HOW DATA CAN BE USED AGAINST PEOPLE: A CLASSIFICATION OF PERSONAL DATA MISUSES

A PREPRINT

Jacob Leon Kröger
Technische Universität Berlin
Weizenbaum Institute for the Networked Society
Hardenbergstraße 32, 10623 Berlin
kroeger@tu-berlin.de

Milagros Miceli
Technische Universität Berlin
Weizenbaum Institute for the Networked Society
Hardenbergstraße 32, 10623 Berlin
m.miceli@tu-berlin.de

Florian Müller
Universität Kassel
Faculty of Social Sciences
Nora-Platiel-Str. 5, 34109 Kassel
florian.mueller@uni-kassel.de

December 30, 2021

ABSTRACT

Even after decades of intensive research and public debates, the topic of data privacy remains surrounded by confusion and misinformation. Many people still struggle to grasp the importance of privacy, which has far-reaching consequences for social norms, jurisprudence, and legislation. Discussions on personal data misuse often revolve around a few popular talking points, such as targeted advertising or government surveillance, leading to an overly narrow view of the problem. Literature in the field tends to focus on specific aspects, such as the privacy threats posed by 'big data', while overlooking many other possible harms. To help broaden the perspective, this paper proposes a novel classification of the ways in which personal data can be used against people, richly illustrated with real-world examples. Aside from offering a terminology to discuss the broad spectrum of personal data misuse in research and public discourse, our classification provides a foundation for consumer education and privacy impact assessments, helping to shed light on the risks involved with disclosing personal data.

Keywords Privacy · Data protection · Personal data · Surveillance · Discrimination · Harms · Consequences

1 Introduction

The protection of personal data is a highly controversial issue. While scores of researchers, activists and politicians advocate the right to informational privacy and stress the importance of comprehensive data protection laws [1, 2, 3, 4], others argue against strong legal restrictions, pointing to the wide-ranging benefits of data collection and use [5, 6, 7]. Many people, asserting they have "nothing to hide" [8], even dismiss the importance of data protection altogether, believing that privacy only truly matters for those on the wrong side of law. While the nothing-to-hide argument has long been exposed as misguided [9, 10], it is not only held by ordinary citizens but also backed by some of the most powerful organizations on earth, including governments and multinational corporations.

During his time as Google's CEO, Eric Schmidt notoriously stated, "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place" [11]. Following the same reasoning, the British government chose the campaign slogan "If you've got nothing to hide, you've got nothing to fear" to promote a nation-wide CCTV surveillance program [4]. As these examples illustrate, the various ways in which privacy invasions can cause harm to law-abiding citizens are often ignored, underestimated or even deliberately concealed. As a result, many people, including court members, struggle to articulate why the protection of personal data is important [12]. This state of misinformation has severe consequences on policy and public discourse, with data protection advocates being referred to as "privacy alarmists" [13] and privacy itself being framed as "old-fashioned[,] antiprogressive, overly costly" [1] and "primarily an antiquated roadblock on the path to greater innovation" [14]. This widespread sentiment also helps legitimize and perpetuate current privacy laws, which are riddled with loopholes and fail to consistently safeguard people from harmful, abusive and ethically questionable data practices [15, 16, 17].

In the face of these challenges, researchers have called for a closer examination and better understanding of the actual harms that can result from the disclosure and processing of personal data. In this vein, Solove argues that "Privacy is far too vague a concept to guide adjudication and lawmaking, as abstract incantations of the importance of 'privacy' do not fare well when pitted against more concretely stated countervailing interests" [18]. Along these lines, many theorists have made attempts to convey the importance of privacy protection by presenting categories and real-life examples of personal data misuse. Some notable examples are the "Data Harm Record" by the Data Justice Lab [19], an "Inventory of Risks and Harms" provided by the Centre for for Information Policy Leadership [20] and Wolfie Christl's extensive work on corporate surveillance in everyday life [21, 22]. Furthermore, scholars have written several essays on the societal values related to and protected by informational privacy (e.g., [1, 3, 4]) with Magi, for example, providing a list of "fourteen reasons privacy matters" [2].

Existing classifications often focus on data practices of companies, on novel privacy threats posed by big data technologies and/or specific categories of harm resulting from personal data use (e.g., bodily harm, loss of liberty, financial loss, reputational harm). What seems to be lacking thus far, however, is a general classification of the possible *actions* that lead to these harms – in other words: a classification capturing the manifold ways in which personal data can be *used* against people, by criminal, private, public and governmental organizations, or by other individuals.

In an attempt to fill the identified gap, this paper proposes a classification scheme of personal data misuses.[1] As previous work has stated, taxonomies comprise subjective social, technical, and political choices [23]. Classifications (ours included) are always normative attempts to "impose order onto an undifferentiated mass" [24]. While we acknowledge the subjective character of our endeavor, we also strive for a holistic overview and see value in creating a structured classification of the possible ways in which personal data can be weaponized. We argue that without a comprehensive and clear overview, many potential paths of harm can easily be overlooked in privacy impact assessments and public discourse, leading to an overly narrow view of the problem. This paper is based on extensive literature research, including previous investigations and press articles, as well as discussions among the three authors and, occasionally, advisors and fellow researchers throughout many months until reaching theoretical saturation [25]. Our classification scheme comprises the following eleven categories:

1. **Consuming data for personal gratification** – Section 2.1
2. **Generating coercive incentives** – Section 2.2
3. **Compliance monitoring** – Section 2.3
4. **Discrediting** – Section 2.4
5. **Assessment and discrimination** – Section 2.5
6. **Identification of personal weak spots** – Section 2.6
7. **Personalized persuasion** – Section 2.7
8. **Locating and physically accessing the data subject** – Section 2.9
9. **Contacting the data subject** – Section 2.8
10. **Accessing protected domains or assets** – Section 2.10
11. **Reacting strategically to actions or plans of the data subject** – Section 2.11

While we acknowledge that a holistic exploration of the topic is particularly important in view of the rapid proliferation of data-based services and the accompanying rise of governmental and corporate mass surveillance [16], the focus of this paper is not limited to the domain of big data, nor even to the digital domain. The classification is meant to be universally applicable, independent of how the data was obtained (e.g., online or offline, legally or illegally, collected or inferred, with or without the knowledge of the data subject), who causes the threat (e.g., individual person, corporation,

[1] While the eleven categories of data use were included because they have the potential to cause harm, this is not always the case. In fact, depending on the context, many of the data uses listed can be beneficial for both the data subject and society at large, as will be further discussed in Sect. 3.2.

organized crime group, intelligence agency)[2] and what motivations lie behind it (e.g., financial gain, political objectives, revenge). These parameters will only be included in examples for illustrative purposes.

As even de-identified data has the potential to cause harm to individuals (cf. Sect. 3.2), we chose to adopt a very broad understanding of "personal data" for the purpose of this classification. While privacy law usually applies to information relating to an identified or identifiable natural person (e.g., Art. 4 GDPR), our proposed classification may apply to any information that is, or once was, personal data according to the above definition, including even anonymized data – as long as it still has the potential to cause or facilitate harm against the data subject.

The remainder of this paper is structured as follows. Section 2 presents the eleven identified categories of personal data misuse. Section 3 then explains the utility of the classification scheme and discusses its scope and limitations. Section 4 concludes the paper.

2 Data Misuse Classification

In this section, we present our classification scheme, which comprises eleven categories of personal data misuse.[1] For each of these categories, we will give a short general description and then provide two or three illustrative examples.

Note that the categories are *not* meant to be mutually exclusive, meaning that multiple categories can apply to one instance of data misuse simultaneously. However, the classification scheme is intended to be exhaustive in the sense that all types of personal data misuse should fit into *at least one* of the eleven categories.

2.1 Consuming Data for Personal Gratification

Description: Someone consumes footage of the data subject to gain pleasure or satisfaction (e.g., motivated by curiosity, boredom or sexual desire) without the data subject's consent.

Examples:

- **Ridicule.** Embarrassing footage, such as images or videos showing a person intoxicated, behaving clumsily or having an accident, can be used to amuse oneself at the depicted person's expense. A common example is the consumption of "fail videos", which are intended to amuse their viewers by specifically showing other people's misfortunes, sometimes involving scenes of serious pain and agony [26]. Learning that one has become the target of ridicule on social media can be a deeply humiliating experience [27].
- **Voyeurism.** Intimate footage, such as images or videos showing a person undressing, using the bathroom or engaging in sexual activity, can be exploited for voyeuristic purposes and sexual gratification. Although perpetrators can also observe their unsuspecting subjects of interest directly (e.g, by spying through a peephole) and are therefore not necessarily dependent on recordings, cameras and other electronic devices can significantly facilitate voyeurism and are widely used for this purpose. Across the globe, countless hidden spy cameras have been discovered in public toilets [28], hotel rooms [29] and changing booths [30]. Video voyeurism is considered a sex crime in many countries, with convicted people having been registered as sex offenders and sent to prison [31]. In the case of cyberstalking, the spying can even take place purely via the internet, for example by scanning a target's social media profile or gaining unauthorized access to his or her personal cloud storage.

2.2 Generating Coercive Incentives

Description: Someone uses personal data to choose or create effective incentives for motivating the data subject to behave in a desired manner. Personal data can fulfill two possible functions here: (1) Information about a person's character and personal circumstances (e.g., fears, needs, preferences) can help identify rewards and sanctions with a strong incentive effect on that particular person. (2) As evidenced by the remainder of this paper, personal data can be used in many harmful ways and thus be used to threaten or blackmail the data subject.

Examples:

- **Threats of physical violence.** Those who can track down and thus physically attack a person (cf. Sect. 2.9) can use this capability as a means of pressure against him or her, as is well illustrated by the classic threat "I know where you live". Threats of physical violence are not only often expressed against corporate figures, celebrities and politicians [32] but are also widespread among the general public, such as in schools or workplaces [33]. Realizing such a threat always requires the ability to locate the victim.

[2] The only exception is the first category (Sect. 2.1), which refers to "personal gratification" and therefore only includes actions taken by natural persons.

- **Personalized rewards.** When trying to persuade a person through rewards, information about his or her individual preferences and needs can be exploited to select the most effective incentives. Among methods for employee motivation, for example, a trend can be observed from standardized towards highly personalized rewards [34]. Personalized incentives are also increasingly used to encourage consumers to purchase specific products [35, 36] and to improve patient compliance in medical interventions [37]. As for the motivation of employees, consumers and patients, knowledge about the wants and needs of individuals can also be used for illegal purposes. To successfully bribe a person, for instance, it would obviously be very helpful to know in advance if he or she is receptive to the offered "gift".
- **Personalized sanctions.** When trying to induce a desired behavior in a person by way of threatening sanctions in case of non-compliance, information about his or her fears, needs and vulnerabilities (cf. Sect. 2.6) can be used to identify the most effective threat. To erode prisoners' resistance to questioning, for instance, their personal weaknesses are often exploited in criminal and military interrogations [38]. For the purpose of determining the psychological and cultural vulnerabilities of individual detainees (e.g., phobias, personality features, religious beliefs), modern-day torture prisons – including some operated by Western democracies – sometimes resort to personal medical records, although this is strictly prohibited according to general medical ethics and the Geneva Conventions [39]. Where information about a person's social circle is available, it is also possible to threaten with harming his or her loved ones.
- **Blackmail.** Access to embarrassing or damaging information about a person (e.g., nude photos, sex tapes, drug habits, past misdemeanors) can be used to threaten him or her with revealing the information to third parties or even the public (cf. Sect. 2.4) if certain demands are not met. Shame and fear of reputational destruction can be powerful motivators. An example that gained widespread media attention is "sextortion", a form of blackmail where criminals threaten victims to post stolen intimate photos of them on social media unless they obey certain commands given to them. Some documented cases of sextortion have even led to affected victims committing suicide [40].

2.3 Compliance Monitoring

Description: When incentive systems are installed to ensure that people adhere to certain rules, some sort of surveillance is typically applied to detect behavior worthy of reward or punishment. While empty threats or promises and the mere feeling of being watched can of course also influence people's behavior [41, 42, 43], only the actual observation of people's behavior makes it possible to check for their compliance and implement incentive systems consistently.

Examples:

- **Political oppression.** It is a typical strategy of authoritarian regimes to silence their opposition and break political resistance through strict systems of punishment and incentives, as famously allegorized in George Orwell's dystopian novel Nineteen Eighty-Four [44]. Today, governments have a wide range of surveillance technologies at their disposal to monitor compliance with their laws and rules, including CCTV cameras, internet tracking tools, wiretapping methods, and spyware. Several nations have been accused of specifically spying on human rights activists, journalists and opposition politicians using cellphone malware [45, 46, 47]. Such surveillance tools make it possible for governments to apply incentives and sanctions to people's compliance behavior, which can range from fines, arrests, beatings or death penalties over all sorts of rewards to increasing or lowering a target's ranking in a national scoring system [48].
- **Domestic abuse.** Connected devices play an increasingly important role in intimate partner violence by allowing perpetrators to remotely track and surveil their oppressed victims in various new ways. To isolate their victims and monitor compliance with imposed rules (e.g., no contact with other men, no leaving the house without permission), violent partners can not only resort to GPS tracking, social media stalking and CCTV monitoring, but may also employ advanced surveillance technologies, such as smartphone spyware capable of monitoring outgoing calls, texts and emails [49].
- **Workplace surveillance.** Employers have an expansive range of technologies at their disposal to track staff behavior, work intensity and productivity [21]. Surveillance tech providers offer tools to monitor the email traffic, keystrokes, web browsing patterns, phone calls, social media posts, and even private instant messages of individual employees [50]. For example, email content can be scanned for trigger words like "résumé" to detect when employees are planning to leave a company [51]. New and more intrusive technologies, such as wristband trackers, microchip implants and brain-scanning hats, enable organizations to monitor emotions, fatigue and stress among their personnel [52]. Some employers even use military-grade surveillance tools against their staff that were originally developed for the Pentagon and the CIA to be used against terrorists in Iraq and Afghanistan [53].

2.4 Discrediting

Description: Personal data is shared in ways that cause legal and/or reputational harm to the data subject. The latter refers not exclusively to the subject's overall societal standing but also to his or her respect and esteem held by friends, family members, employers, colleagues and other direct social contacts.

Examples:

- **Publication of nude pictures and sex tapes.** A common means of public humiliation, which often has serious consequences, is the release of images or videos showing the victim in an intimate situation. TV sports commentator Erin Andrews, for example, was filmed through peepholes while changing clothes in a hotel room and thereby exposed to over 16 million viewers on the internet [54]. Various celebrities suffered a similar experience when their private photos, many containing nudity, were distributed online following the iCloud leaks in 2014 [55]. Another example is "revenge porn", which refers to sexually explicit media recorded in an intimate relationship and later disclosed to the public to embarrass a former parter [56]. To maximize the damage, revenge porn has often been published along with the victims full name, city of residence, profession, and social-media profile [57]. Leakage of nude pictures and sex tapes have led not only to massive reputational harm, public outrage and destroyed careers, but also to serious mental health consequences and even suicides [58].
- **Political discrediting tactics.** Information that casts a poor light on individual activists, political candidates or public officials can be released to undermine their reputation, credibility and political influence. Not only election campaigns and authoritarian regimes, but also private companies and public authorities in modern democracies have attempted to use negative personal information to discredit their critics and opponents. Well-known examples include General Motor's actions against car safety activist Ralph Nader [59], the COINTELPRO scandal, where US law enforcement agencies illegally infiltrated and discredited anti-war and civil-rights organizations [60], and the publication of Martin Luther King's extramarital affairs by the FBI [18].
- **Legal evidence.** Those who possess evidence of a person's unlawful conduct can disclose it to law enforcement authorities or use it against him or her in court. For example, many technology companies collect large amounts of rich and varied data about their customers which can potentially reveal their personal failures and offences. Among other pieces of personal data, private emails [61], audio files recorded by Amazon's smart assistant Alexa [62], health and activity data from wearable fitness trackers [63] and detailed location histories from Google timeline [64] were already requested as evidence by law enforcement. In 2019 alone, Google was requested to disclose data from over 340,000 user accounts to authorities [65]. While the production of evidence is obviously important to a functioning legal system, excessive surveillance can undermine civil liberties [10]. As Aleksandr Solzhenitsyn noted: "Everyone is guilty of something or has something to conceal. All one has to do is look hard enough to find what it is" [66].

2.5 Assessment and Discrimination

Description: Personal data is used to evaluate people according to certain criteria or to classify them into certain groups, based on which they are subsequently treated.

Examples:

- **Identification of political opponents.** On the basis of their actions and expressed attitudes, people can be identified as opponents to specific political movements, governments, or individual politicians. A person's social media activities and cellphone location, for example, can reveal his or her participation in a particular street protest [67, 68]. In some countries, authorities combine vast amounts of data on individual citizens, including medical records, travel bookings, online purchases, social media comments, location data and even information on interpersonal relationships in order to identify people who act against the government's interests [69] and are "suspected of politically sensitive activity" [70]. Private companies from Western democracies have already helped authoritarian states in identifying and persecuting their critics. Yahoo, for instance, provided a foreign government with email records of two dissident journalists, who were subsequently sentenced to ten years in prison [71].
- **Discriminatory hiring practices.** A wide and growing range of personal data is being consulted for recruitment decisions, including biometric information, health details and social media data [21, 22], often resulting in discriminatory and unlawful hiring practices [72]. There is a whole industry of employment screening companies offering detailed background reports on individual job applicants to employers [22].
- **Discriminatory provision of goods and services.** Profiling information on potential customers can enable firms to adjust the prices and availability of their offerings in order to maximize their profit and avoid low-value

customers. Where information about a customer's income or net worth are available, for example, it is possible to personalize product prices according to his or her spending capacity ("price discrimination") [73]. Similarly, personal risk factors and other background information can be used by companies to adjust a person's insurance premiums [74] and to reject his or her credit or rental applications. For all these purposes, highly intimate personal data is regularly used. For instance, some firms offer credit scorings based on people's likes and posts on social media, club and subscription activity, GPS location data, shopping habits, and online behvioral analytics, including invidual mouse clicks and information on how quickly loan applicants scroll through certain websites [75]. In 2015, Facebook even filed a patent to assess a person's creditworthiness based on his or her circle of friends [76].

2.6 Identification of Personal Weak Spots

Description: Personal data is screened for vulnerabilities (e.g., physical, psychological, financial, social) to be able to harm the data subject effectively and/or stealthily.

Examples:

- **Torture.** In order to inflict the greatest possible pain on a human being, it can be helpful to know his or her personal vulnerabilities and fears (e.g., claustrophobia, fear of isolation, cultural sensitivities). In torture prisons, for example, medical and psychological assessments are sometimes used to identify weak spots of individual detainees [39, 77]. Similarly, in psychological warfare, personal weaknesses can be exploited to strategically destroy the morale of enemies. For instance, secret police in the German Democratic Republic created psychograms of individual political dissidents to identify effective ways of depressing their psychological states [78]. Knowledge about physical vulnerabilities, such as illnesses, allergies, bodily defects or physical substance dependences, can also be exploited to effectively and/or stealthily harm a person. For example, there have been attempts to secretly murder people by withholding live-saving medications [79] or hiding allergens in their food [80].
- **Bullying.** Personal weak spots of classmates or work colleagues (e.g., physical vulnerabilities, illness, anxieties, relationship problems) are often exploited by bullies to torment their victims, causing "devastating mental, physical, and social consequences" [81]. Knowledge about personal sensitivities – and, thus, the ability to trigger strong reactions in their targets – can also help bullies to get away with their attacks, since others may find the victim's reaction incomprehensible or even laughable [82]. Therefore, when fallen into the wrong hands, information about personal weak spots can lead to the data subject being more vulnerable to bullying tactics.
- **Legal vulnerabilities.** Perpetrators who want to harm a person (e.g., through assault, theft or fraud) can benefit from knowledge about the person's level of legal protection. It may be useful to perpetrators, for example, to know whether their victim has a legal expenses insurance, close ties with legal experts, the time and resources for a lengthy court battle and/or the funds to work with a good lawyer. In fact, two of the most common reasons why victims of workplace harassment do not file a complaint are their time constraints and their inability to afford a lawyer [83]. Knowledge of such vulnerabilities can reassure perpetrators that their victim is defenseless and that they are unlikely to face consequences for causing harm to them.

2.7 Personalized Persuasion

Description: A message is targeted and/or tailored based on information about the receiver (e.g., preferences, personality traits, political attitudes, fears) to increase the message's persuasive effect.

Examples:

- **Commercial advertising.** Social networking websites, search engines and online ad networks make extensive use of personal data to target advertising to individual members of their audience [84, 85, 86]. For example, in "behavioral targeting", ads are served based on people's previous online activity and browsing behavior [87]. Empirical research has shown that ad targeting based on people's smallest expressions of preference, such as a single "like" on Facebook, can already result in an effect of mass psychological persuasion [88]. Marketers can also target ads based on lifestyle characteristics, demographics (e.g., sex, age, income, employment status) and real-time location [84] or even emotions and mental states, such as when people are sad or fearful [89] or feel less attractive [90]. Furthermore, as people tend to be more receptive to ads when they feature people who resemble themselves, algorithms are being developed to automatically mimic facial characteristics of target individuals [35]. Information about people's attitudes and behavior can be used as real-time feedback to incrementally fine-tune and improve algorithms until they show the deserved manipulative effect [91].

- **Political campaigns.** Like commercial advertisers, political parties are increasingly making use of online personalization techniques to boost the effectiveness of their campaign ads [22], which has been recognized as a threat to voter self-determination and democracy at large [92]. This issue became a focus of public debate when, after the 2016 US presidential election, consulting firm Cambridge Analytica was accused of influencing voter opinions using detailed personal data harvested from millions of Facebook accounts [93]. Based on individual psychographic profiles derived from the Facebook data, undecided voters were served ads designed to "target their inner demons", as the whistleblower Christopher Wylie described [94]. Empirical research indicates that personalized political advertising can have a significant effect on the electoral behavior of individuals [95].
- **Social engineering attacks.** In a common fraud scheme known as "phishing" or "social engineering", cybercriminals send deceptive messages to their victims, prompting them to reveal sensitive information, such as usernames, passwords and credit card details [96]. Where insights about the receiver are available, phishing messages can be personalized to attract more attention or deceptively signal trustworthiness – and thereby increase the overall effectiveness of the attack [97]. Phishing can not only hit private individuals, but through their employees also major corporations, such as Google and Facebook [98], and governmental institutions, such as the White House [99]. Interpol classifies social engineering as one of the world's emerging fraud trends [100], with human influenceability recognized as the weakest link in the computer security chain [101].

2.8 Contacting the Data Subject

Description: Contact information (e.g., e-mail address, phone number, mail address, social media account, videoconferencing ID) is exploited to send unsolicited objects or messages to a person.

Examples:

- **Fraudulent messages and unsolicited advertising.** Companies and criminals can exploit contact details to unsolicitedly contact a person for commercial or fraudulent purposes. While there have been legislative approaches to bring the issue under control [102], unsolicited advertising remains a widespread phenomenon, with commercial spam messages making up roughly half of the global email traffic [103]. Besides advertisement, electronic messages may include malware or links to phishing websites [96]. Phone scams are also a widespread threat which may result in people losing their entire life savings [104].
- **Threat messages and letter bombs.** Any type of contact channel can be exploited to threaten and intimidate the message receiver, with some common examples being hate mail, phone treats or insults on social media. Empirical research shows that many people already experience abusive messages at a young age [105]. Not only the content, but also the nature and frequency of contact can be harassing (e.g., repeated phone calls at inconvenient times). Apart from threats of violence, physical parcels and letters can contain dangerous items, such as poison or explosives, with the potential to injure or kill the receiver. For example, a series of package bombs in Texas killed two and seriously injured five in 2018 [106]. In the same year, letter bombs were sent to several critics of the Trump administration [107].
- **Online sexual predation.** Social networking websites, instant messaging apps, online chat rooms and other communication channels can be exploited by sexual predators to lure potential victims. Among internet users, minors face a particularly high risk of being contacted by strangers with dubious intentions [108], which is often underestimated by parents [109]. Even gaming platforms have been exploited for online sex crimes against children [110]. Once a dialogue with their target is established, sexual predators can try to establish an emotional connection ("child grooming"), pressure their victim to engage in sexual activity, or even try to set up in-person meetings. For cases where the target's whereabouts are revealed to an offender and physical contact is established, see Sect. 2.9.

2.9 Locating and Physically Accessing the Data Subject

Description: Personal data is used to track people down and gain direct physical contact to them without their consent.

Examples:

- **Sex crimes.** Insights into the whereabouts of their targets can enable predatory stalkers to prepare and carry out a sexual assault. It could help them to know, for example, at what times the victim is alone in unguarded places. Online stalking – or "cyberstalking" – can evolve into offline stalking when the target's location is revealed to the perpetrator, potentially entailing trespassing and physical assault [111, 112]. With the offender's ability to locate the victim, cyberstalking can even end in murder, as in the case of 15-year-old Carly Ryan from South Australia [113].

- **Religious, racist and political persecution.** Today, as in most of human history, many people are persecuted because of their religious beliefs [114], ethnicity [115], sexual orientation [116] or political affiliation [117]. Information on the hiding place or whereabouts of persecuted individuals can allow their oppressors to track them down for arrest, physical harm or assassination. A historical example is the national census data collected in Nazi Germany, which later helped Hitler's henchmen to locate and deport Jews and other Holocaust victims with horrendous precision [118]. While some persecuted individuals fortunately managed to hide from the Nazis until the end of World War II, modern and ubiquitous surveillance technologies (e.g., CCTV with facial recognition, license plate scanners, GPS tracking) enable today's governmental and non-governmental oppressors to trace their declared enemies with even greater efficiency [119, 120, 121]. A person's location may even be revealed through seemingly non-sensitive data such as photo metadata [122] or smartphone motion sensor readings (even when GPS is turned off) [123].
- **Organized crime.** Information on the whereabouts of their enemies and targets (e.g., members of enemy gangs, targets for contract killing, witnesses of crimes) can enable criminals to find and attack them. For this reason, witness protection programs often involve a relocation of threatened individuals, the strict protection of address data and sometimes even the construction of a whole new identity for witnesses [124]. Like governmental agencies, criminal organizations have started to make use of sophisticated spyware to monitor potential enemies [125]. Even street gangs have been reported to use digital tools to track down deserters across national borders [126].

2.10 Accessing Protected Domains or Assets

Description: Personal data is used to gain access to protected domains and assets of the data subject, such as personal accounts, private property or even the subject's whole identity.

Examples:

- **Social media burglary.** Information about people's whereabouts can be exploited to break into their homes while they are out. As a particular example, there has been a trend for burglars to use information shared online by home owners, such as their holiday plans announced in social media posts – a technique also referred to as "Facebook burglary" [127]. Such incidents have inspired projects like *www.PleaseRobMe.com* to warn people about the risks of online oversharing [128].
- **Identity theft.** Various types of personal data, including dates of birth, passport numbers, Social Security numbers, telephone numbers, Medicare numbers, addresses and financial account numbers, can help criminals to steal people's identities and perform activities in their name, such as opening accounts, making purchases or filing fraudulent tax returns [129, 130]. While identity theft has long been a concern, the number of reported cases has risen sharply in recent years [131]. Leaked passwords and answers to security questions (e.g., mother's maiden name) can be exploited to take over a person's online accounts – not only to enrich oneself financially and to collect more personal data but also to message and potentially threaten other people in the name of the victim. Some common consequences for victims of identity theft are lawsuits, the denial of loans and public benefits, harassment by debt collectors, embarrassment, stress, and anxiety [132]. Emerging forms of identity theft even exploit biometric samples to artificially mimic fingerprints or the voice of a victim in order to impersonate them and deceive biometric authentication mechanisms [133].

2.11 Reacting Strategically to Actions or Plans of the Data Subject

Description: Insights into people's actions and intentions are used to interfere with, preempt, or mitigate their plans.

Examples:

- **Stifling of political resistance.** Today's intelligence agencies and secret services have a rich arsenal of surveillance technologies at their disposal (cf. Sect. 2.3). The ability to secretly track citizens' locations and tap their communication channels can enable authoritarian states, for example, to spy out the plans and movements of their political dissidents [134]. For instance, smartphone spyware can allow regimes to read private chats and emails on infiltrated devices [45, 135]. The Guardian has reported on cases where sophisticated government spyware was deployed to "spy on journalists, activists and anti-graft groups as they worked to highlight [. . .] notorious cases of crime, corruption and abuse of authority" [46]. Whether government critics are preparing an information event, planning a fundraising campaign, organizing civil disobedience or arranging a protest march – any insight into their plans can help the incumbent regime to "expose, disrupt, misdirect, or otherwise neutralize" [136] such efforts by intervening early and strategically.
- **Predictive policing.** Computerized analytical tools for the identification and prediction of potential criminal activity are being developed and, in some places, already regularly used by law enforcement agencies [137].

Advanced AI-based systems to support this so-called practice of "predictive policing" can combine a variety of sensitive personal information and surveillance technologies, such as location tracking, facial recognition and gait analysis, to calculate risk scores for individual citizens and classify them as potential suspects [70]. Apart from the danger that such approaches can lead to discriminatory or biased policing (e.g., over-policing of low-income or minority communities) [138], there is also concern that predictive analytics in law enforcement can lead to wrongful accusations and convictions due to algorithmic errors [139]. A broad coalition of civil rights groups, including the the Electronic Frontier Foundation and the American Civil Liberties Union, has issued a "statement of concern" warning about the dangers of predictive policing, emphasizing its potential to undermine constitutional rights of individuals [140]. While still not very effective [141], predictive policing is an attempt to spy out, predict and thwart people's (criminal) intentions.

- **Forestalling legal action.** Knowledge about a person's plan to take legal action (e.g., criminal complaint, whistleblowing to authorities) can enable the accused party to prepare for a legal battle or to thwart the anticipated threat altogether – for example, by bribing, intimidating, discrediting or otherwise impeding the accuser. When it becomes known to the wrong people that a person holds incriminating evidence or is prepared to appear as a principal witness in court, the person may even be in danger of being preemptively killed, especially in investigations against organized crime groups [142, 143]. In corporate and governmental organizations, where whistleblowing is considered an important mechanism to "unmask certain types of infringements which are particularly harmful to the public interest" [144], surveillance tools can be employed by the management to automatically detect employees with the potential of becoming whistleblowers [145, 146]. One possible red flag could be an employee's "context switching", meaning that the employee asks a colleague to switch to a secure communication channel, such as an encrypted instant messenger or offline face-to-face conversation, "indicating that the subject matter is too risky for the corporate network" [50].

3 Discussion

In the previous section, we have proposed a classification scheme for personal data misuses, illustrating the wide variety of potentially harmful actions that can be enabled and facilitated by obtaining information about individuals. In this section, we will explain its utility by outlining possible applications of the scheme (Sect. 3.1) and then discuss its scope and limitations (Sect. 3.2).

3.1 Utility of the Classification Scheme

By providing a comprehensive answer to the question "in which ways can personal data be used against the data subject?", our proposed classification scheme can serve as a tool and theoretical foundation for privacy impact assessments, helping the assessors to avoid potential blind spots. When gauging which of the eleven classes presented in Sect. 2 are relevant to a given situation, not only the specific types of collected data should be taken into consideration, but also – as far as assessable – the technical capabilities and probable intentions of the respective data controller(s).

Furthermore, our classification scheme (and the examples provided) can be used to educate and raise awareness about potential harms that may result from disclosing personal data to malicious or negligent actors, thus helping people to comprehend an appreciate the importance of privacy protection. In particular, this paper offers a structured response and antithesis to the misguided, yet widespread, nothing-to-hide attitude, which ignores many possible types of personal data misuse [4, 9, 10].

3.2 Scope and Limitations of the Classification Scheme

Given the holistic focus and broad applicability of our classification scheme, there are several points that need to be addressed to clarify its scope and meaning.

First, it is important to recognize that many of the harms and abuses from the examples provided in Sect. 2 can also happen without the responsible party having access to individuals' personal data. For example, incentive systems (Sect. 2.2) as well as marketing and phishing messages (Sect. 2.7) do not need to be personalized to be effective. They can also be selected or designed based on general knowledge about human preferences and psychology, or simply be very effective by chance. Threats like "I know where you live" (Sect. 2.2) can also be effective when the offender making the threat does not, in fact, know how to locate the victim but convincingly pretends to do so. To discredit a person (Sect. 2.4), not only damning evidence and actual personal secrets can be exploited, but – as long as it appears credible to the respective audience – also untrue and fabricated information. To break into a house or gain unauthorized access to a person's user account (Sect. 2.10), perpetrators do not necessarily require information about their victims' login credentials or whereabouts. And even to spread unsolicited advertisements (Sect. 2.7), distributors do not necessarily need to know individuals' specific addresses but can also distribute their messages to randomly chosen or randomly generated email or postal addresses and phone numbers. Nevertheless, having access to personal data can make all these actions easier, safer and much more efficient from the data controller's perspective and – as the examples in Sect. 2 illustrate – can also open up new subforms and paths of harm and exploitation within the proposed categories.

Second, as data pseudonymization and anonymization are commonly applied by data controllers to remove their collected data from the scope of privacy law [22, 147], it should be noted that many of the threats listed in Sect. 2 can also be enabled and facilitated by de-identified data. For example, insights into the browsing behavior of Internet users can be used to personalize incentives (Sect. 2.2), individually tailor persuasive messages (Sect. 2.7) and to treat users differently in terms of service offerings and pricing (Sect. 2.5), even without their real names attached to the data. Furthermore, data anonymization can often be reversed using system backdoors or statistical techniques [148, 149, 150]. Also, as we have explored in previous work, a rich variety of sensitive personal information can be inferred from hidden patterns and correlations in collected data [151], including from "innocuous" and seemingly anonymous sensor data from mobile and wearable devices [123, 152, 153, 154]. Thus, de-identified data must not be left out of consideration when assessing potential harms resulting from data collection and the use of modern technologies – and when designing corresponding technical, organizational, and regulatory safeguards. Rather than focusing on "personal data" per se, the focus should be on harms resulting from data use and on how they can be mitigated.

Third, while all classes of data use presented in Sect. 2 certainly have the potential to cause harm and be ethically indefensible, this is not always the case. In fact, depending on the context and the underlying intentions, many of the data uses described can be beneficial for both the data subject and society at large. Means of compliance monitoring, for example, which can enable political oppression, domestic abuse and intrusive workplace surveillance (cf. Sect. 2.3), can also serve the general public interest (e.g., speed cameras for traffic control, financial transparency obligations to avoid tax evasion, observation of violent criminals). Of course, while the vast majority of people would arguably agree with the framing of the previous sentence, the categorization of data uses into "good" and "bad" is often more complicated. It is ultimately a subjective evaluation, and the lawfulness of data uses depends on the respective legal system. From a societal perspective, evaluating the costs and benefits of data uses requires a complex balancing of interests (e.g., ease of use and affordability of products vs. protection of civil liberties). Under current frameworks of data governance, which are riddled with loopholes and often utterly unfit for purpose [15, 155], it is very important not to equate or confuse "legal" with "socially acceptable". Under the prevailing legal paradigm of privacy self-management, for example, individuals can authorize almost any type of data disclosure and processing without having the slightest clue what exactly they are consenting to [15]. Many data practices flourishing in this legal environment are highly questionable, with large parts of the data economy subsisting on business models frowned upon by the majority of the population, such as behavioral targeting [156]. Recent legal advances, such as EU's new General Data Protection Regulation, have failed to change the fact that "[e]very day, people are confronted with misleading consent requests, uncontrolled tracking and surveillance in online advertising, and large tech firms' uncanny knowledge of their intimate lives" [157].

4 Conclusion

Discussions around the misuse of personal data are often characterized by a narrow understanding of the problem. Public attention is fixed on a few prominent topics and threats, while many other issues of relevance remain largely ignored. To help broaden the view on data privacy, this paper has proposed a holistic classification of the ways in which personal data can be used against people. By illustrating the variety of harmful actions that can be facilitated by the disclosure of personal information, the classification and the real-world examples provided herein may serve as an inspiration for consumer education and privacy impact assessments. The eleven categories of data misuse demonstrate that access to personal information can be a powerful instrument (and sometimes even a necessary precondition) for harming, discriminating, influencing, and oppressing people. Importantly, many of these threats are independent from the victim's law-abidance and may therefore also affect people who supposedly have "nothing to hide". In conclusion, the protection of personal data and the regulation of its use are issues of enormous importance that should concern all of society. The ultimate purpose of personal data protection is not to protect data, but to protect people against the harms resulting from data disclosure and misuse. Of course, our classification scheme represents only one of many possible ways of looking at the value of informational privacy. We hope to inspire fellow researchers to further develop and build upon our work.

References

[1] Julie E Cohen. What privacy is for. *Harv. L. Rev.*, 126:1904, 2012.

[2] Trina J Magi. Fourteen reasons privacy matters: A multidisciplinary review of scholarly literature. *The Library Quarterly*, 81(2):187–209, 2011.

[3] Jeffrey Rosen. Why privacy matters. *The Wilson Quarterly*, 24(4):32–38, 2000.

[4] Daniel J Solove. Why privacy matters even if you have 'nothing to hide'. *Chronicle of Higher Education*, 15, 2011.

[5] Kent Walker. Where everybody knows your name: A pragmatic look at the costs of privacy and the benefits of information exchange. *Stan. Tech. L. Rev.*, page 2, 2000.

[6] Thomas M Lenard and Paul H Rubin. The big data revolution: Privacy considerations. *Technology Policy Institute*, 2013.

[7] Tal Z Zarsky. Incompatible: the gdpr in the age of big data. *Seton Hall L. Rev.*, 47:995, 2016.

[8] Timothy Casey. The Value of Deviance: Understanding Contextual Privacy. *Loyola University Chicago Law Journal*, 51(1):65–105, 2019.

[9] Daniel J Solove. I've got nothing to hide and other misunderstandings of privacy. *San Diego L. Rev.*, 44:745, 2007.

[10] Alex Abdo. You may have 'nothing to hide' but you still have something to fear | american civil liberties union. https://www.aclu.org/blog/national-security/secrecy/you-may-have-nothing-hide-you-still-have-something-fear, 2013. (Accessed on 04/17/2021).

[11] Richard Esguerra. Google ceo eric schmidt dismisses the importance of privacy | electronic frontier foundation. https://www.eff.org/deeplinks/2009/12/google-ceo-eric-schmidt-dismisses-privacy, 2009. (Accessed on 04/22/2021).

[12] Daniel Solove. 10 reasons why privacy mattersy. https://teachprivacy.com/10-reasons-privacy-matters/, 2014. (Accessed on 04/29/2021).

[13] Omri Ben-Shahar. Privacy paranoia: Is your smartphone spying on you? https://www.forbes.com/sites/omribenshahar/2016/07/05/privacy-paranoia-is-your-smartphone-spying-on-you/?sh=49b91e9d7021, 2016. (Accessed on 04/22/2021).

[14] Gordon Hull. Successful failure: What Foucault can teach us about privacy self-management in a world of Facebook and big data. *Ethics and Information Technology*, 17(2):89–101, 2015.

[15] Jacob Leon Kröger, Otto Hans-Martin Lutz, and Stefan Ullrich. The myth of individual control: Mapping the limitations of privacy self-management. *Social Science Research Network (SSRN)*, 2021.

[16] Shoshana Zuboff. *The age of surveillance capitalism*. Profile books, 2019.

[17] Jacob Leon Kröger, Jens Lindemann, and Dominik Herrmann. How do app vendors respond to subject access requests? a longitudinal privacy study on ios and android apps. In *International Conference on Availability, Reliability and Security*, pages 1–10, 2020.

[18] Daniel J Solove. A taxonomy of privacy. *U. Pa. L. Rev.*, 154:477, 2005.

[19] Joanna Redden, Jessica Brand, and Vanesa Terzieva. Data harm record – data justice lab. https://datajusticelab.org/data-harm-record/, 2020. (Accessed on 04/29/2021).

[20] Centre for Information Policy Leadership. Risk, high risk, risk assessments and data protection impact assessments under the gdpr. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf, 2016. (Accessed on 04/29/2021).

[21] Wolfie Christl. Networks of control: A report on corporate surveillance, digital tracking, big data & privacy. Technical report, Cracked Labs, Vienna, 2016.

[22] Wolfie Christl. How companies use data against people. Technical report, Cracked Labs, Vienna, 2017.

[23] Geoffrey C. Bowker and Susan Leigh Star. *Sorting things out: classification and its consequences*. Inside technology. MIT Press, Cambridge, Mass, 1999.

[24] Kate Crawford and Trevor Paglen. Excavating AI: The Politics of Images in Machine Learning Training Sets, September 2019.

[25] Anselm L. Strauss and Juliet M. Corbin. *Basics of qualitative research: techniques and procedures for developing grounded theory*. Sage Publications, Thousand Oaks, 2nd ed edition, 1998.

[26] Megan O'Neill. The Psychology Of Fail Videos. https://www.adweek.com/performance-marketing/fail-videos/, 2010. (Accessed on 04/16/2021).

[27] Emma Pryde. This Is What Happens When You Become a Meme. Vice. https://www.vice.com/en/article/yvwk5j/what-happens-to-people-when-they-become-a-meme-078, 2015. (Accessed on 04/16/2021).

[28] Tiffany May and Su-Hyun Lee. Is There a Spy Camera in That Bathroom? In Seoul, 8,000 Workers Will Check. The New York Times. https://www.nytimes.com/2018/09/03/world/asia/korea-toilet-camera.html, 2018. (Accessed on 04/16/2021).

[29] Sophie Brown. Student Horrified After Finding Hidden Camera In Shower At Travelodge Hotel In Oxford. HuffPost UK. https://www.huffingtonpost.co.uk/2015/09/03/travelodge-spy-camera_n_8082632.html, 2015. (Accessed on 04/16/2021).

[30] Niraj Chokshi. Transgender Woman Is Charged With Voyeurism at Target in Idaho. The New York Times. https://www.nytimes.com/2016/07/15/us/target-transgender-idaho-voyeurism.html, 2016. (Accessed on 04/16/2021).

[31] BBC News. BBC Radio producer jailed over sex tapes. http://news.bbc.co.uk/2/hi/uk_news/england/london/8549608.stm, 2010. (Accessed on 04/16/2021).

[32] J Reid Meloy, Lorraine Sheridan, and Jens Hoffmann. *Stalking, threatening, and attacking public figures: A psychological and behavioral analysis*. Oxford University Press, 2008.

[33] Steve Albrecht. Threat assessment teams: Workplace and school violence prevention. fbi law enforcement bulletin. https://leb.fbi.gov/articles/featured-articles/threat-assessment-teams-workplace-and-school-violence-prevention, 2010. (Accessed on 04/16/2021).

[34] Gaurav Lahiri, Jeff Schwartz, and Erica Volini. Personalized incentives and talent management strategies. deloitte insights. https://www2.deloitte.com/us/en/insights/focus/human-capital-trends/2018/personalized-incentives-talent-management-strategies.html, 2018. (Accessed on 04/16/2021).

[35] Bruce Schneier and Alicia Wanless. Persuasion is essential to society and democracy, but we need new rules governing how big tech companies can harness it. https://foreignpolicy.com/2020/12/11/big-tech-data-personal-information-persuasion/, 2020. (Accessed on 04/16/2021).

[36] Mali Cohen Denzinger. Why ai driven personalized incentives work l sisense. https://www.sisense.com/blog/ai-driven-personalized-incentives-work/, 2017. (Accessed on 04/16/2021).

[37] Irv Lichtenwald. Personalized incentives are the key to patient compliance. medsphere. https://www.medsphere.com/blog/personalized-incentives-are-the-key-to-patient-compliance/, 2018. (Accessed on 04/16/2021).

[38] Mark Costanzo and Allison Redlich. Use of physical and psychological force in criminal and military interrogations. *Policing around the world: Police use of force*, pages 43–51, 2010.

[39] Rebecca Gordon. How Psychologists Are Taking A Stand Against Torture. HuffPost. https://www.huffpost.com/entry/how-psychologists-are-taking-a-stand-against-torture_b_5b981d5de4b021ab2c5f9868, 2018. (Accessed on 04/16/2021).

[40] BBC News. Webcam blackmail cases have doubled, police say. https://www.bbc.com/news/uk-38150313, 2016. (Accessed on 04/16/2021).

[41] Tom Noah, Yaacov Schul, and Ruth Mayo. When both the original study and its failed replication are correct: Feeling observed eliminates the facial-feedback effect. *Journal of personality and social psychology*, 114(5):657, 2018.

[42] Ivan Manokha. Surveillance, panopticism, and self-discipline in the digital age. *Surveillance & Society*, 16(2):219–237, 2018.

[43] Jonathon W Penney. Chilling effects: Online surveillance and wikipedia use. *Berkeley Tech. LJ*, 31:117–182, 2016.

[44] George Orwell. *Nineteen eighty-four*. Oxford University Press, 2021.

[45] Thomas Brewster. Exclusive: Saudi dissidents hit with stealth iphone spyware before khashoggi's murder. https://www.forbes.com/sites/thomasbrewster/2018/11/21/exclusive-saudi-dissidents-hit-with-stealth-iphone-spyware-before-khashoggis-murder/?sh=26d794d82e8b, 2018. (Accessed on 04/16/2021).

[46] David Agren. Mexico accused of spying on journalists and activists using cellphone malware. the guardian. https://www.theguardian.com/world/2017/jun/19/mexico-cellphone-software-spying-journalists-activists, 2017. (Accessed on 04/22/2021).

[47] Deutsche Welle. Turkey used german spy software on opposition politicians and activists. https://www.dw.com/en/turkey-used-german-spy-software-on-opposition-politicians-and-activists/a-43787769, 2018. (Accessed on 04/22/2021).

[48] Fan Liang, Vishnupriya Das, Nadiya Kostyuk, and Muzammil M Hussain. Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. *Policy & Internet*, 10(4):415–453, 2018.

[49] Claire Reilly. Cameras, surveillance and domestic abuse: A sinister match - cnet. https://www.cnet.com/news/cameras-surveillance-and-the-sinister-tech-behind-domestic-abuse/, 2018. (Accessed on 04/17/2021).

[50] Olivia Solon. Big brother isn't just watching: workplace surveillance can track your every move. https://www.theguardian.com/world/2017/nov/06/workplace-surveillance-big-brother-technology, 2017. (Accessed on 04/17/2021).

[51] Lisa Vaas. Employee surveillance – how far is too far? – naked security. https://nakedsecurity.sophos.com/2017/11/08/employee-surveillance-how-far-is-too-far/, 2017. (Accessed on 04/21/2021).

[52] Emine Saner. Employers are monitoring computers, toilet breaks – even emotions. is your boss watching you? | surveillance | the guardian. https://www.theguardian.com/world/2018/may/14/is-your-boss-secretly-or-not-so-secretly-watching-you, 2018. (Accessed on 04/17/2021).

[53] Peter Waldman, Lizette Chapman, and Jordan Robertson. Palantir knows everything about you. https://www.bloomberg.com/features/2018-palantir-peter-thiel/, 2018. (Accessed on 04/17/2021).

[54] CBS News. Erin andrews leaves tennessee courtroom in tears before jury views stalker's nude videos - cbs news. https://www.cbsnews.com/news/erin-andrews-tennessee-courtroom-jury-stalker-nude-videos/, 2016. (Accessed on 04/17/2021).

[55] Paul Farrell. Nude photos of jennifer lawrence and others posted online by alleged hacker. https://www.theguardian.com/world/2014/sep/01/nude-photos-of-jennifer-lawrence-and-others-posted-online-by-alleged-hacker, 2014. (Accessed on 04/17/2021).

[56] Wikipedia. Revenge porn. https://en.wikipedia.org/wiki/Revenge_porn. (Accessed on 04/17/2021).

[57] Scott R Stroud. The dark side of the online self: A pragmatist critique of the growing plague of revenge porn. *Journal of Mass Media Ethics*, 29(3):168–183, 2014.

[58] Associated Press. Ex-rutgers student dharun ravi found guilty of hate crimes in spying case | new jersey | the guardian. https://www.theguardian.com/world/2012/mar/16/rutgers-dharun-ravi-guilty-webcam-spying, 2012. (Accessed on 04/17/2021).

[59] Craig R. Whitney. G.m. settles nader suit on privacy for $425,000. the new york times. https://www.nytimes.com/1970/08/14/archives/gm-settles-nader-suit-on-privacy-for-425000-gm-pays-nader-425000-in.html, 1970. (Accessed on 04/17/2021).

[60] Wikipedia. Cointelpro. https://en.wikipedia.org/wiki/COINTELPRO. (Accessed on 04/17/2021).

[61] Rebecca Rosen. How your private emails can be used against you in court - the atlantic. https://www.theatlantic.com/technology/archive/2011/07/how-your-private-emails-can-be-used-against-you-in-court/241505/, 2011. (Accessed on 04/17/2021).

[62] Christopher Mele. Bid for access to amazon echo audio in murder case raises privacy concerns. the new york times. https://www.nytimes.com/2016/12/28/business/amazon-echo-murder-case-arkansas.html, 2016. (Accessed on 04/17/2021).

[63] Christine Hauser. In connecticut murder case, a fitbit is a silent witness. the new york times. https://www.nytimes.com/2017/04/27/nyregion/in-connecticut-murder-case-a-fitbit-is-a-silent-witness.html, 2017. (Accessed on 04/17/2021).

[64] Jana Winter. How law enforcement can use google timeline to track your every move. https://theintercept.com/2015/11/06/how-law-enforcement-can-use-google-timeline-to-track-your-every-move/, 2015. (Accessed on 04/17/2021).

[65] Google. Requests for user information – google transparency report. https://transparencyreport.google.com/user-data/overview. (Accessed on 04/17/2021).

[66] Aleksandr Solzhenitsyn. Cancer ward, trans. *Nicholas Beythel and David Burg. New York: Farrar, Straus, and Giroux*, 1968.

[67] Larry Greenemeier. What is the big secret surrounding stingray surveillance? https://www.scientificamerican.com/article/what-is-the-big-secret-surrounding-stingray-surveillance/, 2015. (Accessed on 04/17/2021).

[68] Kristina Cooke. U.s. police used facebook, twitter data to track protesters: Aclu. https://www.reuters.com/article/us-social-media-data-idUSKCN12B2L7, 2016. (Accessed on 04/17/2021).

[69] Amy B Wang. A suspect tried to blend in with 60,000 concertgoers. china's facial-recognition cameras caught him. - the washington post. `https://www.washingtonpost.com/news/worldviews/wp/2018/04/13/china-crime-facial-recognition-cameras-catch-suspect-at-concert-with-60000-people/`, 2018. (Accessed on 04/17/2021).

[70] Stefaan Verhulst. China seeks glimpse of citizens' future with crime-predicting ai. financial times. `https://www.ft.com/content/5ec7093c-6e06-11e7-b9c7-15af748b60d0`, 2017. (Accessed on 04/21/2021).

[71] Ewen MacAskill. Yahoo forced to apologise to chinese dissidents over crackdown on journalists | technology | the guardian. `https://www.theguardian.com/technology/2007/nov/14/news.yahoo`, 2007. (Accessed on 04/17/2021).

[72] Charles A Sullivan and Michael J Zimmer. *Cases and materials on employment discrimination*. Wolters Kluwer Law & Business, 2017.

[73] Frederik Zuiderveen Borgesius and Joost Poort. Online price discrimination and eu data privacy law. *Journal of consumer policy*, 40(3):347–366, 2017.

[74] A. Spender, C. Bullen, L. Altmann-Richer, J. Cripps, R. Duffy, C. Falkous, M. Farrell, T. Horn, J. Wigzell, and W. Yeap. Wearables and the internet of things: Considerations for the life and health insurance industry. *British Actuarial Journal*, 24:e22, 2019.

[75] Mikella Hurley and Julius Adebayo. Credit scoring in the era of big data. *Yale JL & Tech.*, 18:148, 2016.

[76] Robinson Meyer. Facebook's new patent, 'digital redlining,' and financial justice - the atlantic. `https://www.theatlantic.com/technology/archive/2015/09/facebooks-new-patent-and-digital-redlining/407287/`, 2015. (Accessed on 04/17/2021).

[77] Physicians for Human Righs. Science article shows that the us government used bad science to commit and conceal torture. `https://phr.org/news/science-article-shows-that-the-us-government-used-bad-science-to-commit-and-conceal-torture/`, 2011. (Accessed on 04/17/2021).

[78] Konrad-Adenauer-Stiftung. *Was war die Stasi?: Einblicke in das Ministerium für Staatssicherheit der DDR (MfS)*. Konrad-Adenauer-Stiftung, 2002.

[79] Lara Salahi and Emily Friedman. Kristen labrie guilty of attempted murder for withholding son's cancer medication - abc news. `https://abcnews.go.com/Health/Autism/kristen-labrie-guilty-attempted-murder-withholding-sons-cancer/story?id=13356743`, 2011. (Accessed on 04/17/2021).

[80] Andy Campbell. M&m murder: Veronica cirella killed her allergic daughter with peanut chocolates, cops say | huffpost. `https://www.huffpost.com/entry/mm-murder-veronica-cirella-peanut-allergy_n_1408480`, 2012. (Accessed on 04/17/2021).

[81] David Hanscom. Bullying is assault and should be treated as such. psychology today. `https://www.psychologytoday.com/us/blog/anxiety-another-name-pain/202010/bullying-is-assault-and-should-be-treated-such`, 2020. (Accessed on 04/17/2021).

[82] Jaana Juvonen and Sandra Graham. *Peer harassment in school: The plight of the vulnerable and victimized*. Guilford Press, 2001.

[83] UpCounsel. Eeoc complaints: Everything you need to know. `https://www.upcounsel.com/eeoc-complaints`, 2020. (Accessed on 04/17/2021).

[84] Wikipedia. Targeted advertising. `https://en.wikipedia.org/wiki/Targeted_advertising`. (Accessed on 04/17/2021).

[85] Otto Hans-Martin Lutz, Jacob Leon Kröger, Manuel Schneiderbauer, and Manfred Hauswirth. Surfing in sound: Sonification of hidden web tracking. In *International Conference on Auditory Display (ICAD)*. Georgia Institute of Technology, 2019.

[86] Philip Raschke, Sebastian Zickau, Jacob Leon Kröger, and Axel Küpper. Towards real-time web tracking detection with t.ex - the transparency extension. In *Annual Privacy Forum*, pages 3–17. Springer, 2019.

[87] Jun Yan, Ning Liu, Gang Wang, Wen Zhang, Yun Jiang, and Zheng Chen. How much can behavioral targeting help online advertising? In *Proceedings of the 18th international conference on World wide web*, pages 261–270, 2009.

[88] Sandra C Matz, Michal Kosinski, Gideon Nave, and David J Stillwell. Psychological targeting as an effective approach to digital mass persuasion. *Proceedings of the national academy of sciences*, 114(48):12714–12719, 2017.

[89] Kaitlyn Tiffany. Online ads can be targeted based on your emotions - vox. https://www.vox.com/the-goods/2019/5/21/18634323/new-york-times-emotion-based-ad-targeting-sadness, 2019. (Accessed on 04/18/2021).

[90] Lucia Moses. Marketers should take note of when women feel least attractive. adweek. https://www.adweek.com/brand-marketing/marketers-should-take-note-when-women-feel-least-attractive-152753/, 2013. (Accessed on 04/18/2021).

[91] Swathi Meenakshi Sadagopan. Feedback loops and echo chambers: How algorithms amplify viewpoints. https://theconversation.com/feedback-loops-and-echo-chambers-how-algorithms-amplify-viewpoints-107935, 2019. (Accessed on 05/09/2021).

[92] Mostafa M. El-Bermawy. Your echo chamber is destroying democracy | wired. https://www.wired.com/2016/11/filter-bubble-destroying-democracy/, 2016. (Accessed on 04/19/2021).

[93] Jim Isaak and Mina J Hanna. User data privacy: Facebook, cambridge analytica, and privacy protection. *Computer*, 51(8):56–59, 2018.

[94] Carole Cadwalladr and Emma Graham-Harrison. Revealed: 50 million facebook profiles harvested for cambridge analytica in major data breach | cambridge analytica | the guardian. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election, 2018. (Accessed on 04/19/2021).

[95] Alan S Gerber, Gregory A Huber, David Doherty, Conor M Dowling, and Costas Panagopoulos. Big five personality traits and responses to persuasive appeals: Results from voter turnout experiments. *Political Behavior*, 35(4):687–728, 2013.

[96] Ross Anderson. *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons, 2020.

[97] Sherly Abraham and InduShobha Chengalur-Smith. An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, 32(3):183–196, 2010.

[98] Chris Baraniuk. Google and facebook duped in huge 'scam'. https://www.bbc.com/news/technology-39744007, 2017. (Accessed on 04/19/2021).

[99] BBC News. Email prankster 'fooled' white house officials. https://www.bbc.com/news/world-us-canada-40788080, 2017. (Accessed on 04/19/2021).

[100] Marie Keyworth. Vishing and smishing: The rise of social engineering fraud - bbc news. https://www.bbc.com/news/business-35201188, 2016. (Accessed on 04/19/2021).

[101] John Markoff. As artificial intelligence evolves, so does its criminal potential. the new york times. https://www.nytimes.com/2016/10/24/technology/artificial-intelligence-evolves-with-its-criminal-potential.html, 2016. (Accessed on 04/19/2021).

[102] Thomas K Ledbetter. Stopping unsolicited commercial e-mail: Why the can-spam act is not the solution to stop spam. *Sw. UL REv.*, 34:107, 2004.

[103] Statista. Global spam volume as percentage of total e-mail traffic from january 2014 to september 2020. https://www.statista.com/statistics/420391/spam-email-traffic-share/, 2020. (Accessed on 04/19/2021).

[104] FTC Consumer Information. Phone scams. https://www.consumer.ftc.gov/articles/0208-phone-scams, 2019. (Accessed on 04/19/2021).

[105] Ellen M Selkie, Jessica L Fales, and Megan A Moreno. Cyberbullying prevalence among us middle and high school–aged adolescents: A systematic review and quality assessment. *Journal of Adolescent Health*, 58(2):125–133, 2016.

[106] Manny Fernandez, Serge F. Kovaleski, and John Ismay. For austin bomb investigators, each new blast offers new clues. the new york times. https://www.nytimes.com/2018/03/20/us/austin-bomb-san-antonio-fedex.html, 2018. (Accessed on 04/19/2021).

[107] Devlin Barrett, Mark Berman, and Cleve R. Wootson. Clinton and obama bombs: Secret service intercepts suspicious packages - the washington post. https://www.washingtonpost.com/nation/2018/10/24/bomb-sent-bill-hillary-clintons-home-new-york-city-suburb/, 2018. (Accessed on 04/19/2021).

[108] Paul Bocij. *Cyberstalking: Harassment in the Internet age and how to protect your family*. Greenwood Publishing Group, 2004.

[109] Sahara Byrne, Sherri Jean Katz, Theodore Lee, Daniel Linz, and Mary McIlrath. Peers, predators, and porn: Predicting parental underestimation of children's risky online experiences. *Journal of Computer-Mediated Communication*, 19(2):215–231, 2014.

[110] Ned Potter. Playstation sex crime: Criminal used video game to get girl's naked pictures - abc news. https://abcnews.go.com/Technology/story?id=7009977&page=1, 2009. (Accessed on 04/19/2021).

[111] Brian H Spitzberg and Gregory Hoobler. Cyberstalking and the technologies of interpersonal terrorism. *New media & society*, 4(1):71–92, 2002.

[112] Paul Bocij, MD Griffiths, and Leroy McFarlane. Cyberstalking: A new challenge for criminal law. *The Criminal Lawyer*, 122:3–5, 2002.

[113] The Carly Ryan Foundation. Carly's story. https://www.carlyryanfoundation.com/carlys-story. (Accessed on 04/19/2021).

[114] Brian J Grim and Roger Finke. *The price of freedom denied: Religious persecution and conflict in the twenty-first century*. Cambridge University Press, 2010.

[115] Rob Witte. *Racist violence and the state: a comparative analysis of Britain, France and the Netherlands*. Routledge, 2014.

[116] Arzu Güler, Maryna Shevtsova, and Denise Venturi. *LGBTI asylum seekers and refugees from a legal and political perspective: Persecution, asylum and integration*. Springer, 2018.

[117] Halya Coynash and Austin Charron. Russian-occupied crimea and the state of exception: repression, persecution, and human rights violations. *Eurasian Geography and Economics*, 60(1):28–53, 2019.

[118] Peter Preston. Six million and counting | history books | the guardian. https://www.theguardian.com/books/2001/feb/18/historybooks.features, 2001. (Accessed on 04/19/2021).

[119] Evan Selinger and Woodrow Hartzog. The inconsentability of facial surveillance. *SSRN*, 2020.

[120] Shyang-Lih Chang, Li-Shien Chen, Yun-Chung Chung, and Sei-Wan Chen. Automatic license plate recognition. *IEEE transactions on intelligent transportation systems*, 5(1):42–53, 2004.

[121] Muhammad Usman Iqbal and Samsung Lim. Privacy implications of automated gps tracking and profiling. *IEEE technology and society magazine*, 29(2):39–46, 2010.

[122] Eyder Peralta. Betrayed By Metadata: John McAfee Admits He's Really In Guatemala. https://www.npr.org/sections/thetwo-way/2012/12/04/166487197/betrayed-by-metadata-john-mcafee-admits-hes-really-in-guatemala?t=1626301235932, 2012. (Accessed on 04/22/2021).

[123] Jacob Leon Kröger, Philip Raschke, and Towhidur Rahman Bhuiyan. Privacy Implications of Accelerometer Data: A Review of Possible Inferences. In *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy (ICCSP)*, pages 81–87, New York, NY, 2019. ACM.

[124] Yvon Dandurand and Kristin Farr. *A review of selected witness protection programs*. Public Safety Canada, 2012.

[125] Irene Plagianos. 'el chapo' tech guru testifies on spyware, fleeing from the law and flipping on drug lord. los angeles times. https://www.latimes.com/nation/la-na-el-chapo-technology-guru-20190110-story.html, 2019. (Accessed on 04/19/2021).

[126] Joyce Hackel. The long reach of el salvador's gangs extends even to victims who've fled to the us. https://www.pri.org/stories/2016-05-26/salvadoran-gangs-use-facebook-track-down-victims, 2016. (Accessed on 04/19/2021).

[127] Mark Johanson. How burglars use facebook to target vacationing homeowners. https://www.ibtimes.com/how-burglars-use-facebook-target-vacationing-homeowners-1341325, 2013. (Accessed on 04/19/2021).

[128] Jennifer Van Grove. Are we all asking to be robbed? https://mashable.com/2010/02/17/pleaserobme/?europe=true, 2010. (Accessed on 04/19/2021).

[129] Katherine Slosarik. Identity theft: An overview of the problem. *The Justice Professional*, 15(4):329–343, 2002.

[130] Keith B Anderson, Erik Durbin, and Michael A Salinger. Identity theft. *Journal of Economic Perspectives*, 22(2):171–192, 2008.

[131] Katherine Skiba. Identity theft cases doubled from 2019 to 2020, ftc says. https://www.aarp.org/money/scams-fraud/info-2021/ftc-fraud-report-identity-theft-pandemic.html, 2021. (Accessed on 04/19/2021).

[132] Federal Trade Commission. Identity theft - presentation. https://www.consumer.ftc.gov/sites/default/files/powerpoint/idtgov.pptx, 2016. (Accessed on 04/19/2021).

[133] Taylor Armerding. Thieves can steal your voice for authenticatoin | cso online. https://www.csoonline.com/article/3196820/vocal-theft-on-the-horizon.html, 2017. (Accessed on 04/19/2021).

[134] Warwick Ashford. Spyware targets north korean dissidents via social links, says mcafee. https://www.computerweekly.com/news/450433004/Spyware-targets-North-Korean-dissidents-via-social-links-says-McAfee, 2018. (Accessed on 04/22/2021).

[135] Jacob Leon Kröger and Philip Raschke. Is my phone listening in? on the feasibility and detectability of mobile eavesdropping. In *IFIP Annual Conference on Data and Applications Security and Privacy*, pages 102–120. Springer, 2019.

[136] Nelson Blackstock. *COINTELPRO: The FBI's Secret War on Political Freedom.* Anchor Foundation, New York, 1988.

[137] Wikipedia. Predictive policing. https://en.wikipedia.org/wiki/Predictive_policing. (Accessed on 04/17/2021).

[138] Nil-Jana Akpinar, Maria De-Arteaga, and Alexandra Chouldechova. The effect of differential victim crime reporting on predictive policing systems. In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, pages 838–849, 2021.

[139] Molly Griffard. A Bias-Free Predictive Policing Tool: An Evaluation of the NYPD's Patternizr. *Fordham Urb. LJ*, 47:43, 2019.

[140] ACLU. Statement of concern about predictive policing. https://www.aclu.org/other/statement-concern-about-predictive-policing-aclu-and-16-civil-rights-privacy-racial-justice, 2016. (Accessed on 04/22/2021).

[141] Ed Yong. A popular algorithm is no better at predicting crimes than random people - the atlantic. https://www.theatlantic.com/technology/archive/2018/01/equivant-compas-algorithm/550646/, 2018. (Accessed on 04/22/2021).

[142] U.S. Department of Justice. Organized crime member pleads guilty to attempted murder of witness. https://www.justice.gov/usao-sdny/pr/organized-crime-member-pleads-guilty-attempted-murder-witness, 2018. (Accessed on 04/22/2021).

[143] Yaniv Kubovich, Barak Ravid, and Sharon Pulwer. Witness in organized crime trial killed in tel aviv car blast. https://www.haaretz.com/israel-news/witness-in-organized-crime-trial-killed-in-tel-aviv-blast-1.5416771, 2016. (Accessed on 04/22/2021).

[144] Anti-Corruption Helpdesk Transparency International. The impact of the new General Data Protection Regulation (GDPR) on whistleblowing. https://knowledgehub.transparency.org/assets/uploads/helpdesk/GDPR-and-whistleblowing_2018-PR.pdf, 2018. (Accessed on 04/22/2021).

[145] Avery Kleinman and Christine Anderson. Fda surveillance threatened whistleblowers. https://www.pogo.org/analysis/2014/02/fda-surveillance-threatened-whistleblowers/, 2014. (Accessed on 04/22/2021).

[146] Internet Encyclopedia of Philosophy. Surveillance ethics. https://iep.utm.edu/surv-eth/. (Accessed on 04/22/2021).

[147] Sandra Wachter and Brent Mittelstadt. A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review*, (2):494–620, 2019.

[148] Jordan M Blanke. Protection for 'inferences drawn'. *Global Privacy Law Review*, 1(2):81–92, 2020.

[149] Daniel Le Métayer. Whom to trust? Using technology to enforce privacy. In D. Wright and P. De Hert, editors, *Enforcing Privacy*, pages 395–437. Springer, 2016.

[150] T. J. Kasperbauer. Protecting health privacy even when privacy is lost. *Journal of Medical Ethics*, 46(11):768–772, 2020.

[151] Jacob Leon Kröger, Philip Raschke, Jessica Percy Campbell, and Stefan Ullrich. Surveilling the gamers: Privacy impacts of the video game industry. *Social Science Research Network (SSRN)*, 2021.

[152] Jacob Leon Kröger, Otto Hans-Martin Lutz, and Florian Müller. What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking. In Samuel Fricker, Michael Friedewald, Stephan Krenn, Eva Lievens, and Melek Önen, editors, *Privacy and Identity Management. Data for Better Living: AI and Privacy*, IFIP Advances in Information and Communication Technology, pages 226–241. Springer, Cham, 2019.

[153] Jacob Kröger. Unexpected inferences from sensor data: a hidden privacy threat in the internet of things. In *IFIP International Internet of Things Conference*, pages 147–159. Springer, 2018.

[154] Jacob Leon Kröger, Otto Hans-Martin Lutz, and Philip Raschke. Privacy Implications of Voice and Speech Analysis – Information Disclosure by Inference. In M Friedewald, M Önen, E Lievens, and S Krenn, editors, *Privacy and Identity Management. Data for Better Living: AI and Privacy*, pages 242–258. Springer,, Cham, March 2020.

[155] Daniel J Solove. Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, 126:25, 2012.

[156] Russell Heimlich. Internet users don't like targeted ads | pew research center. https://www.pewresearch.org/fact-tank/2012/03/13/internet-users-dont-like-targeted-ads/, 2012. (Accessed on 04/28/2021).

[157] Brave. Europe's governments are failing the gdpr. https://brave.com/wp-content/uploads/2020/04/Brave-2020-DPA-Report.pdf, 2020. (Accessed on 04/28/2021).