available Data"? Exploring Blurred Public-Private Boundaries and Ethical Practices Through a Case Study on Instagram", *Journal of Empirical Research on Human Research Ethics*, 2019

In a similar vein as above, Zimmer contends that "the uncertainty in the intent and expectations of users of social media and Internet-based platforms – often fuelled by the design of the platforms themselves – creates a conceptual gap in our ability to apply the definition of "private information" to ensure subject privacy is properly addressed"[34]. **The onus therefore lies on researchers to move beyond justifications such "the data is already public".** He adds, "it remains unknown whether users truly understood the technical conditions under which they made information visible on these social media platforms or whether they foresaw their data being harvested for research purposes, rather than just appearing onscreen for fleeting glimpses by their friends and followers"[35]. This is especially true in the case of groups that are vulnerable online, such as the youth, older adults, individuals with minimal digital literacy and those whose first language may differ from that of a website's terms of use and conditions[36]. It is therefore difficult to gauge whether users of online platforms are fully aware of the type of data that is being collected, what it is utilised for, who it is shared with, who it is managed by, and how it is stored. This is an important aspect that should be taken into account when designing internet research projects so as to ensure that users' data is handled appropriately.

The ethical guidelines set out by the Association of Internet Researchers frame privacy as "a concept that must include a consideration of expectations", i.e. what an individual may legitimately expect others might do with the content he/she published online[37]. According to Sugiura et al., despite the expectation of a degree of privacy by web users, the greater the acknowledged 'public nature' of a forum – such as posting on social media as opposed to closed chatrooms – the less obligation there may be to protect individual privacy, confidentiality, right to informed consent, etc.[38]

Researchers have in fact long been grappling with concepts such as privacy and the boundary between public and private as it pertains to the Internet[39]. Boyd, for example, has framed the manner in which social media platforms think of privacy in simple, binary terms—"data are either exposed or not"[40]. Against this backdrop, she contends that privacy should instead amount to the users' sense of control over what information is shared, with whom, and under which conditions. On the other hand, such control is lost when different contexts are merged into one when sharing one's posts across different platforms, for example, where different privacy settings apply.

---

[34] Zimmer, Michael. "Addressing Conceptual Gaps in Big Data research Ethics: An Application of Contextual Integrity", *Social Media + Society,* Vol. April-June 2018, p. 5. https://doi.org/10.1177/2056305118768300
[35] Ibid
[36] Ferguson, Robert Douglas. "Negotiating Consent, Compensation, and Privacy in Internet Research", In Zimmer, Michael and Kinder-Kurlanda, Katharina (eds.). *Internet Research Ethics for the Social Age: New Challenges, Cases, and Contexts.* New York, Peter Lang, 2017, p. 271.
[37] Markham, Annette and Buchanan, Elisabeth. "Ethical Decision-Making and Internet Research", *Association of Internet Researchers,* 2012, p. 7. https://aoir.org/reports/ethics2.pdf
[38] Sugiura, Lisa, Rosemary Wiles, and Catherine Pope. "Ethical Challenges in Online Research: Public/Private Perceptions." *Research Ethics,* Vol. 13, No. 3–4, July 2017, p. 193. doi:10.1177/1747016116650720.
[39] Markham, A N, Tiidenberg Katrin and Herman Andrew. "Ethics as Methods: Doing Ethics in the Era of Big Data Research", *Social Media + Society*, Vol. July-September, 2018. https://doi.org/10.1177/2056305118784502
[40] Boyd, Danah. "Facebook's Privacy Trainwreck. Exposure, Invasion and Social Convergence", *Convergence: The International Journal of Research into New Media Technologies.* Vol. 14, No. 1, 2008, p. 16. doi: 10.1177/1354856507084416

Conventional ethical approaches fail to respond to the new challenges posed by the rapidly evolving field of digital research, particularly due to the nature of different media, the scale of data collection, and users´ expectation of privacy. However, it is imperative that **scholars engage with principles of consent, privacy and ownership within this particular context of online platforms**[41]**.** As noted above, assumptions that dismiss any requirement to seek consent because the data is "publicly available" should be challenged. There seems to be a general consensus among experts of the ethics of internet research that a more sensitive approach is required.

Zimmer "invokes Nissenbaum's (2004, 2010) theory of "**privacy as contextual integrity**" as a useful heuristic to guide ethical decision-making in big data research projects"[42]. Rather than prescribing universal rules on ethical big data research, he goes on to suggest that approaching research ethics through the lens of contextual integrity will empower researchers to be more attentive of the normative bounds of how information flows within specific contexts." Here, Zimmer points to Carpenter and Dittrich's proposition to transition from an informed consent-driven to a risk analysis review that addresses potential harms stemming from research, ultimately framing the idea of research protection from 'human subjects research' to **'human harming research**" [43]. In doing so, researchers who might otherwise be inclined to believe that no human is directly involved in the research study would be compelled to address the ethical implications of any harm to broader populations outside the immediate research project."[44]. This is the approach adopted in PaCE, relying on the framework of the ELSI analysis to identify potential human harms.

Contextual integrity accordingly becomes a benchmark theory of privacy, a conceptual framework that links the protection of personal information to the norms of personal information flow within specific contexts. This theory is relevant to the present ELSI analysis as it moves beyond a simple public-private dichotomy and offers a more nuanced perspective on privacy as it pertains to ethics, consent and harm. The theory of contextual integrity links privacy to specific contexts by providing a framework to evaluate the flow of information and help identify and explain why certain information flows are acceptable in one context and problematic in another[45]. Contextual integrity can be linked to the sensitive approach advocated by Ravn, Barnbell and Barbosa Neves wherein individual privacy remains the central concern[46].

---

[41] Ravn, Signe, Barnwell Ashley, & Barbosa Neves Barbara. "What is "Publicly Available Data"? Exploring Blurred Public-Private Boundaries and Ethical Practices Through a Case Study on Instagram", *Journal of Empirical Research on Human Research Ethics*, 2019

[42] Zimmer, Michael. "Addressing Conceptual Gaps in Big Data research Ethics: An Application of Contextual Integrity", *Social Media + Society,* Vol. April-June 2018, p. 2. https://doi.org/10.1177/205630511876830

[43] Zimmer, Michael. "Addressing Conceptual Gaps in Big Data research Ethics: An Application of Contextual Integrity", *Social Media + Society,* Vol. April-June 2018, p. 4. https://doi.org/10.1177/205630511876830

[44] Zimmer, Michael. "Addressing Conceptual Gaps in Big Data research Ethics: An Application of Contextual Integrity", *Social Media + Society,* Vol. April-June 2018, p. 6. https://doi.org/10.1177/205630511876830

[45] Zimmer, Michael. "Addressing Conceptual Gaps in Big Data research Ethics: An Application of Contextual Integrity", *Social Media + Society,* Vol. April-June 2018, p. 6. https://doi.org/10.1177/205630511876830

[46] Ravn, Signe, Barnwell Ashley, & Barbosa Neves Barbara. "What is "Publicly Available Data"? Exploring Blurred Public-Private Boundaries and Ethical Practices Through a Case Study on Instagram", *Journal of Empirical Research on Human Research Ethics*, 2019

Contextual integrity can also be likened to the 'situational ethics' principle adopted by most guidelines in that "each research situation is unique and it is not enough – or possible – to apply a standard template in order to guarantee ethical practice"[47]. The AoIR guidelines, for example, state that researchers must balance the rights of the subjects – in this case the people whose data is extracted – as people with the social benefits of researchers and the right of researchers to conduct research[48].

4.3 Intellectual property

As social media environments have evolved, so too have intellectual property and data protection laws, accordingly provoking difficult questions about the terms of access to platforms and their responsibility to the creators of information on those platforms[49]. In clarifying the legal landscape surrounding web-scraping, legal experts Snell and Menaldo list a number of issues that should be considered both by website owners and those seeking to perform analytics based on data gathered from websites. These include[50]:

> "a) the language of the terms of use or service, and whether such terms address access to the website through automated means, use of any data collected through such means and use of the website for other than the user's personal, non-commercial use;
> b) the enforceability of the terms of use, for example, whether they are presented to the user through a clickwrap mechanism that requires the user to indicate his or her assent to those terms as opposed to a browsewrap agreement, or on a terms of use page that can be reached through a conspicuous link on every other page on the website and which indicates that any use of the website is subject to the user's agreement to those terms;
> c) use of technological tools to deter unwanted crawling or scraping or to specify crawl rates, including but not limited to the robots.txt protocol;
> d) whether access to the website is protected...;
> e) whether data on the website content is protected by copyright; and
> f) whether the website owner will license or authorize uses of content".

While the above standpoint is largely US-centric, the issues raised by Snell and Menaldo nevertheless serve as a reminder that the legality of web scraping is heavily context-specific and need to be explored on a case-by-case basis, much along the lines of situational ethics noted above.

In this context, Krotov and Silva have identified the legal issue of copyright infringement: the scraping and republishing of data or information that is owned and explicitly copyrighted by a

---

[47] Williams, Matthew L, Burnap Pete and Sloan Luke. "Towards an Ethical Framework for Publishing Twitter Data in Social Research: Taking into Account Users' Views, Online Context, and Algorithmic Estimation", Vol. 51, No. 6, 2017, p. 1152.
[48] Markham, Annette and Buchanan, Elisabeth. "Ethical Decision-Making and Internet Research", *Association of Internet Researchers,* 2012, p. 4. https://aoir.org/reports/ethics2.pdf
[49] Hutchinson, Jonathan, Martin Fiona, and Sinpeg Aim. "Chasing Isis: Network Power, Distributed Ethics, and Responsible Social Media Research", In Zimmer, Michael and Kinder-Kurlanda, Katharina (eds.). *Internet Research Ethics for the Social Age: New Challenges, Cases, and Contexts.* New York, Peter Lang, 2017, p. 57
[50] Snell, James and Menaldo, Nicola. "Web Scraping in an Era of Big Data 2.0", *Bloomberg Law,* June, 2016. https://www.bna.com/web-scraping-era-n57982073780/

website owner can lead to 'copyright infringement'[51]. It is important to note that while different countries have different copyright regulations, Article 15 of the EU directive on copyright in the Digital Single Market states that "the rights provided... shall not apply in respect of the use of individual words or very short extracts of a press publication"[52]. Moreover, the protection granted to press publications under this directive does not apply to websites, such as blogs. This does not necessarily mean that a website owns the data generated by its users. As a case in point, Krotov and Silva explain that a website devoted to product reviews does not necessarily own the reviews left by the website users[53]. Moreover, ideas cannot be copyrighted – only the specific form or representation of those ideas is covered by copyright. This means that one can use copyrighted data to create summaries of that data, for example. The use of copyrighted material nonetheless remains subject to the copyright laws, such as the EU copyright directive.

The question of who owns the data posted on a digital platform continues to be another ongoing debate from a legal standpoint. Puschmann contends that in many contexts the initial answer is no one: "while suggestions have been made that users have a natural right to the data they produce and the metadata that surrounds it, such data are generally not considered to constitute (intellectual) property. Laws protecting the privacy of users apply to social media platforms, but the fact that most information is disclosed willingly...and that providers are granted the right to analyse the data and experiment with the site's features when users sign the terms of service means that companies are under very few constraints to make use of the data."[54]

In conducting their own literature review, Krotov and Silva find that, in the legal field, a website owner can effectively prevent access to a website by explicitly prohibiting this in the terms of use policy listed on the website. Failure to comply with these terms can in turn lead to a "breach of contract" on the part of a website's user: "in order to prosecute someone for violating the 'terms of use', the website user needs to enter an explicit agreement with the website owner to comply with the 'terms of use' policy (e.g. by clicking on a checkbox). Thus, simply prohibiting Web Crawling and Web Scraping on the website may not preclude someone from crawling the website from a legal standpoint"[55].

---

[51] Krotov, Vlad and Leiser, Silva. "Legality and Ethics of Web Scraping".*Proceedings of the Twenty-fourth Americas Conference on Information Systems*), New Orleans, September 2018.
[52] European Parliament and The Council. Directive 2019/790 of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0790&from=EN
[53] Krotov, Vlad and Leiser, Silva. "Legality and Ethics of Web Scraping".*Proceedings of the Twenty-fourth Americas Conference on Information Systems*), New Orleans, September 2018.
[54] Puschmann, Cornelius. "Bad Judgement, Bad Ethics: Validity in Computational Social Media Research", In Zimmer, Michael and Kinder-Kurlanda, Katharina (eds). *Internet Research Ethics for the Social Age: New Challenges, Cases, and Contexts.* New York, Peter Lang, 2017, p. 109
[55] Krotov, Vlad and Leiser, Silva. "Legality and Ethics of Web Scraping".*Proceedings of the Twenty-fourth Americas Conference on Information Systems*), New Orleans, September 2018.

4.4 Surveillance and related individual and societal impacts

Surveillance is defined as the "close watch kept over someone or something"[56]. While surveillance tools have existed even before modern technology, they take some specific forms in the modern era, becoming routine and systematic. The panopticon is arguably the most well-known metaphor of surveillance. Michel Foucault describes the prisoner of a panopticon as being at the receiving end of asymmetrical surveillance: "He is seen, but he does not see; he is an object of information, never a subject in communication."[57] The inmate polices himself for fear of punishment.

Surveillance is used for many different projects, such as policing, deterrence consumption, entertainment, taxation, health promotion, education, governance, accountability, child-rearing and military conquest. Moreover, a system or technological tool can result in surveillance even though it was not initially designed to achieve such an objective: "Uses are not necessarily established in advance, but are emergent, resulting from the creative insights of individuals who envision novel possibilities for systems developed for entirely different purposes. Due to the proliferation of surveillance, it is increasingly difficult to suggest a single coherent purpose, such as social control".[58]

In Foucault's example, the many are seen by the few, describing the notice of surveillance. The goal is to enact social control over the many in the most invisible manner possible. By controlling and potentially silencing dissident voices, the few can exacerbate their powers. The business model of profiling and personalisation adopted by social media platforms can be considered a case in point. The digital traces that users leave behind are being used to further an industry of personalisation – social media platforms have long claimed that being able to track what people see and do on the internet provides them with a competitive advantage. At the same time, however, there is little doubt that "what Amazon knows about the literary preferences of people around the world goes far beyond what it needs to know in order to sell more books"[59]. Zuboff refers to this model as "surveillance capitalism" or the commodification of personal data often without the explicit consent of social media users[60]. Combining state surveillance together with its capitalist counterpart means that "digital technology is separating the citizens in all societies into two groups: the 'watchers' (invisible, unknown, and unaccountable) and the 'watched'"[61]. This in turn confers disproportionate power to those who hold the surveillance technology. It is further well evidenced that the impacts and harms that arise from surveillance are unevenly distributed across the population and tend to disproportionately effect those who are already subject to other forms of social discrimination (e.g., the poor, immigrants, racial minorities).[62]

---

[56] Merriam-Webster Dictionary. "Surveillance" https://www.merriam-webster.com/dictionary/surveillance
[57] Foucault, Michael. *Surveiller et Punir: Naissance de la Prison.* Gallimard, Paris, 1975, p. 200-201.
[58] Haggarty, Kevin D. "Tear down the walls: on demolishing the panopticon", In Lyon, David (ed.), *Theorizing Surveillance: The panopticon and beyond,* New York, Routledge, 2011, p. 27
[59] Puschmann, Cornelius. "Bad Judgement, Bad Ethics: Validity in Computational Social Media Research", In Zimmer, Michael and Kinder-Kurlanda, Katharina (eds). *Internet Research Ethics for the Social Age: New Challenges, Cases, and Contexts.* New York, Peter Lang, 2017, p. 101
[60] Zuboff, Shoshana.*The Age of Surveillance Capitalism.,*New York, Public Affairs, 2019.
[61] Naughton, John. "The goal is to automate us: welcome to the age of surveillance capitalism", *The Guardian*, 20 January 2019, https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook
[62] Eubanks, Virginia. *Automating Inequality: how high tech tools, profile, police and punish the poor.* St Martins Press, 2018; Browne, Simone, *Dark Matters: On the Surveillance of Blackness*, Duke University Presss 2015. .

It is well established that surveillance impinges on privacy[63]. In this context, surveillance also includes non-obtrusive observation of online communities, otherwise described as 'lurking'. According to Grincheva, lurking presupposes an invisible presence on a site[64]. While lurking allows researchers to collect data without influencing participants' behaviour, some scholars contend that this puts the researcher in a questionable position to gaze on others.

Data mining, scraping, and crawling can be considered to be forms of non-intrusive lurking and are categorised as "covert surveillance" by Wright and Raab as they are invisible to users[65]. Wright and Raab highlight that surveillance not only reduces privacy but also affects the opportunities, chances, and life styles of individuals, and, in so doing, has a direct impact on the very nature of society in terms of discrimination and exclusion. Given that surveillance systems can have such a deleterious impact on society, they suggest that assessors ask: "Who authorised the system (e.g., Parliament) and how was it authorised? Has the system been the subject of public scrutiny (if not consensus)?...**does the project, technology, application or service sort individuals into groups according to some predetermined profile that may advantage some groups and disadvantage others?** Does the surveillance in question have a negative impact on social cohesion?"[66]. The following sub-section addresses the question of ICTs and social harm from lurking in greater detail.

4.5 Individual and social harm

In outlining the main arguments around social harm, Zimmer and Kinder-Kurlanda explore how "harm" is possible to someone in online communities[67]. Drawing upon the Kantian idea of respect for the dignity of the person, Marx argues that "when the self can be technologically invaded without permission and even often without the knowledge of the person, dignity and liberty are diminished. Respect for the individual involves not causing harm, treating persons fairly through the use of universally applied valid measures, offering meaningful choices, and avoiding manipulation and coercion"[68].

As noted in the preceding sub-section, internet research that involves scraping or crawling can have broader implications for the nature of society itself, such as by enhancing the power of some groups to the detriment of others. Women and people of colour, for example, are systematically more prone to online harassment and abuse. Hoffman and Jonas assert that in view of the greater burden shouldered by these groups in participating online, it is the duty of researchers to avoid

[63] Solove, Daniel. *Understanding Privacy,* Cambridge MA, Harvard University Press, 2008, p. 1
[64] Grincheva, Natalia. "Museum Ethnography in the Digital Age: Ethical Considerations", In Zimmer, Michael and Kinder-Kurlanda, Katharina (eds). *Internet Research Ethics for the Social Age: New Challenges, Cases, and Contexts.* New York, Peter Lang, 2017, p. 190
[65] Wright, David and Raab, Charles D. "Constructing a surveillance impact assessment". *Computer Law and Security Review.* Vol. 28, Issue 6, December 2012, p. 616. https://doi.org/10.1016/j.clsr.2012.09.003
[66] Wright, David and Raab, Charles D. "Constructing a surveillance impact assessment", *Computer Law and Security Review.* Vol. 28, Issue 6, December 2012, p. 618. https://doi.org/10.1016/j.clsr.2012.09.003
[67] Zimmer, Michael and Kinder-Kurlanda, Katharina (eds.). *Internet Research Ethics for the Social Age: New Challenges, Cases, and Contexts.* Peter Lang, New York, 2017, p. xx.
[68] Marx, Gary T. "Ethics for the New Surveillance", *The Information Society*, Vol. 1, No. 3, 1998, p. 172

replicating or compounding existing injustices and to foreground the needs and the safety of vulnerable users and the conditions that lead to their vulnerability in the first place[69].

Surveillance has impacts both when it is covert (exposure to greater risk of some subsequent harm, reducing agency and self-determination, facilitating discrimination), but also when it becomes overt (individuals realise they are under surveillance, experience their own visibility). Surveillance, including lurking, can have harmful psychological impacts by creating embarrassment, shame, stigmatisation, or otherwise putting a person in a negative light[70]. This is partly to do with the affordances and features of the internet and online platforms that magnify the harms and injustices that some users face by making tweets or posts go viral and triggering an onslaught of harassment that is hard to escape and even harder to erase[71].

In attempting to counter the concerns raised against social media platforms, legal scholar and journalist Jeong, cited in Hoffman and Jones, finds that too much attention is paid to the *content* posted on these platforms as opposed to patterns of *behaviour* that might require greater attention[72]. Moreover, platforms exacerbate this problem by relying on users to report one another, thus shifting the onus on individuals policing one another without recognising their differences in power and experience of harm.

Several scholars have also raised concerns of bias in big data itself. Crawford points out that hidden biases in both the collection and analysis of data present considerable risks and are as important to the big-data equation as the numbers themselves[73]. She refers to the Twitter data generated during Hurricane Sandy as a case in point. Drawing upon a study that combined Hurricane Sandy-related Twitter and Foursquare data, Crawford notes that the study produced several expected findings in terms of grocery shopping peaks before the storm as well as some surprising ones, such as nightlife picking up day after the storm, arguably due to cabin-fever. What she calls attention to, however, is the fact that the data did not represent the whole picture as the largest number of tweets came from Manhattan which was not the hub of the disaster but appeared to be so given the high level of smartphone ownership and Twitter use in the city. In contrast, very few tweets emerged from the more severely affected locations, such as Coney Island, but extended blackouts and limited cellular access meant that fewer tweets emerged from the worst hit areas. This can be thought of as a "signal problem" – data are assumed to accurately reflect the social world, but there are significant gaps, with little or no signal from particular communities[74].

---

[69] Hoffman, Anna Lauren and Jonas Anne. "Recasting Justice for Internet and Online Industry Research Ethics", In Zimmer, Michael and Kinder-Kurlanda, Katharina (eds). *Internet Research Ethics for the Social Age: New Challenges, Cases, and Contexts.* New York, Peter Lang, 2017, p. 3

[70] Wright, David and Raab, Charles D. "Constructing a surveillance impact assessment", *Computer Law and Security Review.* Vol. 28, Issue 6, December 2012, p. 620. https://doi.org/10.1016/j.clsr.2012.09.003

[71] Hoffman, Anna Lauren and Jonas Anne. "Recasting Justice for Internet and Online Industry Research Ethics", In Zimmer, Michael and Kinder-Kurlanda, Katharina (eds). *Internet Research Ethics for the Social Age: New Challenges, Cases, and Contexts.* New York, Peter Lang, 2017, p. 12

[72] Hoffman, Anna Lauren and Jonas Anne. "Recasting Justice for Internet and Online Industry Research Ethics", In Zimmer, Michael and Kinder-Kurlanda, Katharina (eds). *Internet Research Ethics for the Social Age: New Challenges, Cases, and Contexts.* New York, Peter Lang, 2017, p. 13

[73] Crawford, Kate. "The Hidden Biases in Big Data", *Harvard Business Review,* 1 April 2013, https://hbr.org/2013/04/the-hidden-biases-in-big-data

[74] Ibid

Marx has noted, however, that measuring the concept of harm, whether in the collection or the use of the data, can be made problematic: "Should harm be measured objectively or subjectively, and how should we respond to individual and cultural differences in defining it?"[75] This is why what one might regard as a negative psychological impact – as a harm – depends on the context and one the person deciding whether someone's claim of harm can be regarded as valid or not. Equally, how harmful something may be perceived to be is also context-dependent.[76] The argument that harm is contextual is also reflected in the ethical framework developed by AoIR, which states that a 'one size fits all' approach is unhelpful in assessing harm[77].

In addition to the psychological harm issues it may raise, lurking can also have political impacts, many of which arise from the way surveillance impacts privacy. This point is especially relevant to the development of ICT tools in that tool developers should consider the manner in which lurking could potentially have a chilling effect on freedom of speech and association, and accordingly on democracy. Wright and Raab recommend that in assessing the political impacts of a surveillance system, "one should ask questions such as who is being surveilled by whom and for what purpose? Who has authorised the surveillance? **Will the project or technology enhance the power of some at the expense of others?** Who will have access to the data gathered by a surveillance system and how will such data be used? Will it undermine the electorate's trust in their elected officials? Will the surveillance system support or undermine democracy?"[78].

[75] Marx, Gary T. "Ethics for the New Surveillance", *The Information Society*, Vol. 1, No. 3, 1998, p. 184
[76] Wright, David and Raab, Charles D. "Constructing a surveillance impact assessment", *Computer Law and Security Review*. Vol. 28, Issue 6, December 2012, p. 620. https://doi.org/10.1016/j.clsr.2012.09.003
[77] Markham, Annette and Buchanan, Elisabeth. "Ethical Decision-Making and Internet Research", *Association of Internet Researchers,* 2012, p. 4. https://aoir.org/reports/ethics2.pdf
[78] Wright, David and Raab, Charles D. "Constructing a surveillance impact assessment", *Computer Law and Security Review*. Vol. 28, Issue 6, December 2012, p. 619. https://doi.org/10.1016/j.clsr.2012.09.003

5.0 ELSI assessment of PaCE tools

Following the literature review on the current debates around ICT tools development, especially their potential ethical, social and legal impacts, Section 5 provides an overview of potential social, ethical, and legal risks the PaCE consortium foresee in developing its ICT tools and the manner in which these are addressed and mitigated.

As part of the Horizon 2020, part of the EU Research and Innovation programme, the PaCE research project aims to:

> *combat the negative tendencies, to build upon the lessons of positive examples, and hence play a part in constructing a firmer democratic and institutional foundation for the citizens of Europe. PaCE will analyse, in detail, the type, growth and consequences of such movements in terms of their particular characteristics and context. From this, it will analyse the causes of these movements and their specific challenges to liberal democracy across Europe. In particular, it will focus on transitions in these movements (especially changes in leadership) and how they relate to the liberal reaction to them. PaCE will propose policy-oriented responses to these challenges, developing risk-analyses for each kind of response, each kind of movement and the type of transition. Throughout the project, it will engage with citizens and policy actors, especially groups under-represented in public affairs, face-to-face and via new forms of democratic participation appropriate to our digital age. It will develop new tools for identifying populist narratives and for democratic consultation. This activity will result in result in specific interventions aimed at three audiences: the public, politicians and educators.*

In this context and under Work Package 3, the aim of the ICT tools developed in PaCE is to produce "*a publicly available tool (algorithm or application software) allowing policy actors and citizens to identify populist narratives and counter-narratives in the media and allowing policy actors and citizens to assess their individual exposure to public populist narratives and policy actors and citizens to adequately react to populist public narrative.*"[79]

For the development of ICT tools, the PaCE consortium has considered the legal grounds as outlined in the GDPR. While we do not specifically dedicate a section to the GDPR Data Privacy Impact Assessment (DPIA), we have ensured that DPIA considerations have been referred to throughout the description of ICT tools and the discussion section of this report. In keeping with the principle of Responsible Research and Innovation (RRI), we have attempted to rethink research and innovation governance with a view to ensuring that processes as well as outcomes of research and innovation are acceptable, desirable and sustainable.

5.1 Affected individuals and organisations

On the one hand, the individuals affected by the developed ICT tools, such as the users of those tools or consortium partners, might be conscious of potential risks and mitigation strategies. On the other hand, affected individuals, such as individuals whose data is being scraped, might not be

[79] According to PaCE Grant Agreement.

aware of the process. We envisage the following individuals to be potentially affected by the ICT tools developed in the PaCE project:

- Users of the ICT tools;
- Third party persons, such as other researchers;
- People whose data is extracted by the tools;
- The PaCE consortium; and

- European Commission as a funder of the project.

5.2 Data Protection and GDPR

As previously stated, the ICT tools developed as part of the PaCE project will use data collected from Common Crawl and Twitter, depending on whether permission is granted by the latter. With regards to the terms of use, both Common Crawl and Twitter permit the use of crawling if carried out in accordance with the restrictions of the robots.txt file, with Twitter expressly prohibiting any type of scraping without prior permission from the Service[80]. Although Common Crawl only aggregates publicly accessible data, it might still include **personal data** which can entail an infringement of individual privacy rights. Under the GDPR framework, publicly available data may contain personal data. The GDPR lists the forms of the protections for individual privacy as well as all the responsibilities of the data controller. Relying on a simple understanding of publicly available data is therefore not sufficient for the processing of data to be legal. Under the GDPR rules, the processing of personal data is permitted, provided that certain requirements are met. These are outlined in the sub-section below.

Purpose for data processing: legitimate interest

The objective of the PaCE ICT tools is to identify populist (and related) narratives in order to gain an overview that may be as comprehensive and precise as possible on these discourses as they are expressed by the general public online. PaCE ICT tools aim to allow researchers, decision-makers, media representatives and the general public to gain an overview of these narratives and the grievances voiced by the general public they express. PaCE ICT tools exclude discourses from government representatives and party leaders.

PaCE is a research project conducted in the public interest, i.e. that of understanding and responding to populist movements in Europe. Hence, Article 6(e) of the GDPR, i.e., "processing is necessary for the performance of a task carried out in the public interest" applies. This public interest resides in the research objectives of PaCE to further social knowledge about the world of politics, the objective of EU-funded research to create and disseminate socially valuable knowledge, and the contractual commitments of the partners to disseminate PaCE's research findings.

[80] Common Crawl. "Terms of Use". https://commoncrawl.org/terms-of-use/; Twitter. "Twitter Terms of Service". Last modified May 25, 2018. https://twitter.com/en/tos#intlTerms

We recognise that a limit is put to this public interest basis, as made explicit in the GDPR, i.e. "where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child." (Art 6(f)). PaCE ICT tools will have to be designed in such a way as to protect "the interests or fundamental rights and freedoms of the data subject". To do so, it has, in particular, been decided not to publish individual narratives that could have made narratives traceable back to their original author.

Furthermore, the personal data that may be processed as part of the narrative analysis work might entail what the GDPR identifies as "special categories of data" (Art. 9), i.e., "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"[81]. As indicated in the GDPR, the processing of this category of data is prohibited except in certain conditions, including two particular exceptions that apply to the PaCE project:

- 2(e) "processing relates to personal data which are manifestly made public by the data subject";
- 2(j) "processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject."[82]

Article 89 of the GDPR allows member states to diverge from the general rights of the data subject under Regulation ("derogations) if personal data or special category of personal data is being processed for scientific or research purposes[83]. These derogations apply in relation to the following rights:

- the right of access (Article 15) - giving the data subject rights to access the data processed
- the right of rectification (Article 16) - giving the data subject rights to correct errors in the data
- the right to restrict processing (Article 18) - giving the data subject rights to request that processing be restricted to particular purposes and uses; and
- the right to object to processing (Article 21) - giving the data subject the right to object to the processing occurring at all.

[81] European Parliament and The Council. Regulation 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://data.europa.eu/eli/reg/2016/679/2016-05-04
[82] European Parliament and The Council. Regulation 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://data.europa.eu/eli/reg/2016/679/2016-05-04
[83] There appear to be such derogations in the relevant implementing legislation in partner countries: Austria, Belgium, Bulgaria, Germany, Ireland, and the United Kingdom.

A requirement for these derogations is often that they apply when allowing these rights would impair or prevent the research activity in question – for example, if allowing data subjects in a statistical study to "correct" the data would change the validity of the research. When these rights can be facilitated within a given research design, they should be.

As a general rule, a data controller is under the obligation to provide a data subject with information about the processing, including when data has not been obtained from the data subject. This is clearly a challenge for any form of large-scale web-scraping, where the identifiers or contact details of the data subjects are unknown, as it is the case in the PaCE project. Article 5(b) of the GDPR provides an exemption for when "the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, **scientific or historical research purposes or statistical purposes**, subject to the conditions and safeguards referred to in Article 89(1)"[84].

These safeguards include:

- ensuring that technical and organisational measures are in place, in particular to ensure respect for the principle of data minimisation,
- Measures such as pseudonymisation provided that the original purpose of data collection can be fulfilled in that manner; and
- Where those purposes can be fulfilled by further processing which does not permit, or no longer permits, the identification of data subjects, those purposes shall be fulfilled in that manner.

The PaCE research consortium puts in place several safeguards, or **mitigation strategies,** through the design of the ICT tools to omit the use of personal information and protect the privacy of individuals. In particular, the dataset used for the ICT tools development omits the following:

- Information that is not publicly accessible;
- Facebook content;
- Pictures and videos;
- Contact information of individuals, such as names, email addresses, phone numbers.

Once the dataset has been processed by the data collectors and the mentioned personal information has been omitted through the use of keywords and filters, the data will be aggregated to ensure that no particular narratives can be traced back to an individual author. Results will then be published on the public website. The objectives of the publication of the results of this study on the public website are threefold:

- To raise awareness on the part of the general public, policy-makers, as well as decision-makers of the existence, nature, and quantity of identified narratives around public grievances discussed publicly online and how these evolve;

[84] European Parliament and The Council. Regulation 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://data.europa.eu/eli/reg/2016/679/2016-05-04

- For the public to reflect on what is considered to be a populist narrative and other related narratives; and
- To highlight the potential legitimacy of grievances these narratives reveal without stigmatizing those who proffer them
- To give access to the data to other researchers on populism and beyond.

The PaCE consortium arrived at the understanding that even if personal data is excluded from the scraped data, the risk of individual privacy infringement would remain should individual narratives be republished. Indeed, even if pseudonymised, the author of a narrative could be reidentified by searching the narrative online. After several discussions with the ICT developer, it was agreed that individual narratives would not be re-published on the public website. Hence, only types of narratives and aggregated results will be made public. The aggregation of narratives is a technical and organisational measure to ensure the minimisation of personal data. The main principle underlying this exercise is the protection of individuals as a key principle, as advocated by Ravn, Barnbell and Barbosa Neves[85].

5.3 Intellectual property

As noted in sub-section 4.3, the question of who owns the data posted on a digital platform continues to be another ongoing debate. While users can prohibit the access to the website through the terms of use policy, it does not prevent the scraping activities from a legal standpoint.

Twitter and Common Crawl Services explicitly state that the content generated on their sites is the sole responsibility of the person or entity from whom the consent originated. The Services also carry a separate clause for copyright infringement by asking users to report any content that they believe constitutes a copyright or intellectual property infringement.

To ensure the PaCE research project complies with intellectual property and copyright law, the PaCE consortium has decided in accordance with a 'situational ethics' principle to not publish individual narratives, thereby eliminating as such the possibility to link these narratives to their original sources.

In this regard, the intellectual property and copyrights have been adhered to for the development of the PaCE ICT tools.

5.4 Ethical and social considerations

The ELSI analysis this deliverable reports on has explored potential risks PaCE ICT tools might lead to for individuals as well as potential risks to specific groups and society as a whole. This sub-section highlights both categories of potential risks and discuss mitigation strategies.

[85] Ravn, Signe, Barnwell Ashley, & Barbosa Neves Barbara. "What is "Publicly Available Data"? Exploring Blurred Public-Private Boundaries and Ethical Practices Through a Case Study on Instagram", *Journal of Empirical Research on Human Research Ethics*, 2019. https://doi.org/10.1177/1556264619850736

5.4.1 Surveillance

Given that the ICT tools developed by the PaCE project entail an aspect of 'live-listening' , that is scraping the Web for keywords as they are being written and published online, there is a potential to view it as a form of non-obstructive observation that scholarly literature describes as 'lurking'. Not all Web users may be aware of potential lurking activities being carried out and aggregated on a different platform for research purposes in the realm of the PaCE project.

Past strategies to address ethical and privacy concerns related to non-obtrusive lurking have included the omission of personal information, such as names, age, gender, profession, etc[86] – a measure that is currently required under the GDPR. Another potential mitigation strategy is that data collectors engage with principles of consent, privacy, and ownership[87]. While ideally a consent-driven approach would resolve the issue of lurking and covert surveillance, the reality is that requiring consent is not practically feasible considering the massive amount of online data is being crawled. This point is echoed by Salganik[88] in his book in that informed consent is not always logistically practical due to the fact that it is not uncommon for users to publish content under an alias or anonymously, accordingly making it difficult for data collectors to obtain consent from all. Moreover, he adds that people can also change their behaviour when they know they are being observed by researchers. This in turn has the potential to influence the research data and consequently the research findings. It must be noted however that this presents an ethical conundrum for this consortium as not informing users would in theory constitute as lurking – an issue of which this consortium is aware.

Based on these arguments, we suggest the adoption of a more **sensitive approach** argued by Ravn, Barnbell and Barbosa Neves – wherein data is engaged with at the aggregate level and not through the reproduction of posts – and where protecting individuals is a key principle[89]. The PaCE project will make every effort it can practically to be transparent about its activity so that people who actively think they may be data subjects in our research can find out what we are doing. Moreover, we have identified the potential risk that people who hold certain political views or express themselves in a particular – populist – manner may feel particularly surveilled and, hence, further alienated by a project that seeks to analyse their discourses online. It is to avoid this that the consortium has collectively decided to also include liberal narratives in its data scraping and analysis.

---

[86] Grincheva, Natalia. "Museum Ethnography in the Digital Age: Ethical Considerations", In Zimmer, Michael and Kinder-Kurlanda, Katharina (eds). *Internet Research Ethics for the Social Age: New Challenges, Cases, and Contexts.* New York, Peter Lang, 2017, p. 192

[87] Ravn, Signe, Barnwell Ashley, & Barbosa Neves Barbara. "What is "Publicly Available Data"? Exploring Blurred Public-Private Boundaries and Ethical Practices Through a Case Study on Instagram", *Journal of Empirical Research on Human Research Ethics*, 2019. https://doi.org/10.1177/1556264619850736

[88] Salganik, Matthew J.*Bit by Bit: Social Research in the Digital Age*, New Jersey, Princeton University Press, 2018.

[89] Ravn, Signe, Barnwell Ashley, & Barbosa Neves Barbara. "What is "Publicly Available Data"? Exploring Blurred Public-Private Boundaries and Ethical Practices Through a Case Study on Instagram", *Journal of Empirical Research on Human Research Ethics*, 2019. https://doi.org/10.1177/1556264619850736

In addition to the risk an individual might encounter through the development of the PaCE ICT tools, the consortium also understands the potential risks to specific groups and the society as a whole. The following sub-section of the report will highlight the potential risks and discuss mitigation strategies.

5.4.2 Individual and social harm

The discussions that took place within the consortium around how to approach populist narratives online led to questioning the project's approach to the notion of populism. The PaCE project is grounded upon an understanding of populism as being a threat to liberal democracy and the values and principles held dear in the EU (see for instance Pappas[90]). This theoretical framework and approach to populism emerges from a political science perspective to examine political parties and leaders that are identified as populists. The ELSI analysis we went through as part of Task 6.4 reported in the present document made it clear that we had to adapt this framework for the empirical study of discourses of the general public online that is conducted as part of WP3 of the PaCE project. We came to the conclusion that discourses from the general public should not be approached in the same way as those from politicians. Indeed, these two groups have different responsibilities, positions, and interests that have implications in the way their discourses can and should be examined. The key point is that while a normative approach can be appropriate in the political science field in order to distinguish between a good political system or leader and a problematic one, such an approach falls short when it comes to seeking to better understand the views of the general public. Furthermore, a judgmental approach to the views expressed by the general public might further antagonise members of this public and contribute to their sense of alienation. This is especially problematic considering the fact that individuals who resort to populist rhetoric often feel estranged and silenced in their society[91]. These considerations have been discussed between the authors of this deliverable (DS and TRI), with the partner developing the ICT tools (CF) in several calls held during Task 6.4, and with the whole consortium during a conference call on the ethics of the design of PaCE ICT tools on 4 October 2019. These discussions made it possible to raise our awareness of this issue within PaCE narrative analysis and to orient the discussion in such a way as to take into account this concern within the tools' development.

Polarization and stigmatization

This ELSI analysis has also examined the potential risks of PaCE tools to contribute to deepening polarisation within society. The narrative analysis work of Work Package 3 seeks to explore and better understand online discourses by the general public that resort to populist rhetoric. In addition, the consortium aims to bring people together by showing that many of the grievances voiced online do have a legitimacy.

---

[90] Pappas, Takis S. "Modern Populism: Research Advances, Conceptual and Methodological Pitfalls, and the Minimal Definition", *Politics: Oxford Research Encylopedia,* 2016, doi: 10.1093/acrefore/9780190228637.013.17

[91] Algan, Yann, Beasley Elisabeth, Cohen Daniel, and Foucault Martial. *Les Origines du Populisme: Enquête sur un schisme politique et social.* Paris, Éditions du Seuil et La République des Idées, 2019.

In more detail, the ELSI study highlighted how the PaCE ICT tools could potentially contribute to further exacerbating a social context characterised by polarisation between liberals and populists. Indeed, as shown in the previous PaCE task 6.3 by engaging with various stakeholders through a workshop and interviews and reviewing the literature on populism, we saw that the label populism is often used or perceived to be used as a pejorative term. Giving this label to narratives published online by the public might be seen as an aggressive gesture of 'liberals' against 'populists'. This risk has been intensely discussed as part of T6.4 as it is a key concern of PaCE partners – especially those involved in civic engagement – to avoid such type of alienation of a part of the society. The issue of potentially silencing and treating as illegitimate voices expressed by the public was also a strong concern raised.

In order to mitigate these risks, it was decided that the public website will rather be framed under the language of 'grievances', i.e., a space in which online expressions of grievances are examined. The focus on populist narratives remains; however, they are treated as public expressions of grievances taking the shape of populist rhetoric, i.e., framing the issues they raise by denouncing an elite that would be deceiving the ordinary people. In addition, future consultation with the public website developer (CF) will take place to ensure that the framing and the terminology used is not stigmatising toward people resorting to populist rhetoric.

Keyword and narrative bias

The way we communicate and the words we choose is often times a result of the people we engage with and groups we are part of. Social identity theory claims that the way people see themselves is based on the group they belong to. Henry Tajfel and John Turner explain the self-concept perceived by the individual belonging to a specific group[92]. It is therefore essential to consider the context and language of narratives to avoid a specific bias against certain groups over others.

The PaCE consortium has developed a list of keywords to be used for the Web searching activities and the aggregation of narratives. Since the keyword chosen for the Web searching activities will ultimately lead the selection of narratives, it is essential to consider whether there is an integrated bias in the choice for specific keywords. These keywords are based on the research and categorization developed and tested by the TU Dresden into communication activities by populist movements and its similarities[93]. The PaCE consortium has worked with different partners to be able to include as many languages as possible and adequately portray the nuances of a language. However, the PaCE project is aware that not all languages spoken in the European Union will be included, leading to a bias toward specific language choices, especially English, over others. To raise awareness of this limitation of the study and be explicit about it, including by indicating it on the Website constitutes a mitigation strategy in and of itself.

---

92 Tajfel, Henry. and Turner, John. "An integrative theory of intergroup conflict", In Hatch, Mary Jo and Schultz, Majken (eds.). *Organizational Identity: A Reader*, Oxford, Oxford University Press, 2004, pp. 56-65

93 Wirth, Werner et al. "The appeal of populist ideas, strategies, and styles: A theoretical model and research design for analyzing populist political communication". *NCCR democracy,* Working Paper No. 88, Zurich, 2016, http://pwinfsdw.uzh.ch/publications/workingpaper/pdf/wp88.pdf

Furthermore, the AI training tool that has been developed to identify different types of populist narratives has been trained on a large dataset with the supervision of experienced researchers to limit the number of false-positives and true-negatives and resolve any challenges when scraping the Web for populist narratives. In addition, the keywords used for the Web scraping are publicly available and can be revisited, in case this is needed.

Distorted portrait of reality

Once the narratives have been scraped from the Web, the data collectors will aggregate the narratives to be able to maintain user confidentiality and privacy. In accordance with the experiences of other social science researchers[94], the data collectors will aggregate narratives to ensure that narratives are not traceable by search engines. While the data collectors will take care to ensure that the meaning of those narratives is not obscured, the grouping entails potential medium risks for a distorted aggregation of narratives, especially considering different languages. The likelihood of harm is in this case possible since it entails a potential to portray a distorted reality that might be used to base research or policy decisions upon. We have not come across a suggestion in the literature, such as in Zimmer and Kinder-Kurlanda[95], on how to mitigate these types of risks to social harm. One suggested mitigation is to state clearly that the suggested narratives are a part of the discussion and only reflect the views shared online.

Another potential risk factor is that especially the voices and opinions of under-represented groups are not being adequately represented on the Internet. This might include people of a certain age group or in a certain geographical location with lower access rates to the Internet. By searching the Web and collecting narratives, the PaCE consortium risks amplifying the voices of some groups over others to the target audience of policy- and decision-makers, researchers, and the general public. The PaCE consortium is aware of this risk and its implication for the research. To reduce this risk, it will be made clear the ICT tools research findings are as the findings of the online discussion only, not the general public discourse as a whole.

[94] Zimmer, Michael and Kinder-Kurlanda, Katharina (eds.). *Internet Research Ethics for the Social Age: New Challenges, Cases, and Contexts.* Peter Lang, New York, 2017.
[95] Ibid

6.0 Conclusion and recommendations

Based on the above discussion, we propose below a list of recommendations that can guide the development of PaCE tools as well as similar ICT tools designed by other consortia or organisations.

1. **Ensure that the purposes and objectives of the development of ICT tools are clear** with all parties involved, beyond the limited sense of the formal task description and grant agreement commitments. This will help to guide design and development decisions further down the line. Having clear purposes is necessary on data protection grounds. Clarifying the objectives should include making a clear argument about the causal pathway to social benefits – how will what the project is developing contribute to society? What will users be able to do with the tool? The consortium has discussed this in the context of the PaCE project and the anticipated benefits include:
    a. Policy-makers will be exposed to voices and opinions of the public in a quantified and clustered way which supports decision-making. They will be able to better see how narratives are spread and distributed and how they ebb and flow over time. As such, they will be able to better understand the concerns of the public amongst informational noise. In particular, information on trends is useful decision-making information.
    b. The public will have their perspectives collated and presented to policy-makers through an additional channel.
    c. Researchers and academics will gain access to a structured source of information on the general public's populist narratives that can be exploited within the PaCE project and in other research activities, as yet unknown to the PaCE consortium.

2. Further work should be included in Task 6.4 ELSI of public engagement to **support the responsible development of the public facing component of the web-application**. The public facing part of this app will be an important part of how PaCE interfaces with the public, and how the tool is framed, communicated and supported, as well as what users will be able to do with the two are important parts of creating an ethical application.

3. **The limitations, gaps and (justified) assumptions of the tool should be documented** – Whilst the project is making every endeavour to create an accurate and scientifically justified tool, every measurement project, and every AI project includes assumptions, and methodological limitations. The better we as a consortium understand these, the better we will be able to communicate what the tool can actually do. A risk with such applications is that the view they provide on reality is taken for reality. A user should be able to understand the potential blind spots in the tool they are using and to be aware of the various assumptions within which the data and results have been produced. We should design the tool to support the broadest possible sense of algorithmic transparency.

a. This documentation should inform the dissemination and communication activity conducted in WP 5. All partners in the consortium should be familiar with this and should not over-promise or make unjustified claims for the tool's capabilities.

4. Alternative ways of clustering, collating and describing the collective narratives must be explored. This specific **Web tool for PaCE will not republish individual statements by users**, as the potential privacy and data protection and ethical risks are too high given the context, in particular the risks to data subjects from labelling their speech as populist. Context and risk assessment are very important from a data protection and privacy perspective, and in this particular context it would be inappropriate for this project to republish individual statements in a verbatim manner (whilst it might be appropriate in other research contexts). This has been agreed by the consortium. The web tool should be accompanied by an **accurate and detailed explanation of the data processing** being conducted by the project. Whilst we cannot possibly reach all data subjects, even with disproportionate effort, we should make a clear effort to do so on the web tool and on the project website (if separate). This information should include all the information required under Article 14 of the GDPR[96]:
    a. the identity and the contact details of the controller and, where applicable, of the controller's representative;
    b. the contact details of the data protection officer, where applicable;
    c. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
    d. the categories of personal data concerned;
    e. the recipients or categories of recipients of the personal data, if any;
    f. where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available;
    g. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
    h. where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
    i. the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;
    j. where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the

[96] European Parliament and The Council. Regulation 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://data.europa.eu/eli/reg/2016/679/2016-05-04

lawfulness of processing based on consent before its withdrawal; *(Our processing is not based upon consent).*

k. the right to lodge a complaint with a supervisory authority;
l. from which source the personal data originate, and if applicable, whether it came from publicly accessible sources *(description of Common Crawl);*
m. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

5. The consortium should **plan for how it will respond to a data subject access request** (Article 15 GDPR), or request for erasure or restriction of processing. Processing for research and statistical purposes may mean we do not have to erase data or restrict processing, but we should consider how we will best communicate this to data subjects.

6. Tool development should **pay attention to common application security risks**[97] and security measures, as good application security supports both user and data subject privacy. Particular attention should be paid to the circumstances in which our data minimisation or anonymisation/clustering could be subverted or removed.

[97] Owasp. Owasp Top 10 - 2017: The Ten Most Critical Web Application Security Risks, https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

7.0 Guidance documents

The following list compiles documents that may provide guidance to conduct a similar ELSI process as the one conducted for PaCE ICT tools. Please note that this is not an exhaustive list. The reference list (section 8 of the present document) may also be consulted for additional guiding documents.

European Union and European Commission:

- EU High-Level Expert Group on Artificial Intelligence, 2019,"Ethics Guidance for Trustworthy Artificial Intelligence (AI)", https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top
- European Commission, Feb 2019, "Horizon 2020 Programme. Guidance How to complete your ethics self-assessment", https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf
- European Union Agency for Network and Information Security, Dec 2015, Privacy by design and in big data. An overview of privacy enhancing technologies in the era of big data analytics, https://arxiv.org/pdf/1512.06000.pdf

National Data Commission Offices:

- Information Commissioner's Office (ICO), 2018, "Sample DPIA Template", https://gdpr.eu/wp-content/uploads/2019/03/dpia-template-v1.pdf
- Daten Ethik Kommission, 2019, "Opinion of the Data Ethics Commission. Executive Summary", https://datenethikkommission.de/wp-content/uploads/191023_DEK_Kurzfassung_en_bf.pdf

Ethical guidelines:

- Association of Internet Researchers (AoIR), 2012, "Ethical Decision-Making and Internet Research. Recommendations from the AoIR Ethics Working Committee (Version 2.0"), https://aoir.org/reports/ethics2.pdf.
- Association of Internet Researchers (AoIR), 2002, "Ethical decision-making and Internet research. Recommendations from the AoIR ethics working committee", https://aoir.org/reports/ethics.pdf
- Don Gotterbarn, Keith Miller, and Simon Rogerson, 1997, Software engineering code of ethics. *Commun. ACM* 40, 11, 110-118, https://ethics.acm.org/code-of-ethics/software-engineering-code/

Relevant academic literature (non-exhaustive):

- Jobin et al, "The global landscape of AI ethics guidelines", *Nature Machine Intelligence,* 1, 2019, pp. 389-399, https://www.nature.com/articles/s42256-019-0088-2
- Ravn, S. et al., "What is "Publicly Available Data"? Exploring Blurred Public-Private Boundaries and Ethical Practices Through a Case Study on Instagram", *Journal of Empirical Research on Human Research Ethics*, 2019. https://doi.org/10.1177/1556264619850736

- Sugiura, l. et al., "Ethical Challenges in Online Research: Public/Private Perceptions." *Research Ethics,* Vol. 13, No. 3–4, July 2017, pp. 184–199. doi:10.1177/1747016116650720.
- Zimmer, M., "Addressing Conceptual Gaps in Big Data research Ethics: An Application of Contextual Integrity", *Social Media + Society,* Vol. April-June 2018, pp. 1-11. https://doi.org/10.1177/2056305118768300

8.0 Reference List

Algan, Yann, Beasley Elisabeth, Cohen Daniel, and Foucault Martial. *Les Origines du Populisme: Enquête sur un schisme politique et social.* Paris, Éditions du Seuil et La République des Idées, 2019.

ALLEA. "European Code of Conduct for Research Integrity", March 2017. https://allea.org/code-of-conduct/

Amazon. "Amazon S3". https://aws.amazon.com/s3/

Boyd, Danah. "Facebook's Privacy Trainwreck. Exposure, Invasion and Social Convergence", *Convergence: The International Journal of Research into New Media Technologies.* Vol. 14, No. 1, 2008, pp. 13-20. doi: 10.1177/1354856507084416

Boyd, Danah and Crawford, Kate. "Critical Questions for Big Data", *Information, Communication, & Society,* Vol. 15, No. 5, 2012, pp.662-679.

Browne, Simone. *Dark Matters: On the Surveillance of Blackness*, U.S.A, Duke University Press 2015.

Common Crawl. http://commoncrawl.org/the-data/

Eubanks, Virginia. *Automating Inequality: how high tech tools, profile, police and punish the poor, New York,* St Martins Press, 2018.

European Parliament and The Council. Regulation 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://data.europa.eu/eli/reg/2016/679/2016-05-04

European Parliament and The Council. Directive 2019/790 of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0790&from=EN

European Union Agency for Network and Information Security. "Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics." December 2015. https://arxiv.org/pdf/1512.06000.pdf

Ferguson, Robert Douglas. "Negotiating Consent, Compensation, and Privacy in Internet Research", In Zimmer, Michael and Kinder-Kurlanda, Katharina (eds). *Internet Research Ethics for the Social Age: New Challenges, Cases, and Contexts.* New York, Peter Lang, 2017, pp. 269-275.

Foucault, Michael. *Surveiller et Punir: Naissance de la Prison.* Gallimard, Paris, 1975.

Grincheva, Natalia. "Museum Ethnography in the Digital Age: Ethical Considerations", In Zimmer, Michael and Kinder-Kurlanda, Katharina (eds). *Internet Research Ethics for the Social Age: New Challenges, Cases, and Contexts.* New York, Peter Lang, 2017, pp. 187-194.

Goddard, Michelle. "The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact", *International Journal of Market Research*, Vol. 59. No. 6, November 2017, pp. 703–705. https://doi.org/10.2501/IJMR-2017-050

Haggarty, Kevin D. "Tear down the walls: on demolishing the panopticon", In Lyon, David (ed.), *Theorizing Surveillance: The panopticon and beyond,* New York, Routledge, 2011. pp. 23-45

Hawkins, Kirk. "Don't try to silence populists - listen to them", *The Guardian*, 9 March 2019. https://www.theguardian.com/world/commentisfree/2019/mar/09/dont-try-to-silence-populists-listen-to-them

Hoffman, Anna Lauren and Jonas Anne. "Recasting Justice for Internet and Online Industry Research Ethics", In Zimmer, Michael and Kinder-Kurlanda, Katharina (eds). *Internet Research Ethics for the Social Age: New Challenges, Cases, and Contexts.* New York, Peter Lang, 2017, pp. 3-19

Hutchinson, Jonathan, Martin Fiona, and Sinpeg Aim. "Chasing Isis: Network Power, Distributed Ethics, and Responsible Social Media Research", In Zimmer, Michael and Kinder-Kurlanda, Katharina (eds). *Internet Research Ethics for the Social Age: New Challenges, Cases, and Contexts.* New York, Peter Lang, 2017, pp. 57-71.

Krotov, Vlad and Leiser, Silva. "Legality and Ethics of Web Scraping".*Proceedings of the Twenty-fourth Americas Conference on Information Systems*, New Orleans, September 2018.

Landers, Richard, Brusso Robbie, Cavanaugh Katelyn & Collmus Andrew. "A Primer on Theory-Driven Web Scraping: Automatic Extraction of Big Data From the Internet for Use in Psychological Research". *Psychological Methods.* Vol. 21, No. 4, May 2016, pp. 475-492. doi:10.1037/met0000081.

Markham, Annette and Buchanan, Elisabeth. "Ethical Decision-Making and Internet Research", *Association of Internet Researchers,* 2012, pp. 1-19. https://aoir.org/reports/ethics2.pdf

Markham, Annette, , Tiidenberg Katrin and Herman Andrew. "Ethics as Methods: Doing Ethics in the Era of Big Data Research", *Social Media + Society*, Vol. July-September, 2018. https://doi.org/10.1177/2056305118784502

Marx, Gary T. "Ethics for the New Surveillance", *The Information Society*, Vol. 1, No. 3, 1998, p. 171-185

Merriam-Webster Dictionary. "Surveillance" https://www.merriam-webster.com/dictionary/surveillance

Owasp. Owasp Top 10 - 2017: The Ten Most Critical Web Application Security Risks, https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

Pappas, Takis S. "Modern Populism: Research Advances, Conceptual and Methodological Pitfalls, and the Minimal Definition", *Politics: Oxford Research Encylopedia,* 2016, doi: 10.1093/acrefore/9780190228637.013.17

Paul, Richard and Elder, Linda. "Miniature guide to Ethical Reasoning", *Critical Reasoning*, 2005. http://www.criticalthinking.org/files/SAM-EthicalReasoning2005.pdf

Privazy Plan. http://www.privacy-regulation.eu/en/article-9-processing-of-special-categories-of-personal-data-GDPR.htm

Puschmann, Cornelius. "Bad Judgement, Bad Ethics: Validity in Computational Social Media Research", In Zimmer, Michael and Kinder-Kurlanda, Katharina (eds). *Internet Research Ethics for the Social Age: New Challenges, Cases, and Contexts.* New York, Peter Lang, 2017, pp. 95-113.

Ravn, Signe, Barnwell Ashley, & Barbosa Neves Barbara. "What is "Publicly Available Data"? Exploring Blurred Public-Private Boundaries and Ethical Practices Through a Case Study on Instagram", *Journal of Empirical Research on Human Research Ethics*, 2019. https://doi.org/10.1177/1556264619850736

Robson, James. "Participant Anonymity and Participant Observations", In Zimmer, Michael and Kinder-Kurlanda, Katharina (eds). *Internet Research Ethics for the Social Age: New Challenges, Cases, and Contexts.* New York, Peter Lang, 2017, pp. 195-202.

SATORI, "Report on standardizing operating procedures in ethics assessment", July 2017. http://satoriproject.eu/media/D7.1_Standardizing_ethics_assessment.pdf

Snell, James and Menaldo, Nicola. "Web Scraping in an Era of Big Data 2.0", *Bloomberg Law,* June, 2016. https://www.bna.com/web-scraping-era-n57982073780/

Solove, Daniel. *Understanding Privacy,* Cambridge MA, Harvard University Press, 2008.

Stahl, Carsten Bernd and Wright, David. "Ethics and Privacy in AI and Big Data: Implementing Responsible Research and Innovation". *IEEE Security and Privacy*. Vol 16, No. 3, May/June 2018, pp. 26-33. doi: 10.1109/MSP.2018.2701164

Sugiura, Lisa, Rosemary Wiles, and Catherine Pope. "Ethical Challenges in Online Research: Public/Private Perceptions." *Research Ethics,* Vol. 13, No. 3–4, July 2017, pp. 184–199. doi:10.1177/1747016116650720.

Tajfel, Henry. and Turner, John. "An integrative theory of intergroup conflict", In Hatch, Mary Jo and Schultz, Majken (eds.). *Organizational Identity: A Reader*, Oxford, Oxford University Press, 2004, pp. 56-65

Twitter. "Twitter Terms of Service". Last modified May 25, 2018. https://twitter.com/en/tos#intlTerms

Williams, Matthew L, Burnap Pete and Sloan Luke. "Towards an Ethical Framework for Publishing Twitter Data in Social Research: Taking into Account Users' Views, Online Context, and Algorithmic Estimation", Vol. 51, No. 6, 2017, pp. 1149-1168.

Wirth, Werner et al. "The appeal of populist ideas, strategies, and styles: A theoretical model and research design for analyzing populist political communication". *NCCR democracy,* Working Paper No. 88, Zurich, 2016, http://pwinfsdw.uzh.ch/publications/workingpaper/pdf/wp88.pdf

Wright, David and Raab, Charles D. "Constructing a surveillance impact assessment". *Computer Law and Security Review*. Vol. 28, Issue 6, pp 613-626. December 2012. https://doi.org/10.1016/j.clsr.2012.09.003

Zimmer, Michael. "But the data is already public: on ethics of research in Facebook", *Ethics and Information Technology,* Vol. 12, 2010 pp. 313-325.

Zimmer, Michael. "Addressing Conceptual Gaps in Big Data research Ethics: An Application of Contextual Integrity", *Social Media + Society,* Vol. April-June 2018, pp. 1-11. https://doi.org/10.1177/2056305118768300

Zimmer, Michael and Kinder-Kurlanda, Katharina (eds.). *Internet Research Ethics for the Social Age: New Challenges, Cases, and Contexts.* Peter Lang, New York, 2017.