Chapter 10
Unwinding a Legal and Ethical Ariadne's Thread Out of the Twitter Scraping Maze

Arianna Rossi, Archana Kumari, and Gabriele Lenzini

Abstract Social media data is a gold mine for research scientists, but such type of data carries unique legal and ethical implications while there is no checklist that can be followed to effortlessly comply with all the applicable rules and principles. On the contrary, academic researchers need to find their way in a maze of regulations, sectoral and institutional codes of conduct, interpretations and techniques of compliance. Taking an autoethnographic approach combined with desk research, we describe the path we have paved to find the answers to questions such as: what counts as personal data on Twitter and can it be anonymized? How may we inform Twitter users of an ongoing data collection? Is their informed consent necessary? This article reports practical insights on ethical, legal, and technical measures that we have adopted to scrape Twitter data and discusses some solutions that should be envisaged to make the task of compliance less daunting for academic researchers. The subject matter is relevant for any social computing research activity and, more in general, for all those that intend to gather data of EU social media users.

Keywords Social media data scraping · Text and data mining · Social computing · Research ethics · GDPR compliance · Anonymization · Pseudonymization · Informed consent · Data integrity · Twitter

1 Introduction

The social media "data gold mine" [25] is increasingly exploited by researchers from all domains. Platforms like Twitter, Reddit, and Facebook present a volume and variety of data that would be otherwise impossible to obtain, like the insights into the opinions and experiences of various communities regardless of their

A. Rossi (✉) · A. Kumari · G. Lenzini
University of Luxembourg, Interdisciplinary Center for Security, Reliability and Trust (SnT), Esch-sur-Alzette, Luxembourg
e-mail: arianna.rossi@uni.lu; gabriele.lenzini@uni.lu

S. Schiffner et al. (eds.), *Privacy Symposium 2022*,
https://doi.org/10.1007/978-3-031-09901-4_10

physical location [49]. However, the norms constituting ethical behaviour around the harvesting of information shared on social networks are object of animated debates in the scientific community, especially when such data is sensitive (e.g., health data) or used to derive insights on vulnerable populations (e.g., mental health predictions). Harvesting social media data does not only raise ethical concerns but also raises questions about its legitimacy and lawfulness: only because researchers *can* easily access such data, it does not mean that they *should* dispose of it at their will. Generally speaking, the mining and analysis of data available on social platforms engenders "new forms of discrimination, exclusion, privacy invasion, surveillance, control, monetisation and exploitation" (p. 42) [33]. It is indisputable that harvesting social media data to derive clinical insights may have legal and ethical implications: for instance, those sufferings from mental health issues are considered a vulnerable population, hence deserve extra protection. But using social media as a source of material for research purposes raises issues even beyond such clearly questionable cases, for example, on whether it is possible to apply a level of ethical safeguard comparable to other research studies on human beings.

This article seeks to shed light on the use of Twitter data for academic research to address common challenges arising from social computing [44], which consists in harvesting information available on platforms that enable social interactions. In particular, it focuses on social media *data scraping* [38], an approach in text and data mining [30] that uses software to find and extract contents from websites, usually at scale. There is a lack of consensus among researchers about the ethical attitudes and the legal practices surrounding data scraping [60]. Similar dilemmas about the application of research ethics to online media exist among university's institutional review boards, at least in the USA [59]. Such uncertainty leaves many questions unanswered and creates practical difficulties for researchers like us that need to navigate a maze of legal obligations and considerations with ethical import to collect and analyse Twitter data. Some questions concern the legal protection of personal data and its technical implementation. For instance, which content disclosed on social media is personal data and is it possible to anonymize it? Other questions concern ethical research conduct: how may ethical safeguards be transposed to an online context where data is gathered in the absence of the research subjects, who moreover are often unaware that what they post online may be collected by third parties [26, 46]? The questions about data protection and research ethics that we address in this article are provided in Sect. 2.

To find suitable answers and discuss the legal and ethical implications of social media scraping, we follow two research methods. First, we review the relevant provisions of the General Data Protection Regulation (GDPR) and research ethics principles, together with their scholarly interpretation. Second, we follow an autoethnographic approach [2] to explore the interplay between research ethics and data protection compliance, and to reflect on the difficulties of devising and applying concrete protection measures to the analysis of Twitter data.

Contribution This paper contributes to the current discussion on the ethics and lawfulness of employing social media information in academic data science research. In particular:

- it offers practical recommendations for academic researchers who seek to navigate legal compliance and ethical foresight, by referring to the specific use case of Twitter;
- it explores the reciprocal influence between research ethics principles and data protection compliance measures;
- it proposes and critically discusses solutions that should be envisaged to make the task of compliance less daunting for academic researchers.

Relevance The matters that we discuss are relevant for research performed on social media platforms like Twitter, Facebook, and Reddit, to cite a few. Moreover, they could be of interest for both EU researchers (see, e.g., the ethical requirements for Horizon project proposals [35]) and non-EU researchers who intend to analyse data of individuals located in the EU.

Disclaimer This article is not meant to become a checklist for compliance nor it intends to provide a collection of golden rules to gain ethical clearance. What we describe in this work is exploratory in nature and specific to the context of our particular research study. Our discussions can serve as inspiration, but none of the measures should be applied uncritically to similar research activities, because they may not be appropriate for other types of platforms, institutions, jurisdictions, research goals, etc. As an integral part of other research activities, the respect of applicable legal obligations and of research ethics principles is a creative exercise based on critical thinking that should lead to the design of ad hoc solutions. For a general guidance on internet research, dedicated guidelines [56, 62] are more appropriate.

2 Methodology and Research Questions

Even though automatically collecting social media data for research is a widespread activity, there is no standardized practice on how to perform it legally and ethically, one reason being that it is challenging to define and circumscribe the exact issues concerning research ethics and the applicable laws. We first explore the data protection implications and how to fulfil the related legal obligations (Sect. 4). Our approach resorts to a classical desk review that analyses inputs from relevant articles of the GDPR; their scholarly interpretation, with a focus on academic research [16, 29, 40, 45, 51]; and official guidance from data protection and cybersecurity authorities (like the European Data Protection Board—EDPB—and the European Union Agency for Cybersecurity—ENISA) [4–6, 20, 22, 31]. Similarly, to address the ethics-oriented questions (Sect. 5), we base our discussion on guidelines from

professional associations [62], codes of conduct for researchers [3, 19, 43] and academic commentaries [26, 35, 59, 63].

Additionally, we bring our personal contribution to the topic through the reflections and arguments we have developed during our own experience of scraping social media data for research. These were enriched by the long conversations about legal and ethical matters that we had with the Data Protection Officer (DPO), with the Ethical Review Panel (ERP), and with other legal representatives of our institution, the University of Luxembourg. Even if we are a team offering complementary expertise in cybersecurity, data protection, online privacy, and research ethics, we have been challenged to find a way to mine and process social media information in compliance with the provisions of the law and the indications of the DPO and the ERP. To analyse and report such experiences, we follow an autoethnographic approach, which is a "research method that uses personal experience (auto) to describe and interpret (graphy) cultural texts, experiences, beliefs, and practices (ethno)" [2], thus offering an insider's knowledge built on everyday experiences that cannot be easily captured through other research methods. Our field notes and observations, available on demand, are the MSc thesis of one of the authors [34], the documents we filed to ask legal and ethical clearance, and the communications we exchanged internally and with the legal teams.

Questions About Data Protection

- What counts as personal data in social media data?
- Is it possible to anonymize social media data?
- Which legal principles apply in this research context and which measures should be implemented to comply with them?
- How can a great number of social media users be informed that their personal data is being gathered?

Questions About Research Ethics

- Should researchers ask for social media users' consent to research participation, even when their data is public?
- How might social media users express their will of abstaining from or withdrawing their participation and how can their data be hence excluded?
- How can data about underage users be excluded, when it is highly challenging—and even impossible—to determine whether social media contributors are adults or minors?
- What kinds of social responsibility have social media data scientists?
- What additional safeguards should be adopted to minimize the harms and maximize the benefits of the research study?
- What are, if any, the points of tension and of interplay between legal and ethical principles?

3 Research Scenario: Dark Patterns, Twitter, and Accountability

We are currently collecting content submitted by social media users on Twitter on the topic of *dark patterns* [28, 39], as part of the interdisciplinary project "Deceptive patterns online (Decepticon)".[1] Dark patterns are defined as potentially manipulative designs that influence users to take decisions that are contrary to their interests but benefit the companies implementing them, for instance, selecting privacy-adverse settings in an application. Practices that unduly influence the behaviour and choices of individuals are considered illegal in the EU under consumer protection and data protection law, and dark patterns may fall under this category [36]. Understanding what makes a pattern "dark", and potentially illegal, is the goal of the Decepticon project. On Twitter, there is a lively community that shares screenshots of potential dark patterns, with the hashtag `#darkpatterns`. Such content is a precious source of lay user perspectives on a topic that is dominated by expert opinions of lawyers, designers, and academics. It also provides manifold examples of dark patterns that can be used to build large corpora for, e.g., developing machine learning classifiers that automatically recognize dark patterns [9]. At the moment of writing, there is a dearth of data sets of dark pattern samples available for research. Hence, mining social media data could significantly contribute to our understanding of dark patterns and the design of solutions against them.

Text and data mining for research purposes are permitted in the EU at the conditions enshrined in Art. 3 of the Directive (EU) 2019/790 (also known as Copyright Directive) [17]. In line with this, Twitter has put in place a mechanism of verification to allow selected developers to access its content through a dedicated API: without authorization, data scraping is prohibited.[2] In January 2021, Twitter launched an updated version of its API[3] to grant academic researchers free access to full-archive search of public data and other endpoints, meaning that the whole Twitter database (holding data from 2011 till now) can be accessed, excluding the contents marked as private by their authors. Through this API, academic data scientists can scrape an impressive amount of tweets rapidly and free of charge, while leveraging enhanced features to gather specific data of interest.

Before obtaining access to the Twitter's API we were compelled to describe the purpose of our research to the Twitter developers' team, who reviewed our motivation, mission, and practices. We needed to prove that we are employees of an academic institution and explain how we intend to use Twitter, its APIs, and the collected data in our project. In another round of Q&A, we illustrated our methodology for analysing data and our intention of not disclosing it to government

[1] https://irisc-lab.uni.lu/deceptive-patterns-online-decepticon-2021-24/.

[2] "[S]craping the Services without the prior consent of Twitter is expressly prohibited" https://twitter.com/en/tos#intlTerms.

[3] https://developer.twitter.com/en/docs/twitter-api/early-access.

entities. After this, we were authorized to open an academic developer account, get access to the API, and start mining data.

Once we obtained the authorization, we started questioning what was the rightful way to proceed. From an ethical standpoint, data scientists are held accountable for their research conduct, including data management. Similarly, in the GDPR accountability corresponds to an ethical responsibility concerning the collection, storage, processing, and sharing of personal data. It means that the burden of evaluating the lawfulness and fairness of data processing falls primarily on those that collect and use the data, who also need to be able to demonstrate how they do it in a compliant manner [11]. Although resorting to social media data is a widespread practice both in academia and industry, e.g., to gather big data sets of user opinions on a specific topic, there is no sound checklist that can guide researchers towards legal and ethical behaviour. Understanding and implementing abstract rules into concrete decisions and actions appear labyrinthine even for experts, especially because each study deserves a customized solution.

4 Protecting Users' Data and Identity

Although the Data Protection Directive 95/46/EC EU already regulated the use of personal data before the entry into force of the GDPR, research practices involving personal information have never been so much under the spotlight. The GDPR has generated anxiety within the academic walls [14], even though the regulation provides several exemptions and derogations that benefit researchers with a certain degree of freedom. Nevertheless, they are not exempted from the application of technical and organizational measures that are meant to safeguard the rights and freedoms of individuals (Art. 89) [16], like data minimization and access control. To carry out a study involving personal data analysis, it is mandatory to engage with the expert opinion of the Data Protection Officer (DPO) of the university and to maintain a record of processing activities (art. 30 GDPR). Thus, before the data collection starts, at our institution, principal investigators are expected to fill in a Register of Processing Activities (RPA) where they detail the categories of personal data they intend to collect, the retention period, the envisaged security measures and other relevant information. This ex-ante activity has forced us to interpret the legal notions contextually, draft a concrete data protection plan adhering to principles like data minimization and storage limitation, and make data-protection-by-design choices [15, 20].

4.1 Personal Data in Social Media Research

According to the GDPR, personal data "is any information that relates to an identified or identifiable living individual" (Article 4). This definition is only

apparently simple because it hides a continuum of data. Even isolated pieces of information, when linked together, can lead to the identification of a person. Pseudonymized [40] data is considered personal data because it can be recombined to identify individuals, and so is encrypted data, when it can be easily decrypted. On the contrary, anonymized data that is irreversibly unlinkable to any individual is no longer considered personal data. But in a world where a simple search online of a quote can lead to its author, it is daunting to fully de-identify personal information. On social media, both actual data produced by the user and metadata about such information can be used to re-identify a person with little effort, like usernames (even pseudonyms [62]), pictures and screenshots, timestamps, location markers, tags, mentions of other users, shared user networks, and names that appear on comments and retweets. Hence, we decided to adopt a broad interpretation of the notion of personal data because both text and pictures may contain references or pieces of information that could be combined to allow re-identification. Thus, even when tweets are shared publicly, assuming that they probably constitute personal data helps to determine the permissible extent of scraping (Sect. 5.1) and the feasibility of anonymization (Sect. 4.2).

4.2 Confidentiality

Protecting the confidentiality of personal data and the identity of individuals greatly overlaps with one of the cornerstones of research ethics (i.e., respect for privacy—Sect. 5.1.2). From the onset of a research project, a data-protection-by-design approach [20] should assess whether personal data can be anonymized and thus be outside of the scope of the GDPR, which would exempt us from applying technical and organizational measures to protect the confidentiality and security of the data (Art. 32.1).

4.2.1 Anonymization and Pseudonymization

Although it would be comfortable to believe that once direct identifiers (i.e., user handles, mentions, etc.) have been removed, social media data becomes anonymized (as it is often claimed), such comfort is illusory. A number of parameters can serve as re-identification clues due to data indexing [56], ranging from looking for the text of online posts on search engines and thereby retrieving its author [7, 41], to the metadata related to online activities [64]. Other media (e.g., videos, images, etc.) associated with tweets may also contain personal data and their URL may readily redirect to the user profile. Hence, even though direct identifiers are masked (e.g., by nulling out that piece of information or by substituting it with a different data value [4]), a tweet can easily be re-associated with its author. On the other hand, a full anonymization of data, understood as an irreversible process that makes it impossible to infer the person to whom the data belongs,

is in fundamental tension with the utility of the data required for the analysis [4, 40]. Further, de-anonymization techniques [58] may invalidate the researchers' endeavours to anonymize the data. Only by aggregating data (e.g., by providing aggregated statistics) and rendering individual events no longer identifiable can a dataset be genuinely anonymized.

Thus, we opted for pseudonymization techniques that only remove certain identifiers with the intent of hindering re-identification, contributing to data minimization and enhancing data security. Pseudonymization, furthermore, offers the advantage of retrieving the authors of the tweets to ask for their consent to republication and to allow them to opt-out from the study (Sect. 5.1.3). Concretely, we have applied a deterministic pseudonymization [22] where each user ID and each tweet ID are replaced with a unique code (i.e., a pseudonym) issued by a counter. The codes are stored in a separate mapping table so that the correspondence between tweet and its author can be re-established at will. All mentions to other users (i.e., user handles) were deleted from the source file, but kept in the mapping table in view of being included in the data analysis since they contain mentions to companies employing dark patterns. As the media URLs may trace to the user, we reported them in a third file (i.e., the link file) and replaced them in the source file with a string that signals whether the tweet contains a media file or not. The timestamp and location of posting underwent a process of generalization [4] (i.e., city to country and exact time to month, year) since such an information granularity is not necessary for our analysis. As a result, we obtained three separate files that only when considered together can render the full picture: (a) the pseudonymized source file, where the tweets were polished from hashtags and user handles and numbered, the authors were replaced with pseudonyms, the time and place were generalized; (b) a mapping table, where user IDs are associated with tweet number and pseudonyms; (c) a link file where media URLs, user handles, and hashtags are stored. The images and other media are stored in a different folder. The files should be stored separately to prevent unauthorized access that would make the users identifiable.

4.2.2 Encryption, Secure Authentication, and Access Control

An additional technical safeguard that enhances security and prevents unauthorized access is encryption (Art. 32), which can be considered as a pseudonymization measure [4]. Encryption, if done properly, converts human-readable data into a form that is unreadable and irreversible, unless one possesses the decryption key [54]. We have stored the encrypted data on a local hard disk and used an encrypted channel to transfer it to a private Git repository. The access to such repository is subject to a strong authentication procedure via SSH public key authentication. Encryption provides confidentiality and secure authentication, but encryption keys are hard to manage and can be irremediably lost, thus password authentication is a viable alternative to access services and data. However, the creation, storage, and retrieval of strong passwords and their sharing across different devices are cumbersome. A role-based access control [54] that distinguishes between students,

senior researchers, principal investigators, etc. ensures further protection from unauthorized access, but setting up and keeping access rules up-to-date may not be accessible for everybody without the support of a technical team. Git repositories that are locally managed by the university's technical departments offer severely monitored means of access control and make us avoid external cloud services that could expose to the risk of data access from other jurisdictions without an adequate level of legal protection.

4.3 Purpose Limitation

The principle of purpose limitation (Article 5(1)(b)) compels researchers to be clear and open about the reasons for obtaining personal data [31]. Purpose limitation is closely linked to the principles of fairness, lawfulness, and transparency (Article 5(1)(a)), but scientists benefit from an exception: the data may be used for secondary processing on the assumption of compatibility with the original purpose of collection (art. 5.1.b and Recital 50 GDPR) [16]. Generally stating that the processing purpose is "to conduct scientific research" may not be enough though, as a similar project may expose to different kinds of harms. In the RPA, we were required to disclose additional details about the intended modalities of data collection and analysis (e.g., automated analysis of images of dark patterns, with the goal of training classification algorithms able to recognize new instances of dark patterns on websites). Such information is key to infer whether an envisioned processing activity may result in a high risk for individuals and thus whether a Data Protection Impact Assessment (DPIA) is necessary [5]. Criteria to evaluate its necessity encompass whether, like in our case, personal data are not collected directly from data subjects and the processing happens at large scale. Our methods, however, do not involve an innovative use of technology with unknown social and personal consequences, nor privacy-intrusive activities like profiling or automated decision-making that may expose individuals to higher (ethical) risks [35]. Thus, it was established that a DPIA was not necessary.

4.4 Data Minimization

Intimately linked to the research purpose, the data minimization principle (Article 5(1)(c)) mandates to collect data that is adequate (i.e., sufficient with respect to the purpose), relevant (i.e., justified by the purpose), and limited to what is necessary (i.e., not more than is needed for that purpose) [31]. We abstained from gathering data on users' profiles that were nor relevant to our research and tweets that did not explicitly mention dark patterns. Instead, we collected usernames to trace back the users and ask their consent for tweet republication (Sect. 5.1.3), as well as the broad location and timestamps of the tweets to discern, e.g., in which countries users

are more concerned about dark patterns and whether this tendency evolves over time. We also scraped media URLs to build a database of dark pattern images, and retweets and likes to grasp the "popularity" of certain dark patterns. Moreover, we gathered mentions that can contain the name of companies employing dark patterns.

4.5 Storage Limitation

The principle of storage limitation (Article 5(1)(e)) prescribes that personal data should only be kept as long as necessary to fulfil the processing purpose [31] and should be deleted or fully anonymized right afterwards. However, this requirement is at odds with research ethics: for reasons of data integrity and research transparency, it is recommended to keep the data for 10 years [19]. Although anonymization should be preferred, a specific research exemption allows to store the data in an identifiable form for longer than what would be strictly necessary [16], provided that reasonable justification and security measures (e.g., encryption, pseudonymization, etc.) are in place [35].

4.6 Legal Basis

Research activities involving personal data must be justified on an appropriate legal basis among consent, public interest or legitimate interest (Art. 6) [16] and may also depend on national laws. There is no straightforward way of determining whether one is more suitable than the other, as each come with its own advantages and disadvantages. Since we indirectly collect information from many individuals, and thus the acquisition of consent would be "complicated or administratively burdensome" [37, p. 58], we followed the lead of the DPO to argue that our data processing is necessary for the performance of a task carried out in the *public interest*.

4.7 Transparency

Transparency is another fundamental principle of data protection (Art. 5(1)) and translates into the disclosure about the use of data and the rights of individuals in this respect [6]. Note that such disclosure is necessary, even when the processing is not based on consent. The transparency obligation mandates the provision of specific pieces of information (Art. 13, e.g., the identity of the entity collecting data, the purposes of data collection, etc.) in an easily accessible and easy to understand manner (Art. 12) before the data collection starts. We benefit, however, from a research exemption when personal data are not directly obtained from the data

subject (Art. 14), since with scraping, data are first collected by the social media platform, and only then gathered and reused by researchers for their own purposes. In such cases, informing thousands of individuals of the processing activities before data collection occurs would constitute a disproportionate effort [16, 35]. Hence, the transparency obligation can be fulfilled by drafting a public notice addressed to all those that may be impacted by the research. We therefore published the notice on our project's website[4] but also pinned a summary of it on our Twitter profile.[5]

We followed best practices of legal design to present the information in a user-centred manner [6, 50, 51]. First, as our audience consists in a broad non-expert user base, we used plain language, removed unnecessary legalistic expressions and applied a conversational style that distinguishes the responsibilities and rights between "we" (i.e., the researchers) and "you" (i.e., research participants). We also clarified technical terms and explained the consequences of certain data practices, e.g., "*We pseudonymize the information that we collect: we separate the identity of the users (like usernames) from the rest of the data (posts, images, etc.) and we replace real identities with fake names (also called pseudonyms). In this way, only us can re-identify the users to whom the data refers*". In addition to plain language, we used layering techniques (e.g., main words in boldface) to allow readers to skim through the text and quickly find the piece information they are looking for. Moreover, sections are structured in accordions, i.e., they can be expanded at request and lighten an otherwise lengthy text, while headings are formulated as FAQs (e.g., *What are your rights concerning your personal data?*).

However, such an on-demand notice [53] is tucked away on the project's website, so there is little chance that Twitter users actively seek for and find it. Thus, we reported a shortened version of it on our Twitter profile and we devised a periodic notice [53] that once a month reminds Twitter users of the existence of our (imperceptible) data collection (see Fig. 10.1). The tweet contains

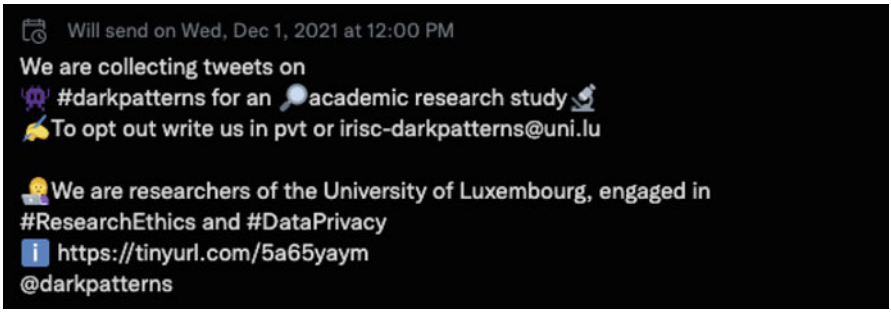

Fig. 10.1 The recurrent tweet scheduled for the first of each month and meant to warn Twitter users of our data collection. It indicates where they can find additional information and how to opt-out from the study

[4] https://irisc-lab.uni.lu/public-notice-for-twitter-and-reddit-web-scraping/.

[5] https://twitter.com/ULDecepticon.

the hashtag `#darkpatterns` and a mention to the highly popular Twitter handle `@darkpatterns` to increase its visibility. It also includes a link to the public notice on our website and a short explanation on how to opt-out from the study (Sect. 5.1.3).

4.8 Data Subjects' Rights

Unlike anonymization, pseudonymization enables tweets' authors to exercise their rights: the right to access (Art. 15), rectify (Art. 16), and erase (Art. 17) their data, as well as to ask us to limit the data processing (Art. 18) and to object to processing (Art. 21), which would prevent us from using the data. However, Art. 89 provides for research-specific derogations when necessary and proportionate. Moreover, since the legal basis is the public interest, the right of erasure can be limited (Art. 17(3)d) because deleting data may prevent data verification and thereby undermine the scientific validity of the research study [16]. However, such limitations may (arguably) apply only to studies where data analysis is concluded [45], because when it is not the case, the exercise of this right does not seriously hamper the research progress.

5 Ethics of Using Social Media Data for Research Purposes

Unlike legal provisions, norms contribute but do not determine what ethical behaviour is [26]. There may be disagreement between researchers and other stakeholders (e.g., the public, ethicists, policymakers, etc.) about what constitutes ethical practices, which may depend on the context where the study occurs [60]. That said, in the EU there is a lively ethics culture surrounding research, crystallized in international, national and institution-specific codes of conduct [19] and even regulations [21]. EU scientific projects, for example, must respect the principle of proportionality and the right to privacy, to the protection of personal data, to the physical and mental integrity and to non-discrimination (Art. 19 of the Regulation establishing Horizon Europe) [21], in line with the European Code of Research Integrity [3] based on principles like reliability, honesty, respect, and accountability. Differently from the USA [26], in Europe research performed on social media data is considered full-fledged research with human subjects. As such, it is governed by the same ethical principles [62].

One of the unique features of this area of research concerns the fact that the content disclosed on a certain platform for a certain reason is extrapolated and reused for other purposes in a different context—without the awareness of the authors of such content [26, 46]. For instance, people may use social media to feel part of a community and share their experiences, e.g., about poor mental health [49]. Even if such information has been disclosed publicly, this does not imply

that one can lightheartedly scrape, analyse, or report it without users' knowledge. This concern recalls the construct of "contextual integrity" [42] that posits that confidentiality expectations are tied to the inherent norms of specific contexts. Given such premises, the participation of individuals to research performed through data mining cannot be considered voluntary nor informed. Data mining thus exposes researchers to risks and questions that are unique to the Internet and constitute an uncharted (or at least only partially explored) territory. The research ethics strategies outlined in the following sections refer to the four core principles underpinning ethical research conduct with human beings [43] and have received the ethical approval of the institutional ERP after two rounds of negotiations.

5.1 Respect for the Autonomy, Privacy, and Dignity

5.1.1 Public vs. Private Information

Data scientists may erroneously be under the impression that information publicly shared on social media platforms can be reused without limitations [35] and at their will, without seeking consent from the interested parties nor ethical clearance, similarly to what is permissible for research conducted in public places where individuals can reasonably expect to be observed [61]. It is true that users share views, pictures, etc. on online platforms that are easily accessible, permanent in time, and designed to boost visibility and engagement. Moreover, the terms and conditions commonly contain clauses warning against third-party access to the data[6] [56]. However, studies demonstrate that most Twitter users ignore that their content can be harvested by others [26, 46], as terms and conditions are simply clicked away.

The distinction between public and private spheres on the internet is decisively blurred, but certain elements can help to infer what is acceptable behaviour (see the concept of contextual integrity recalled above). Whereas social media members disclosing content in a password-protected group may have reasonable expectations of high confidentiality [62], we may assume that users contributing to a public debate on a certain topic with a tweet containing a relevant hashtag, thus designed to be visible and retrievable, will expect less confidentiality (Sect. 5.1.3). Another crucial element is the sensitivity of the information at hand [62]: contents about drug abuse, sexual orientation, and health-related issues as well as data shared by minors should be handled with utmost care as they may cause harm to the authors when leaked outside of the context they were intended for. In such cases, researchers should reflect on the consequences of such disclosure to a different audience in a

[6] The 2021 Twitter's privacy policy states that "Most activity on Twitter is public, including your profile information, [. . .] your Tweets and certain information about your Tweets [. . .]. [. . .] By publicly posting content, you are directing us to disclose that information as broadly as possible, including through our APIs, and directing those accessing the information through our APIs to do the same". Source: https://twitter.com/en/privacy.

different context. Moreover, user permission should be sought [26, 61]. In our case, we deliberated that scraping is permissible, since (i) we only gather manifestly public tweets containing hashtags meant to participate in the lively debate about dark patterns, (ii) the topic is not sensitive and (iii) we abstain from any privacy-invasive processing like profiling.

5.1.2 Anonymity and Confidentiality

No matter if public or private, the information we gather is nevertheless personal and deserves protection (Sect. 4.2). Research investigators have the duty to avoid causing physical, emotional, or psychological harm to participants [7]. Confidentiality seeks to eliminate risks of increased vulnerability, embarrassment, reputation damage, or prosecution [57], hence the need to proceed carefully when information is repurposed in a different context from where it was originally disclosed. In regard to the publication of individual excerpts (like verbatim quotes in academic articles), full anonymization seems difficult to attain because public tweets are retrievable with a simple online search. The only viable manner to conceal users' identity consists in paraphrasing the tweet [62]. However, such an artificial alteration would comprise the ethical tenet of data accuracy and integrity (Sect. 5.2). Hence, we have decided to abstain from quoting verbatim tweets without a good reason [26] and, if that was the case, to ask the permission of the authors. In light of such considerations and given the envisaged opportunity to withdraw from the study, we applied pseudonymization to be able to map tweets to authors and added other security measures to protect the confidentiality of data and identities (Sect. 4.2).

5.1.3 Informed Consent and Opt-out of Unwitting Participants

Our research study has public interest as legal basis rather than ("legal") consent (Sect. 4.6). Nevertheless, informed consent for research participation is still indispensable as an ethical safeguard ("ethical consent"), as it allows individuals to exercise their autonomy [43]. Only when informed about the modality and risks of the study, they can freely express their willingness to take part in the study, refuse their consent or withdraw it whenever they desire. However, scraping data at large subverts such logic given that seeking consent from each potential participant before the study begins would represent a disproportionate effort. Moreover, it is assumed that gathering non-sensitive, visibly public data does not require consent [62]. Yet, informing participants about the study constitutes good practice and may be deemed sufficient, as some surveys reveal [26].

Thus, in our case, we do not ask consent to participate in the study, but we provide public information (Sect. 4.7) and the possibility to withdraw from the study (i.e., retrospective withdrawal [62]), which also partially overlaps with the right to object to processing (Art. 21) enshrined by the GDPR. The withdrawal implies that any further analysis on the collected data must cease, although whether the

already processed data should be excluded from the research findings, as discussed in Sect. 4.8, may eventually depend on practical issues, such as the effort to exclude that data and carry out a new analysis. We inform Twitter users about opt-out options on the periodic tweet, on our Twitter profile, and on our website.

5.2 Scientific Integrity

5.2.1 Data Quality

To ensure the validity of the findings and of the conclusions of a piece of research, the data should not be tampered nor transformed in an unreasonable manner [62]. This is why paraphrasing user-generated quotes to protect user confidentiality should be weighted against the possibility of altering the research results. An additional concern that could hamper data quality derives from the eventuality of including data of vulnerable populations, such as minors, and of false social media profiles powered by bots, while excluding the views of populations that are not present on that platform. Further, given the opacity surrounding the disclosure of data by social media platforms through their API, it is challenging to determine whether the data made available is representative or complete. Lastly, inaccurate and even misleading inferences [62] may be generated through text analysis (e.g., sentiment analysis) and other machine learning techniques (e.g., clustering). Such concerns will be duly addressed when we will perform the data analysis and will be discussed in our next publications.

5.2.2 Minors

Unlike other research methods, data scraping does not make it possible to screen who participates in the research [62]. Such lack of oversight may not only jeopardize scientific integrity but also lead to the mining of the personal data of minors, who are considered a vulnerable population, without authorization from their legal guardian, because the minimal age requirement to register on Twitter and other social media is 13 years. What is more, such platforms do not offer ways to exclude minors' profiles from data collection. This constitutes a serious issue, as minors are not considered capable of providing their consent to research participation and should not even be contacted in this regard. The ad hoc solution we elaborated envisages that we only report the results in an aggregate form, given that the data that is the object of our research is not sensitive and does not point back to individuals. In case we intend to seek (ethical) consent in the view of republishing individual quotes, we envision to only contact users that are presumably over 18 according to the birth date on their profile (which can be, however, fake) or that have a professional profile associated with their social media profile (e.g., a profile on LinkedIn; an academic website; etc). When obtaining consent is not possible but the republication of a

tweet is particularly meaningful, we envision to republish only paraphrased tweets. We have also asked Twitter to implement a functionality that allows developers to filter out minors' data in their next API release, given that they dispose of user age information.

5.3 Social Responsibility

5.3.1 Reputation Damage

An additional ethical dilemma derives from the research topic: dark patterns are ethically questionable and may also be illegal. But when people share their views about interfaces that they deem dark patterns within their digital entourage, they are expressing a personal opinion. Considering such opinions in our analysis may legitimate them and negatively associate the companies therein mentioned to dark patterns (e.g., if we provide figures about the most cited "evil" firms in our database). Even if the analysis is scientifically sound, companies may suffer from reputation damage. This issue echoes ethical questions about vulnerability disclosure in cybersecurity research [48], which may lead to legal suits. Researchers need to find ways to mitigate that risk or, alternatively, solidly motivate their position if they are convinced that naming and shaming would force companies to take action to repair their reputation. An ethical conduct of responsible disclosure demands to engage in a dialogue with the companies before going public whenever possible. In the case of dark patterns, when they may violate the law, we will submit that information to the relevant watchdogs without any public judgement about their lawfulness.

5.3.2 Dual Use

Like other online deception research (e.g., phishing) [24], this study is exposed to the risk of dual use of the findings, because they could lead the mentioned companies to replace a publicly exposed dark patterns with a more aggressive one and inspire other companies to employ dark patterns for their own benefit. However, the dilemma is mild: even if unconventionally delivered through user interface designs, the mechanisms behind manipulative commercial and cybersecurity practices have been known for decades (e.g., [10, 13]). Hence, we deem that our research does not encourage the adoption of dark patterns and that, on the contrary, its benefits outweigh the risks: it contributes to shed light on the pervasiveness of such practice, increase consumer awareness, and foster the creation of solutions.

5.3.3 Risks for Researchers

Using social media can expose researchers to cyber risks, such as cyberbullying, stalking, and media pillories, which can lead to professional and personal issues

like loss of scientific reputation and anxiety. Such risks must be mitigated, especially when they concern early stage researchers like master or PhD students.

5.4 Maximize Benefits and Minimize Harm

All measures listed above are meant to minimize the risks for participants and researchers, while maximizing the research benefits. One further issue concerns compensation: it is common practice to reward research participants for their time and efforts, but doing so with data that was collected indirectly is problematic. Surveyed individuals have expressed that, even without financial compensation, they could benefit from being informed about the publication of the study and the results [26]. This is why we plan to distribute this and following articles in open access and disseminate them on Twitter using the hashtag `#darkpatterns`.

6 Discussion

A total of 15,784 public tweets and 3284 media images have been scraped for the period July 2011–July 2021. The data collection will continue for the 3 years duration of the project, hence the data practices described in these pages may evolve. What lessons may we have drawn from our tentative path out of the legal and ethical maze of Twitter data mining?

6.1 The Question of Time and Expertise

The procedures to obtain ethical clearance and legal authorization should be initiated at least weeks before the start of the planned research activity to avoid any delay. In our case, several months passed between the decision of performing social media scraping and the actual start (Fig. 10.2), due to (a) the conception, design, and application of measures with legal and ethical import, (b) their constant review arising from a more nuanced understanding of the research challenges and the interplay between legal provisions and ethical principles (e.g., pseudonymization to enable opt-out); and (c) the iterative negotiation with the ERP and the DPO about issues like minors' consent, opt-out options, anonymization, etc. These concerns may appear to research scientists like dull conundrums that add unnecessary complexity to other already daunting research tasks. Furthermore, accurately planning data management requires an uncommon high level of competence, both theoretical (e.g., the selection of an appropriate pseudonymization technique for the data at hand) and practical (e.g., its application). This is why we echo Vitak et al. [60] in

Fig. 10.2 This timeline exemplifies the process of devising data protection and ethical measures that started in November 2020 and ended in August 2021

recommending that ethical and lawful deliberation should be constructed together with expert colleagues, ethics boards and legal teams of the institution.

6.2 The Question of Motivation

Burdensome compliance may delay researchers, who are already under time pressure due to, e.g., the project timeline and personal career development plans. Moreover, the quality of researchers' work is almost exclusively evaluated through indicators like publications and project deliverables, without any attention to ethical and lawful conduct. Given that there are no one-size-fits-all approaches, researchers must tailor the limited existing guidelines to their specific use case based on questions like: How sensitive is the subject matter? Are these data meant to be public or private? Can anonymization techniques be successfully applied? Etc. One may wonder what is the reward of spending time and energies in compliance, while delaying the actual research, and what is the penalty for failing to do so, since there are no visible drawbacks. Although ethical and legal aspects are an integral part of researcher's responsibility, merely reiterating this message does not constitute an effective leverage to trigger the desired behaviour. In certain ICT communities, like Human-Computer Interaction, it is impossible to publish a study involving humans without an explicit section about ethical considerations—and indeed, the ACM has recently updated their publication policy in this respect [1]. However, this is not common practice: only a minority of published studies on Twitter [63] and Reddit data [47] mentions institutional ethical clearance. Even then, it is mostly to claim that their study was exempt.

Obtaining approval for data mining may appear superfluous as the data is publicly available on the internet and is often republished in aggregate form. In addition, although we have not investigated this aspect, the research exemption enshrined by Art. 3 of the Copyright directive may erroneously lead data scientists to assume that they have complete freedom to process data available on the internet. Moreover,

given that compliance with data protection provisions may appear "impossible to follow" [14], scientists' decision-making may be influenced by convenience considerations or by anxiety over unforeseen violations of the GDPR, which may lead to exclude EU participants from research studies [18] and impact research integrity. Given that Twitter is the most popular social network platform to examine human interaction [26] (so popular that it has released an API dedicated to academic developers), it is remarkable that data scraping can be regarded as "an uncharted territory". Without convincing incentives that entice researchers to easily embrace cumbersome, time-consuming ethical and legal conduct, one common solution may consist in sidestepping the rules. Thus, which incentives could help researchers to strike a balance between productivity and accountability?

6.3 Incentives

We hereby examine two sorts of incentives. The first set of solutions aims at raising researchers' awareness towards ethical and legal demands and strengthen their ability to address them. Traditional training about the GDPR and research integrity is routinely offered at academic institutions, although it is usually optional, while codes of conducts and documents clarifying procedures are available on the intranet. However, such guidance is often too general to be able to answer doubts about specific technologies or data processing practices. Going beyond awareness and training, in the last few years entire European projects have been dedicated to seek ways to embed ethical and legal training into computer science and engineering curricula[7] and to develop ethical frameworks to support technology developers in the assessment of the impact of their creations.[8] Experiential learning initiatives are being increasingly experimented with the aim of building a more visceral sense of accountability and ethico-legal sensibility through discussion games,[9] science-fiction storytelling [55] and immersive experiences based on videogames and Virtual Reality [32].

That said, all such endeavours are necessary to make researchers raise the relevant questions, but are insufficient to find and implement appropriate answers. In the domain of compliance, it is a well-known fact that higher awareness does not necessarily translate into a safer behaviour—an inconsistency called "knowledge-intention-behaviour gap" (p. 84) [12]. When technologies and procedures are too complex, human beings find workarounds to what they see as an obstacle to their primary task (i.e., performing research). Thus, the second order of solutions should make compliance and ethical decision-making less burdensome for research

[7] For example, Legally-Attentive Data Scientists https://www.legalityattentivedatascientists.eu/; Ethics 4 EU http://ethics4eu.eu/.

[8] For example, https://www.sienna-project.eu/.

[9] Play Decide https://playdecide.eu/.

scientists. Guidance drafted as practical instructions in laymen terms and best practices dedicated to certain technologies or use cases should be created and proactively brought to the attention of researchers. Toolkits for scientists can also prove useful in this respect, such as the toolkit on informed consent created by Sage Bionetworks [27] that contains resources, use cases and checklists to help researchers think through the consenting process. There is an urgent need for usable off-the-shelf solutions that simplify and expedite academic compliance tasks. For instance, together with its academic API, Twitter could offer user-friendly functionalities to filter out minors' data and directly provide pseudonymized data—not to mention a developer policy[10] that would provide clear, simple rules and take less than 17 min to read (i.e., 4842 words). In-house applications that encrypt, pseudonymize, or anonymize information and offer transparent-by-design templates for information notices would also be helpful. When universities cannot develop their own solutions, they could offer contractors' services to their employees at reasonable prices.

7 Limitations and Future Work

The practices described in these pages may need to be updated as the research activities proceed and new (interpretations of) regulations are introduced. It would be important to gauge the effectiveness of our mechanisms of transparency (e.g., how many users tweeting about dark patterns are aware of our public notice and data collection?) and opt-out (e.g., how many Twitter users are aware they can opt-out and find it easy to do so?), and, if necessary, devise better ones (e.g., an automated warning to each tweet that is scraped). Moreover, certain data protection measures may be stronger: we would like to apply random number generators for pseudonyms and additional processes to ensure unlinkability for individual values like tweets [22]. We are currently developing a Python library for the automated masking of location markers, and people and company names (the latter meant to enable sharing of our dataset with other parties without risking defamation charges) [52]. However, named entity recognition techniques on which masking is based are not yet completely reliable, especially on tweets that present atypical sentence structures and wording. An additional promising technique that would enhance the de-identifiability of tweets' authors by removing unique stylistic cues is differential privacy applied to authorship [23]. The question whether it should be the exclusive responsibility of researchers to put in place such (often hard to implement) cybersecurity practices—or whether it should be the duty of the institution to which they belong to offer support as well as data management frameworks for that purpose—remains unanswered.

Ariadne's thread has not guided us out of the maze yet. To perform our planned data scraping on Reddit[11] we will need to assess the relevant ethico-legal concerns

[10] https://developer.twitter.com/en/developer-terms/policy.

[11] https://www.reddit.com/r/darkpatterns/.

and devise the most appropriate measures for that platform, which may depart from those adopted for Twitter data. Other dilemmas remain dangling: is it legal to share our dataset with other parties? One of the aims of our project is to publish part of the scraped dataset on an open source intelligence data sharing platform (i.e., MISP[12]) to enable collaborative data analysis. However, the research exception contained in the Copyright Directive only covers data mining, but not data sharing. Such data disclosure poses original ethical challenges [8]. Future work will be dedicated to devising viable solutions.

8 Conclusions

There is no established protocol that researchers can simply follow to mine social media information legally and ethically. Existing guidelines and best practices leave plenty of questions unsolved, therefore researchers are forced to invest resources to find their way in a maze of regulations, techniques of compliance, scholarly interpretations and codes of conduct that may differ from country to country. By self-reflecting about our experience matured for Twitter data scraping, we learned a few lessons which can be of help to other researchers, even though they do not intend to constitute a checklist.

First, all data and metadata collected from social networks should be considered personal data, thus be subject to the obligations enshrined in the GDPR. Second, even when such data is public and apparently ready to be used, it should still be subject to the same ethical safeguards that apply for research on human subjects. Understanding the sensitivity of the subject matter and the risks deriving from data collection and analysis must inform the acceptability of certain research practices and the approach to data processing, with a golden rule: respect the norms of the context where the information was originally disclosed [60]. Third, even though consent may not be used as legal basis for personal data processing, "ethical" informed consent to research participation should be sought. If this proves impossible due to the amount of people involved and the content is not sensitive, other safeguards may suffice, like a public notice and a visible, user-friendly way to opt-out from the study. Fourth, it is challenging to fully anonymize the content published on social networks (and no, masking usernames does not count as anonymization) as it can be easily traced to its authors. Moreover, full anonymization is at odds with data utility and integrity. Pseudonymization, on the other hand, enables research participants to exercise their data rights (e.g., demand the exclusion of their data from analysis) and to be contacted in case of republication of their posts. However, it is less risky and cumbersome to only publish aggregate data without verbatim quotes. Fifth, as data are only pseudonymized, a number of additional security measures should be taken, like encryption, access control, etc. As a conclusion, before starting social media data collection, research scientists may want to ponder whether this is absolutely necessary and proportionate to their

[12] https://www.misp-project.org/.

research goals. Although we start to see the light at the end of the ethico-legal maze, there are still a number of questions we need to address to continue carrying out research on social media data, whilst solutions to make legal and ethical compliance less demanding are lacking.

Acknowledgments This work has been partially supported by the Luxembourg National Research Fund (FNR)—IS/14717072 "Deceptive Patterns Online (Decepticon)" and the H2020-EU grant agreement ID 956562 "Legally-Attentive Data Scientists (LeADS)". We thank the Data Protection Officer, the legal team and the Ethics Review Panel of the University of Luxembourg for their support. We would also like to acknowledge Maria Botes, Xengie Doan, Rossana Ducato and Soumia Zohra El Mestari for their valuable feedback on an earlier draft of this article and for some of the ideas appearing in this version. Lastly, a great thanks to all Twitter users posting about dark patterns.

References

1. ACM Publications Board: ACM Publications Policy on Research Involving Human Participants and Subjects (Aug 2021), https://www.acm.org/publications/policies/research-involving-human-participants-and-subjects
2. Adams, T.E., Ellis, C., Jones, S.H.: Autoethnography. The International Encyclopedia of Communication Research Methods p. 1–11 (2017), https://onlinelibrary.wiley.com/doi/abs/10.1002/9781118901731.iecrm0011
3. ALLEA—All European Academies: European Code of Conduct for Research Integrity. ALLEA—All European Academies, Berlin (2017), https://www.allea.org/wp-content/uploads/2017/05/ALLEA-European-Code-of-Conduct-for-Research-Integrity-2017.pdf
4. Article 29 Data Protection Working Party: Opinion 05/2014 on Anonymisation Techniques (2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
5. Article 29 Data Protection Working Party: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (Oct 2017), https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711
6. Article 29 Data Protection Working Party: Guidelines on Transparency under Regulation 2016/679, 17/EN WP260 rev.01 (Apr 2018), https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025
7. Beninger, K., Fry, A., Jago, N., Lepps, H., Nass, L., Silvester, H.: Research using Social Media; Users' Views. NatCen Social Research (2014), https://www.natcen.ac.uk/media/282288/p0639-research-using-social-media-report-final-190214.pdf
8. Bishop, L., Gray, D.: Ethical challenges of publishing and sharing social media research data. In: Woodfield, K. (ed.) Advances in Research Ethics and Integrity, vol. 2, p. 159–187. Emerald Publishing Limited (Dec 2017), https://www.emerald.com/insight/content/doi/10.1108/S2398-601820180000002007/full/html
9. Bongard-Blanchy, K., Rossi, A., Rivas, S., Doublet, S., Koenig, V., Lenzini, G.: I am definitely manipulated, even when I am aware of it. It's ridiculous!—Dark Patterns from the End-User Perspective. Proceedings of ACM DIS Conference on Designing Interactive Systems (2021)
10. Boush, D.M., Friestad, M., Wright, P.: Deception In The Marketplace: The Psychology of Deceptive Persuasion and consumer self-protection. Routledge, first edition edn. (2009)
11. Buttarelli, G.: The EU GDPR as a clarion call for a new global digital gold standard. International Data Privacy Law **6**(2), 77–78 (May 2016)
12. Carpenter, P.: Transformational security awareness: What neuroscientists, storytellers, and marketers can teach us about driving secure behaviors. John Wiley & Sons (2019)

13. Cialdini, R.B.: Influence: The Psychology of Persuasion. Harper Business (2006)
14. Cool, A.: Impossible, unknowable, accountable: Dramas and dilemmas of data law. Social Studies of Science **49**(4), 503–530 (Aug 2019)
15. Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.H., Metayer, D.L., Tirtea, R., Schiffner, S.: Privacy and Data Protection by Design—from policy to engineering. Tech. rep., arXiv: 1501.03726 (2014), http://arxiv.org/abs/1501.03726
16. Ducato, R.: Data protection, scientific research, and the role of information. Computer Law & Security Review **37**, 105412 (Jul 2020)
17. Ducato, R., Strowel, A.M.: Ensuring text and data mining: Remaining issues with the EU copyright exceptions and possible ways out. European Intellectual Property Review **43**(5), 322–337 (2021)
18. Duncan, A., Joyner, D.A.: With or Without EU: Navigating GDPR Constraints in Human Subjects Research in an Education Environment. In: Proceedings of the Eighth ACM Conference on Learning @ Scale. p. 343–346. ACM (Jun 2021), https://dl.acm.org/doi/10.1145/3430895.3460984
19. Ethics Review Panel, Animal Experimentation Ethics Committee, Legal Affairs Office: Research ethics guidelines (2017), shorturl.at/nHRV1
20. European Data Protection Board: Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (2019), https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf
21. European Parliament and Council of the European Union: Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe—the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013 (Text with EEA relevance). OJ L 170 (Dec 2021)
22. European Union Agency for Cybersecurity (ENISA): Pseudonymisation techniques and best practices. Recommendations on shaping technology according to data protection and privacy provisions. ENISA (Nov 2019), https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices
23. Fernandes, N., Dras, M., McIver, A.: Generalised Differential Privacy for Text Document Processing, Lecture Notes in Computer Science, vol. 11426, pp. 123–148. Springer International Publishing (2019). https://doi.org/10.1007/978-3-030-17138-4, http://link.springer.com/10.1007/978-3-030-17138-4
24. Ferreira, A., Coventry, L., Lenzini, G.: Principles of Persuasion in Social Engineering and Their Use in Phishing. In: Human Aspects of Information Security, Privacy, and Trust (HAS 2015), Lecture Notes in Computer Science, vol. 90. Springer, Cham (2015)
25. Fiesler, C., Beard, N., Keegan, B.C.: No robots, spiders, or scrapers: Legal and ethical regulation of data collection methods in social media terms of service. Proceedings of the International AAAI Conference on Web and Social Media **14**, 187–196 (May 2020)
26. Fiesler, C., Proferes, N.: "Participant" Perceptions of Twitter Research Ethics. Social Media + Society **4**(1) (2018)
27. Governance Team Sage Bionetworks: The Elements of Informed Consent. A Toolkit V3.0. Tech. rep., Sage Bionetworks (July 2019), https://sagebionetworks.org/wp-content/uploads/2019/07/SageBio_EIC-Toolkit_V2_17July19_final.pdf
28. Gray, C.M., Kou, Y., Battles, B., Hoggatt, J., Toombs, A.L.: The dark (patterns) side of UX design. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems—CHI '18. p. 1–14. ACM Press (2018), http://dl.acm.org/citation.cfm?doid=3173574.3174108
29. Hintze, M.: Viewing the gdpr through a de-identification lens: a tool for compliance, clarification, and consistency. International Data Privacy Law **8**(1), 86–101 (Feb 2018)
30. IBM: What is Text Mining? (last visit October 2021), https://www.ibm.com/cloud/learn/text-mining
31. Information Commissioner Officer (ICO): Guide to the UK General Data Protection Regulation (UK GDPR) (last visit October 2021), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

32. Jin, G., Tu, M., Kim, T.H., Heffron, J., White, J.: Game based cybersecurity training for high school students. In: Proceedings of the 49th ACM Technical Symposium on Computer Science Education. p. 68–73. ACM (Feb 2018). https://doi.org/10.1145/3159450.3159591, https://dl.acm.org/doi/10.1145/3159450.3159591
33. Kennedy, H.: What Should Concern Us About Social Media Data Mining? Key Debates, pp. 41–66. Palgrave Macmillan UK (2016). https://doi.org/10.1057/978-1-137-35398-6, http://link.springer.com/10.1057/978-1-137-35398-6
34. Kumari, A.: Measures Necessary for Scraping and Processing Social Media Personal Data: Technical, Ethical, Legal Challenges and possible Solutions. Ph.D. thesis, Université du Luxembourg (Aug 2021)
35. Kuyumdzhieva, A.: General Data Protection Regulation and Horizon 2020 Ethics Review Process: Ethics Compliance under GDPR. Bioethica **5**(11), 6–12 (Jul 2019)
36. Leiser, M.R.: "Dark Patterns": The Case for Regulatory Pluralism. SSRN Repository (Jun 2020), https://papers.ssrn.com/abstract=3625637
37. Lindén, K., Kelli, A., Nousias, A.: To ask or not to ask: Informed consent to participate and using data in the public interest. In: Proceedings of CLARIN Annual Conference 2019. p. 56–60. CLARIN ERIC (2019)
38. Marres, N., Weltevrede, E.: SCRAPING THE SOCIAL?: Issues in live social research. Journal of Cultural Economy **6**(3), 313–335 (Aug 2013)
39. Mathur, A., Kshirsagar, M., Mayer, J.: What makes a dark pattern. . . dark?: Design attributes, normative considerations, and measurement methods. In: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. p. 1–18. ACM (May 2021), https://dl.acm.org/doi/10.1145/3411764.3445610
40. Mészáros, J., Ho, C.h.: Big Data and Scientific Research: The Secondary Use of Personal Data under the Research Exemption in the GDPR. Hungarian Journal of Legal Studies **59**(4), 403–419 (Dec 2018)
41. Narayanan, A., Shmatikov, V.: De-anonymizing social networks. In: 2009 30th IEEE Symposium on Security and Privacy. p. 173–187 (May 2009)
42. Nissenbaum, H.: Privacy as contextual integrity. Washington Law Review **79**(1), 119–158 (2004)
43. Oates, J., Carpenter, D., Fisher, M., Goodson, S., Hannah, B., Kwiatkowski, R., Prutton, K., Reeves, D., Wainwright, T.: BPS Code of Human Research Ethics. Tech. rep., The British Psychological Society (Apr 2021), https://www.bps.org.uk/sites/bps.org.uk/files/Policy%20-%20Files/BPS%20Code%20of%20Human%20Research%20Ethics.pdf, iSBN 978-1-85433-792-4
44. Parameswaran, M., Whinston, A.B.: Social Computing: An Overview. Communications of the Association for Information Systems **19** (2007)
45. Pormeister, K.: Genetic data and the research exemption: is the gdpr going too far? International Data Privacy Law **7**(2), 137–146 (May 2017)
46. Proferes, N.: Information flow solipsism in an exploratory study of beliefs about twitter. Social Media + Society **3**(1) (Jan 2017)
47. Proferes, N., Jones, N., Gilbert, S., Fiesler, C., Zimmer, M.: Studying reddit: A systematic overview of disciplines, approaches, methods, and ethics. Social Media + Society **7**(2) (2021)
48. Pupillo, L., Ferreira, A., Varisco, G.: Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges. CEPS (2018)
49. Reynolds, E.: Psychologists Are Mining Social Media Posts For Mental Health Research — But Many Users Have Concerns. Research Digest (Jun 2020)
50. Rossi, A., Ducato, R., Haapio, H., Passera, S.: When design met law: Design patterns for information transparency. Droit de la Consommation = Consumenterecht: DCCR **122–123**(5), 79–121 (2019)
51. Rossi, A., Lenzini, G.: Transparency by design in data-informed research: A collection of information design patterns. Computer Law & Security Review **37** (2020)
52. Rossi, A., Arenas, M.P., Kocyigit, E., Hani, M.: Challenges of protecting confidentiality in social media data and their ethical import. In: 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 554–561. IEEE (2022).

https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9799350&casa_token=H9cTFNoGQMQAAAAA:waCDkAbaVeuseLSDt5lHFa9PMY5LKD3BFVYZviWPLVHECCtKfLTWmKYQrwevIh6L0dpzov_1Cyru&tag=1
53. Schaub, F., Balebako, R., Durity, A.L., Cranor, L.F.: A design space for effective privacy notices. In: Eleventh Symposium On Usable Privacy and Security (SOUPS 2015). p. 1–17 (2015)
54. Stallings, W.: Operating system security. John Wiley & Sons, Incorporated (2014)
55. Thornley, C., McLoughlin, S., Murnane, S.: "At the round earth's imagined corners": the power of Science Fiction to enrich ethical knowledge creation for responsible innovation. In: Proc. of 22nd European Conference on Knowledge Management, ECKM 2021 (2021)
56. Townsend, L., Wallace, C.: Social Media Research: a Guide to Ethics. Tech. rep., University of Aberdeen (2016)
57. Townsend, L., Wallace, C.: The Ethics of Using Social Media Data in Research: A New Framework. In: Woodfield, K. (ed.) The Ethics of Online Research, Advances in Research Ethics and Integrity, vol. 2, p. 189–207. Emerald Publishing Limited (Jan 2017), https://doi.org/10.1108/S2398-601820180000002008
58. Tripathy, B.K.: De-anonymization techniques for social networks. In: Dey, N., Borah, S., Babo, R., Ashour, A.S. (eds.) Social Network Analytics, p. 71–85. Academic Press (Jan 2019), https://www.sciencedirect.com/science/article/pii/B9780128154588000049
59. Vitak, J., Proferes, N., Shilton, K., Ashktorab, Z.: Ethics regulation in social computing research: Examining the role of institutional review boards. Journal of Empirical Research on Human Research Ethics **12**(5), 372–382 (Dec 2017)
60. Vitak, J., Shilton, K., Ashktorab, Z.: Beyond the Belmont principles: Ethical challenges, practices, and beliefs in the online data research community. In: Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing. p. 941–953. ACM (Feb 2016)
61. Williams, M.L., Burnap, P., Sloan, L., Jessop, C., Lepps, H.: Users' views of ethics in social media research: Informed consent, anonymity, and harm. In: Woodfield, K. (ed.) Advances in Research Ethics and Integrity, vol. 2, p. 27–52. Emerald Publishing Limited (Dec 2017), https://www.emerald.com/insight/content/doi/10.1108/S2398-601820180000002002/full/html
62. Working Party on Internet-mediated Research: Ethics Guidelines for Internet-mediated Research. The British Psychological Society (2021), https://www.bps.org.uk/sites/www.bps.org.uk/files/Policy/Policy%20-%20Files/Ethics%20Guidelines%20for%20Internet-mediated%20Research.pdf
63. Zimmer, M., Proferes, N.J.: A topology of twitter research: disciplines, methods, and ethics. Aslib Journal of Information Management **66**(3), 250–261 (Jan 2014)
64. Zook, M., Barocas, S., boyd, d., Crawford, K., Keller, E., Gangadharan, S.P., Goodman, A., Hollander, R., Koenig, B.A., Metcalf, J., et al.: Ten simple rules for responsible big data research. PLOS Computational Biology **13**(3), e1005399 (Mar 2017)