3-15-2024

Approaches to Regulating Privacy Dark Patterns

Matthew Gaulton
Western University, mgaulto2@uwo.ca

Dominique Kelly
Western University, dkelly48@uwo.ca

Jacquelyn Burkell
Western University, jburkell@uwo.ca

Approaches to Regulating Privacy Dark Patterns

Legal Memo Prepared for the Office of the Privacy Commissioner of Canada

Contributions Program 2023-2024

Matthew Gaulton

Dominique Kelly

Jacquelyn Burkell

Faculty of Information and Media Studies

The University of Western Ontario

London, Ontario

March 15, 2024

Table of Contents

Introduction

Objectives

In this paper, we will evaluate new bills slated to replace the Personal Information Protection and Electronic Documents Act (PIPEDA) and offer stronger privacy dark pattern protections to Canadians.

Existing scholarship in the realm of privacy law, such as "Deceptive Design and Ongoing Consent in Privacy Law" by Jeremy Wiener and "Privacy Dark Patterns: A Case for Regulatory Reform in Canada" by Ademola Adeyoju, primarily focuses on creating frameworks for understanding privacy dark patterns in the law and explaining the pitfalls and legal inadequacies surrounding dark pattern legislation in Canada.

However, the aim of this paper diverges significantly. While acknowledging the invaluable insights provided by these foundational works, the objective of this article is twofold: First, to offer a comprehensive review of multiple proposed legislative bills slated to replace PIPEDA in Canada; and second, to critically evaluate the effectiveness of these proposed changes, especially in comparison with more robust frameworks like California's Consumer Privacy Act (CCPA) and the European Union's General Data Protection Regulation (GDPR), which offer extensive protections against dark patterns. In doing so, this paper seeks to fill a gap in the existing literature by examining how proposed Canadian legislation measures up to international standards in protecting citizens from the pitfalls of dark patterns.

Privacy dark patterns: Definition, consequences, and countermeasures

Origin of the term "dark patterns"

Coined by UK-based user experience (UX) consultant Harry Brignull in 2010, the term "dark patterns" refers to manipulative user interface (UI) design strategies. These designs are intended to steer users into making decisions or taking actions that predominantly serve the interests of online services, rather than the users themselves (Brignull, 2010; Kelly & Rubin, 2024). Brignull took the initiative to curate a library of examples on his website, originally called darkpatterns.org and now rebranded as "deceptive.design." "Bait and Switch," for example, leads users to unexpected and often undesirable outcomes, while "Friend Spam" dupes users into sharing social media or email credentials under the pretense of social connectivity, only to misuse that access for unsolicited messaging. Another notable example is "Privacy Zuckering," which tricks users into divulging more personal information than they initially intended to share (Brignull, 2010).

Conceptualizing privacy dark patterns

A subset of manipulative design tactics known as "privacy dark patterns" focus specifically on compromising user privacy. These are UI design strategies engineered to influence users to make privacy-invasive choices, such as revealing personal data or consenting to its use (Bösch et al.,

2016; Brignull, 2010; Fritsch, 2017). Examples from Brignull's library, like “Friend Spam” or “Privacy Zuckering,” fall under this category. These tactics are not mere aberrations but are systematically deployed by corporations with the explicit aim of amplifying their collection and use of users' personal data. In essence, privacy dark patterns represent a targeted application of dark patterns to exploit users' personal information.

Why privacy dark patterns work

Privacy dark patterns are effective largely because they exploit “decision-making vulnerabilities” (Susser et al., 2019a, p. 29). These vulnerabilities often manifest as cognitive biases and heuristics (Lukoff et al., 2021; Mathur et al., 2019; Waldman, 2020). Heuristics are mental shortcuts that humans rely on for decision-making (Acquisti et al., 2017). Heuristics help individuals navigate situations where they face limitations in knowledge and reasoning, a condition termed “bounded rationality” (Simon, 2000). However, these mental shortcuts can lead to cognitive biases, severe and systematic errors in thinking, as established by extensive research (e.g., Tversky & Kahneman, 1974; 1986). For instance, setting defaults that make a user's personal data publicly visible taps into the “status quo bias,” a cognitive inclination to maintain one's current state (Mirsch et al., 2017, p. 640).

Bösch et al. (2016) suggest that privacy dark patterns are most potent when users engage in “System 1” thinking, which is automatic and quick, as opposed to “System 2” thinking, which is more deliberate and reflective (Kahneman, 2013). Dark patterns can also be viewed as a specialized form of “nudging,” a concept introduced by Thaler and Sunstein (2008). In nudging, the “choice architecture,” or the context in which decisions are made, is intentionally altered by designers to prompt specific user actions. Such nudges have demonstrated their influence in various contexts; for example, setting a preferred option as a default has been shown to significantly impact behaviour in areas like organ donation (Johnson & Goldstein, 2003).

Examples of privacy dark patterns

Privacy dark patterns manifest in a multitude of insidious ways, each designed to exploit specific vulnerabilities. For instance, “Hidden Legalese Stipulations” involve lengthy and convoluted terms and conditions, deliberately making it difficult for most users to comprehend the legal ramifications of using the online service (Bösch et al., 2016). “Immortal Accounts” present another hurdle by making it arduous, if not impossible, for users to delete their accounts (Bösch et al., 2016). Yet another variation is “Fogging Identification with Security,” where services ostensibly offer enhanced security measures but in reality are seeking to gather more personal data, such as phone numbers (Fritsch, 2017). Dark patterns are also present in tracking cookie consent notices, where opting out of tracking often demands greater effort from the user than opting in (Nouwens et al., 2020). Several consumer protection agencies and regulatory bodies, including France’s Commission Nationale de l’Informatique et des Libertés, the European Data Protection Board, and Norway’s Forbrukerrådet, have developed their own typologies to classify and address these manipulative practices.

Dark patterns often operate through three primary modes of influence: increasing the user's workload (“Obstruction”), confusing or misleading the user (“Obfuscation”), and framing certain options positively or negatively through language and visuals (“Pressure”) (Kelly & Rubin, 2022; Kelly & Burkell, Under Review, 2024a; 2024b). In a privacy context, one form of “Obstruction” occurs when the user is required to click a confirmation button to enact a privacy-friendly choice. For example, when attempting to opt out of a “public” account that exposes their posts to a wide audience, the user might be forced to click an unnecessary additional button. A common manifestation of “Obfuscation” occurs when buttons to enact privacy-invasive choices are more salient – and therefore attention-grabbing – than those that would enable privacy-friendly options. When asking the user to sync their contacts, for instance, a site might make the button to consent to syncing bright and colourful, while the button to skip this step is small, faint, and easy to miss. Finally, an example of “Pressure” can be observed when a site attempts to evoke feelings of fear or guilt in the user by stressing the costs or risks associated with making a privacy-friendly choice. An attempt to opt out of targeted advertising might be accompanied by warnings that the user will see the same number of ads, but that these ads will be “less relevant” to their interests. Table 1 summarizes three major types of privacy dark patterns and 10 subtypes uncovered in a content analysis of five social networking sites (SNSs) (Kelly & Burkell, Under Review, 2024a; 2024b).

Table 1

Descriptions of three major privacy dark pattern types and 10 subtypes identified in a sample of five SNSs, adapted from a model in working papers (Kelly & Burkell, Under Review, 2024a; 2024b).

Privacy dark pattern types and subtypes	**Description**
1 Obstruction	The site increases the effort that users must exert to make a privacy-friendly choice (i.e., by requiring more actions).
1.1 Defaults	Privacy-invasive options are selected by default prior to user interaction, requiring the user to locate and change them.
1.2 Confirmations	Attempts to make privacy-friendly choices are accompanied by pop-ups that require the user to confirm their decision by clicking an additional button.
1.3 Interruptions	Pop-ups asking the user to make a privacy-invasive choice appear and must be manually dismissed. The requests are irrelevant to the user’s current activity.
1.4 Missing Bulk Options	Three or more closely-related privacy-invasive defaults are presented together without a corresponding bulk option (e.g., a “reject all” button).

2 Obfuscation	The site obscures, hides, or omits relevant information and options, with the intent of confusing or misleading the user into making a privacy-invasive choice.
2.1 Attention Manipulation	The buttons for privacy-invasive choices are given greater salience than privacy-friendly choices through their size, colour, placement, and/or contrast.
2.2 False Requirements	In a task flow, several empty fields to be filled in with the user's data appear, without any indication of which fields are required and which are optional.
2.3 False "Private" Account	The user is given the opportunity to set their account to "private," but enacting this setting does not alter all privacy-invasive defaults.
2.4 Concealed Settings	After account registration, the site does not suggest that the user check their account settings to ensure that the current defaults align with the user's preferences.
3 Pressure	The site actively encourages the user to make a privacy-invasive choice by presenting the privacy-invasive choice positively, and/or presenting the privacy-friendly choice negatively, through language and visuals.
3.1 Emotional Pressure	The risks or costs of a privacy-friendly choice (e.g., the loss of certain features) are emphasized to evoke feelings of fear or guilt in the user.
3.2 Conditional Rejections	The button to reject a privacy-invasive option uses wording implying the user will be asked or required to accept the option at a later time (e.g., "not now").

Negative consequences of privacy dark patterns

Dark patterns expose users to privacy risks and harms

The implications of dark patterns extend beyond inconvenience or frustration, posing significant privacy-related risks and potential harms. Unchecked disclosure of personal data online can open a Pandora's box of issues, including reputational damage (Solove, 2007), susceptibility to cyberstalking and identity theft (Kroll & Stieglitz, 2019), and subsequent regret regarding posts (Wang et al., 2011). The data that users willingly or unwittingly share also empowers platforms to make increasingly detailed inferences about them. Actions as seemingly benign as "liking" a post on Facebook (Kosinski et al., 2013) or adding a "friend" on social media (Barocas & Nissenbaum, 2014) can be parsed for additional, more sensitive personal information. Such data mining enables platforms to pinpoint "individual- or person-specific vulnerabilities" (Susser et al., 2019b, p. 6), which can be exploited to subtly guide users' choices via targeted ads (Susser et

al., 2019a) or personalized nudging (Christl, 2017; Susser et al., 2019a; Yeung, 2017). For instance, leaked Facebook documents in 2017 allegedly showed that the platform could target ads to teens at moments of vulnerability (Susser et al., 2019a). Moreover, this accumulation of personal data creates a ticking time bomb in the event of a data breach, leaving users highly vulnerable.

Dark patterns undermine user autonomy

The insidious nature of dark patterns lies not just in their outcomes but also in their means, as they exploit cognitive biases and heuristics that typically function below people's conscious awareness. This subversive influence fundamentally undermines individual autonomy, sabotaging people's ability to make informed and deliberate choices regarding their online privacy. In doing so, dark patterns pose a substantial threat to the very principle of informed consent. Researchers have criticized some forms of "nudging" – often likened to dark patterns in a digital context – as manipulative and contrary to promoting individual well-being (Hansen & Jespersen, 2013; Susser et al., 2019a). These detrimental nudges, derogatorily termed "sludges" by Thaler (2018), serve to underscore the ethical quandaries presented by such surreptitious design techniques. These manipulations cast a long shadow on the integrity of user interactions online, calling into question the ethical foundation of myriad platforms.

Approaches to combatting privacy dark patterns

Rossi and Bongard-Blanchy (2021) identify four "intervention spaces" for dark patterns: technical, design, educational, and regulatory measures. Technical measures include tools that "automatically identify, flag, and even classify potential dark patterns at large scale" (Rossi & Bongard-Blanchy, 2021, p. 3). Researchers working in this area have developed frameworks and tools to automatically detect dark patterns, especially in the context of tracking cookie consent notices (Hausner et al., 2021; Kirkman et al., 2023; Soe et al., 2022). Nonetheless, clear limitations and challenges remain. Not all types of dark patterns can necessarily be detected through automated tools (Kirkman et al., 2023; Soe et al., 2022; Stavrakakis et al., 2021), and as new tools emerge, designers will presumably innovate novel technical approaches to implementing dark patterns to evade detection (Kirkman et al., 2023).

A second approach to combatting dark patterns involves encouraging companies to use design elements that enhance, rather than undermine, users' privacy online. Graßl et al. (2021) demonstrated that tactics typically associated with dark patterns, such as defaults and increasing the user's workload, could be implemented to sway users *away* from consenting to tracking cookies. They term these privacy-protective design strategies "bright patterns." Other research has proposed recommendations for the design of user-friendly account disabling interfaces (Kelly & Rubin, 2024; Schaffner et al., 2022) and explained how nudges can guide users to make privacy- and security-friendly choices (Acquisti et al., 2017). Research reveals that dark patterns erode brand trust and annoy consumers (Bhoot et al., 2020; Consumer Policy Research Centre, 2022; Voigt et al., 2021). Companies that deliberately provide a manipulation-free experience could distinguish themselves from competitors, especially given the ubiquity of dark patterns online (Di Geronimo et al., 2020). However, the incentives for designers to implement dark

patterns remain high because these practices *work* (Luguri & Strahilevitz, 2021; Nouwens et al., 2020): they effectively steer users to disclose more personal data or consent to its use, in turn profiting online companies (Acquisti et al., 2016).

Educational measures aim to bolster users' ability to recognize and resist dark patterns. These interventions ultimately place the burden of evading dark patterns on users – yet even when users are explicitly asked to look for design elements that could influence their behaviour and choices, some studies show that only about half are able to identify dark patterns (Bongard-Blanchy et al., 2021; Di Geronimo et al., 2020). At the same time, research has demonstrated that when teens are asked to set up a private SNS account, consider how SNSs could influence their privacy choices, and identify negative consequences associated with allowing SNSs to influence their behaviour, they are able to identify a wide range of dark patterns and strategies for resistance, and several report the intention to review and alter the privacy settings on their own personal accounts (Kelly & Burkell, Accepted, 2024).

Regulation is the final intervention space for dark patterns. However, while dark patterns remain a pervasive and potent force in shaping online user behavior (Di Geronimo et al., 2020; Luguri & Strahilevitz, 2021; Mathur et al., 2019; Nouwens et al., 2020), regulatory efforts to mitigate their impact are conspicuously lacking, especially outside of the United States and the European Union. In the Canadian context, the existing Personal Information Protection and Electronic Documents Act (PIPEDA) falls short of adequately addressing the use of dark patterns. This legislative gap allows these manipulative designs to continue thriving unchecked, further jeopardizing users' privacy and autonomy. As we move forward in an increasingly digitalized world, it becomes imperative to scrutinize and update the legal frameworks governing online user experience to ensure they align with the principles of transparency, autonomy, and informed consent.

Overview of regulatory frameworks

Canada: The Personal Information Protection and Electronic Documents Act

The Personal Information Protection and Electronic Documents Act (PIPEDA) serves as the cornerstone for privacy regulations in Canada, governing "the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."

In the context of PIPEDA, which succinctly defines personal information as "information about an identifiable individual," the real-world applications are much more expansive, especially in digital environments. IP addresses, for example, not only serve as unique identifiers for computers but can also pinpoint a user's geographic location. Cookies go beyond simple data storage, tracking user activities and preferences, and sometimes retaining login credentials.

Location data can be collected through various means, from a device's GPS to IP-based geolocation techniques, offering a granular view into an individual's habits and movements. Unique device identifiers, such as MAC addresses, are not mere technical details but can be used to specifically identify individuals. In addition, behavioural data, accrued through clicks, interactions, and dwell time on web pages, can coalesce into a unique digital profile of a person. Even something as seemingly benign as search history can divulge critical details about an individual's interests, beliefs, and health conditions. Together, these varied data types demonstrate the far-reaching scope of what PIPEDA considers as personal information in today's digital age.

This legislation applies comprehensively to organizations engaged in commercial activities. A testament to its broad applicability is its enforcement across a diverse array of sectors: companies ranging from Tim Hortons in the food industry to Dell in technology, Home Depot in retail, Facebook in social media, and Loblaws in grocery services have all been subjects of PIPEDA enforcement actions.

Enforcement of PIPEDA is handled by the Office of the Privacy Commissioner of Canada (OPC). The OPC not only oversees compliance but also has various means to resolve violations, ranging from compliance agreements to federal court actions and audits. Canadians can file complaints against organizations via the OPC's website. These complaints are then evaluated based on their validity and can be resolved through multiple channels, offering a structured approach to grievance redressal.

Since PIPEDA became Law in 2001, it has led to 152 reported investigations by the OPC, the details of which are publicly accessible on their website. To put this number into context, it indicates an active enforcement environment but also raises questions about whether this figure is proportionate with the scale of data collection activities in Canada, given the expansive definition of personal information in today's digital landscape.

How PIPEDA is currently protecting Canadians against dark patterns

While the language of "dark patterns" is noticeably absent from PIPEDA, the legislation nonetheless provides a layer of protection against such manipulative practices, particularly those that concern the use and distribution of personal information. The concept of "consent" is central to PIPEDA's enforcement strategy, as evidenced by the OPC focus on this issue. A notable 41 investigations led by the OPC have been specifically related to consent violations, making it the most frequently cited type of complaint. Circumventing user consent, violating established agreements, or taking actions without explicit approval are all tactics commonly associated with dark patterns. Thus, even without the inclusion of the term "dark patterns," PIPEDA's emphasis on consent serves as a key mechanism for protecting Canadians against such deceptive and unethical online practices.

In section 6.1 of PIPEDA, it asserts that “the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization’s activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.”

Schedule 1 of the act incorporates the principles laid out in the National Standard of Canada's Model Code for the Protection of Personal Information. This not only establishes consent as a foundational principle but also provides a nuanced understanding of what this right to consent entails for Canadians. Principle 3 within Schedule 1 further elaborates on the notion of consent, offering specific explanations on the situations that would constitute violations of consent by companies and organizations.

Building on the foundational elements set forth in Schedule 1, Principle 3 provides a comprehensive framework for organizations and how they must obtain and respect user consent, but also for users, and their rights that their consent grants them.

Under the framework of PIPEDA, obtaining consent is a prerequisite for gathering personal data and any activities related to its use or dissemination. Generally, companies aim to secure this consent at the moment they collect the information. However, there are instances where approval for utilizing or disclosing the data might be requested post-collection but prior to its actual use, such as when the organization intends to use the collected data for a new, previously unspecified purpose (PIPEDA 4.3.1).

Under PIPEDA's guidelines, organizations are obligated to both inform and obtain consent from individuals for the collection, use, or disclosure of their personal information. Efforts must be made to clearly articulate the intended purposes so that an individual can genuinely understand how their data will be handled. Additionally, companies cannot make the provision of a product or service contingent on an individual agreeing to the collection, use, or disclosure of more information than is strictly necessary for the stated and legitimate purposes (PIPEDA 4.3.2, 4.3.3).

Organizations need to be adaptable in the manner they request consent, tailoring it to both the context and the nature of the personal information involved. The sensitivity of the data in question plays a crucial role in determining the form of consent required. While certain types of information, such as medical or financial records, are universally understood to be sensitive, the sensitivity of other types of data can depend on the situation. For example, subscribing to a general newsmagazine likely involves less sensitive information than subscribing to a special-interest publication, where the very act of subscribing could reveal particular beliefs or preferences (PIPEDA 4.3.4).

In the process of obtaining consent, it's also imperative for organizations to consider what an individual would reasonably expect in terms of how their data will be used. For instance, if someone subscribes to a magazine, it is reasonable to assume they expect their information to be used for both mailing the magazine and billing. In such cases, their act of subscribing can implicitly be taken as consent for these specific activities. However, if the same individual provides personal data to a healthcare provider, it would not be reasonable to assume they have consented to share that data with a third-party company selling healthcare products. In such cases, explicit consent must be obtained, and under no circumstances should consent be acquired through deceptive practices (PIPEDA 4.3.5).

The methods an organization employs to gain consent can differ based on the situation and the category of information they are gathering. Typically, when dealing with sensitive data, the organization should aim for explicit consent from the individual. For less sensitive data, implied consent is generally sufficient. Additionally, in certain scenarios, a legal guardian or someone with power of attorney can provide consent on behalf of the individual.

Regarding the user and their rights surrounding their consent, there are multiple avenues through which individuals can express their consent. For example, completing and signing an application form not only allows for the collection of information but also serves as a way to inform the person of the specific uses of that information, thus capturing their consent. Another method is the use of checkboxes, which offer an opt-out mechanism. When individuals don't check these boxes, their consent to share information with third parties is implied. Verbal agreement is another route, often employed during telephone interactions. Additionally, simply using a product or service can sometimes be interpreted as granting consent. Importantly, individuals reserve the right to retract their consent at any time. However, this is subject to any legal or contractual limitations and requires reasonable notice. Organizations are obligated to enlighten individuals on the ramifications of such a decision.

Bill C-67: The Digital Charter Act

In response to evolving digital challenges and the significance of personal data protection, Canada has taken steps to update and enhance its privacy regulations. One such step is the introduction of Bill C-27, the Digital Charter Implementation Act, 2022. The Digital Charter Implementation Act, introduces three proposed acts: the Consumer Privacy Protection Act, the Artificial Intelligence and Data Act, and the Personal Information and Data Protection Tribunal Act.

Consumer Privacy Protection Act

This act was designed to promote increased control and transparency over how organizations manage Canadians' personal information. Canadians are granted the right to securely transfer their data between different organizations and to demand its deletion when it is no longer necessary. Special emphasis has been placed on safeguarding minors; the act restricts data collection on them and mandates stricter standards for organizations handling their information. Additionally, the Privacy Commissioner of Canada is endowed with expanded powers, including the ability to direct companies to halt data collection or personal information use. A robust penalty system has also been outlined for non-compliant organizations, with the most severe breaches incurring penalties of up to 5% of global revenue or $25 million, whichever is higher.

Personal Information and Data Protection Tribunal Act

Bill C-27 suggests the creation of this Tribunal to bolster the enforcement mechanisms of the Consumer Privacy Protection Act. The Tribunal's role would be to assess and act on recommendations from the Privacy Commissioner of Canada concerning administrative

monetary penalties for specific violations of the Act. Furthermore, it provides an avenue for both organizations and individuals to appeal decisions made by the Privacy Commissioner.

Electronic Documents Act

Concluding the provisions of the Digital Charter Implementation Act, 2022, this act aims to recognize a section of the current privacy law. This section, which deals with the federal public sector's use of electronic documents, is set to be established as a standalone piece of legislation.

How are we still falling short?

While Bill C-27 represents a commendable step forward in Canada's endeavor to fortify its privacy framework, it is essential to contextualize its provisions in the global landscape. Regulatory frameworks such as California's Consumer Privacy Act (CCPA) and the European Union's General Data Protection Regulation (GDPR) have set high benchmarks in the realm of data protection. These regulations offer comprehensive protections against privacy dark patterns, ensuring that user data is not just safeguarded but that individuals are empowered in their digital interactions. Compared to these standards, Bill C-27, although a positive initiative, still has ground to cover to match the depth and breadth of protections afforded by its international counterparts.

The European Union: The General Data Protection Regulation

The General Data Protection Regulation (GDPR) is a monumental legislative response to the ever-increasing concerns over data privacy in the era of digitalization. Implemented on May 25, 2018, the GDPR was conceived to harmonize data privacy laws across Europe, protect EU citizens' data privacy, and reshape the approach of organizations worldwide towards data privacy. The regulation's development was predicated on a dual objective: to give individuals control over their personal data and to simplify the regulatory environment for international businesses by unifying regulations within the EU.

The GDPR's approach to data privacy is grounded in a set of principles that emphasize transparency, fairness, accuracy, and accountability. One of the key facets of the GDPR is its focus on informed consent. As stated, Article 4(11) of the GDPR provides a clear definition of consent, mandating that it be freely given, specific, informed, and unambiguous. This definition is a direct response to the rise of "dark patterns" – user interfaces designed to coax users into making unintended decisions, often to the advantage of service providers and at the expense of user autonomy.

In the context of dark patterns, one of the most common tactics employed by businesses is to manipulate users into providing consent without an authentic understanding of what they are consenting to. The GDPR's stance on consent directly addresses this, emphasizing the necessity for clarity and understanding in the consent process. Moreover, the GDPR goes a step further to ensure that once consent is given, it is not locked in perpetuity. Article 7 reinforces the fluidity of consent, emphasizing that data subjects have the right to withdraw their consent with the same ease as they gave it. This provision mitigates the impact of dark patterns that make revocation of

consent a labyrinthine process, ensuring that individuals can seamlessly retract permissions if they feel their data is being mishandled or misused.

Furthermore, the GDPR introduces the principle of "Data Protection by Design and Default." As stipulated in Article 25, this section mandates that organizations integrate data protection measures into their processing activities and systems from the inception stage. This proactive approach ensures that privacy is not an afterthought but is ingrained in the very fabric of operations, thus minimizing the potential for dark patterns to infiltrate user interfaces.

While the principles and provisions of the GDPR set the stage for robust data protection, their efficacy rests on rigorous enforcement mechanisms. The regulation empowers national supervisory authorities to monitor and ensure compliance with the GDPR. As detailed in the provided text, Article 58 of the GDPR enumerates the extensive powers vested in these authorities. From issuing warnings and reprimands to imposing substantial administrative fines, the supervisory authorities are equipped with a diverse toolkit to address violations.

The fines, in particular, act as a significant deterrent against non-compliance. Depending on the severity of the infringement, companies can be fined up to 4% of their annual global turnover or €20 million, whichever is higher. Such substantial penalties underscore the seriousness with which the EU views data protection and serve as a strong incentive for organizations to prioritize user privacy.

Central to the GDPR's enforcement framework is the European Data Protection Board (EDPB). Comprising representatives from the data protection authorities of each EU member state, the EDPB plays a pivotal role in ensuring the consistent application of the GDPR across the EU. The board offers guidance, resolves disputes, and fosters cooperation among national supervisory authorities.

In conclusion, the GDPR represents the European Union's comprehensive approach to safeguarding data privacy in an increasingly interconnected world. By emphasizing informed consent, providing avenues for revoking consent, and instituting stringent enforcement mechanisms, the GDPR offers a robust defense against dark patterns and other deceptive practices.

The United States: The California Consumer Privacy Act

The California Consumer Privacy Act (CCPA) continues to be a ground-breaking piece of legislation that addresses the growing concerns surrounding consumer data privacy in the digital age. Rooted in the recognition of privacy as a fundamental human right, the CCPA provides consumers with the authority to control how their personal information is used by businesses (Cal. Civ. Code § 1798.100, 2020; Cal. Civ. Code § 1798.105, 2020). Originating from mounting public pressure and advocacy initiatives, the Act was signed into law in 2018 and became effective on January 1, 2023.

While the CCPA encompasses a broad range of data privacy provisions, one of its noteworthy aspects is its stance on "dark patterns." Dark patterns, as defined within the Act, are deceptive

user interfaces on websites or applications that can trick consumers into making unintended decisions (Cal. Civ. Code § 1798.145, 2020). This can range from misleading wording, hidden terms and conditions, or even design elements that manipulate users into sharing more data than they intend to. The CCPA explicitly states: “A business shall not use dark patterns to subvert or impair a consumer’s choice to opt-out” (Cal. Civ. Code § 1798.135, 2020). By incorporating this provision, the CCPA acknowledges the pervasive nature of dark patterns and takes a firm stand against such manipulative design practices.

To ensure that consumers are genuinely protected from dark patterns, the CCPA provides clear guidelines on how businesses should facilitate the opt-out process (Cal. Civ. Code § 1798.135, 2020). For instance:

1. A business must provide an easy-to-locate "Do Not Sell My Personal Information" link on its website.
2. The process for opting out should be straightforward and must not necessitate more steps than the process for opting in.
3. Businesses cannot use confusing or unclear language that might deter or mislead consumers from opting out.
4. Requiring consumers to provide unnecessary personal information or to listen to reasons why they should not opt out before confirming their decision is prohibited.

The enforcement of the CCPA and its provisions is a critical component of its effectiveness. Initially, the responsibility of overseeing compliance rested with the Office of the Attorney General (OAG) (Cal. Civ. Code § 1798.155, 2020). However, to bolster the enforcement mechanism and provide a more specialized focus on data privacy issues, California established the California Privacy Protection Agency (CPPA) (Cal. Civ. Code § 1798.199.10, 2020).

The CPPA is vested with the authority to enforce the CCPA and its subsequent expansion, the California Privacy Rights Act (CPRA) (Cal. Civ. Code § 1798.199.40, 2020). With its exclusive focus on consumer data privacy, the CPPA plays a pivotal role in ensuring that businesses adhere to the CCPA's mandates and that violations are promptly addressed (Cal. Civ. Code § 1798.199.60, 2020).

In conclusion, the CCPA represents a significant advancement in consumer data protection in the United States. By explicitly addressing the issue of dark patterns and providing clear guidelines on permissible business practices, the Act empowers consumers and holds businesses accountable. The establishment of the CPPA further underscores California's commitment to safeguarding its residents' data privacy rights. As the digital landscape continues to evolve, the CCPA serves as a benchmark for other states and countries to emulate in the quest for robust data privacy protections.

Mechanisms for reporting dark patterns

Introduction

Privacy legislation plays a crucial role in safeguarding user information and granting individuals control over their data. Among the leading frameworks designed to address these concerns globally are the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, the California Consumer Privacy Act (CCPA) in the United States, and the General Data Protection Regulation (GDPR) in the European Union. These legislative acts embody the forefront of efforts to protect privacy in an age where data breaches and unauthorized data usage have become increasingly common.

While each of these laws has its unique jurisdictional scope and regulatory nuances, they share a common goal: to put mechanisms in place that allow users to report and rectify breaches of their privacy rights. This introduction serves as a precursor to an in-depth analysis of how PIPEDA, CCPA, and GDPR facilitate the reporting of "dark privacy" breaches – incidents where personal data is exploited or mishandled in ways that evade immediate detection by the individuals affected.

PIPEDA

Legal mechanisms behind PIPEDA and OPA

When an individual lodges a complaint under PIPEDA, the Office of the Privacy Commissioner of Canada (OPC) assesses whether the Act covers the issue. If so, the OPC initiates an investigation to determine if there has been a breach of privacy rights or a failure in providing proper access to personal information. These investigations are conducted independently and impartially by the OPC, aiming to resolve complaints and prevent future violations.

During these investigations, the OPC may collect evidence, interact with the respondent organization, review relevant records, and conduct necessary interviews. If a contravention is found, the OPC can issue a report of findings, which may include summaries, findings, recommendations, and any agreements made. While the OPC does not have the authority to impose fines for contraventions, it can enter into a Compliance Agreement, enforceable by the Federal Court, where the respondent commits to implementing measures to address the complaint. If a complainant is not satisfied with the OPC's findings, they can request a hearing on the matter in the Federal Court.

The OPC, as an Agent of Parliament, aims to protect and promote privacy rights in Canada. It works to ensure that organizations comply with their privacy obligations under PIPEDA and offers recommendations to prevent recurring issues. In certain cases, the OPC may publicize its findings if it serves the public interest.

Sources

- General information about PIPEDA and the OPA:

    - https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/
- The full text of the Personal Information Protection and Electronic Documents Act (PIPEDA) on the Justice Laws Website:
    - https://laws-lois.justice.gc.ca/eng/acts/P-8.6/
- PIPEDA compliance help from the Office of the Privacy Commissioner of Canada:
    - https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/
- Information on PIPEDA's fair information principles:
    - https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/?cID=7010g000001YZB6

Mechanisms for user reporting

To file a report or complaint under PIPEDA, the Personal Information Protection and Electronic Documents Act, overseen by the Office of the Privacy Commissioner of Canada (OPC), any Canadian citizen can follow these steps:

1. **Attempt to Resolve the Issue Directly**: Before proceeding to file a formal complaint with the Office of the Privacy Commissioner of Canada (OPC), it is recommended that individuals first attempt to resolve their privacy concerns directly with the organization involved.
    a. This step is important as many organizations have dedicated privacy officers or similar points of contact who can address such concerns. The OPC argue that direct resolution is often quicker and less complex than the formal procedures it requires. They also state it's advisable to keep records of all interactions with the organization for future reference
        i. (https://www.priv.gc.ca/en/report-a-concern/file-a-formal-privacy-complaint/file-a-complaint-about-a-business/guide/).
2. **Gather Information and Documentation**: If the privacy concern cannot be resolved directly with the organization, the next step involves gathering all relevant information and documentation.
    a. The onus is completely on the claimant to supply relevant materials, to build grounds for their claim.
    b. This preparation should include any correspondence with the organization, a detailed description of the personal information involved, and a clear explanation of why the organization's response was unsatisfactory or how the organization is suspected of violating PIPEDA.
    c. According to the OPC, this step is crucial for building a strong foundation for the complaint
        i. (https://www.priv.gc.ca/en/report-a-concern/file-a-formal-privacy-complaint/file-a-complaint-about-a-business/guide/)

        ii. (https://priv.gc.ca/en/report-a-concern/file-a-formal-privacy-complaint/file-a-complaint-about-a-business/instructions_pipeda/)
3. **Submit the Complaint to the OPC:** Once all necessary information is collected, the individual can submit their complaint to the OPC. This can be done online, by mail, or by fax.
    a. The complaint should include a comprehensive account of the issue, the steps already taken to resolve it, and the desired outcome.
    b. The OPC's website offers a complaint form and detailed instructions for submitting a complaint, guiding individuals through the process and ensuring that all necessary details are included.
        i. (https://priv.gc.ca/en/report-a-concern/file-a-formal-privacy-complaint/file-a-complaint-about-a-business/instructions_pipeda/) .
4. **Investigation by the OPC**: After receiving the complaint, the OPC may initiate an investigation.
    a. This process involves examining the information provided by both the complainant and the organization in question.
    b. During the investigation, the OPC may request additional information from either party and may conduct interviews or on-site visits. The objective of the investigation is to determine whether there has been a contravention of privacy rights and to seek resolution of the complaint.
        i. (https://www.priv.gc.ca/en/report-a-concern/file-a-formal-privacy-complaint/file-a-complaint-about-a-business/guide/).
5. **OPC's Findings and Recommendations:** At the conclusion of the investigation, the OPC will issue a report of findings.
    a. This report will detail the investigation's discoveries and include a determination of whether there was a violation of PIPEDA.
    b. Additionally, the report may contain recommendations for the organization to address any identified issues.
    c. While these recommendations **are not legally binding**, they carry significant **persuasive authority** and are critical in **guiding** organizations towards compliance with privacy legislation.
        i. (https://www.priv.gc.ca/en/report-a-concern/file-a-formal-privacy-complaint/file-a-complaint-about-a-business/guide/)
        ii. (https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-complaints-and-enforcement-process/enforcement-of-pipeda/)
6. Further Actions: If the complainant is not satisfied with the outcome of the OPC's investigation, they have the option to pursue further action.
    a. This can include applying to the Federal Court for a hearing on the matter. The Federal Court has the authority to review the OPC's findings and make legally binding decisions, including the award of damages where appropriate.

b. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-complaints-and-enforcement-process/enforcement-of-pipeda/

Case Example Involving Facebook: A notable case that illustrates the OPC's role in overseeing compliance with PIPEDA involved an investigation into Facebook, Inc. The OPC found that Facebook had inadequate safeguards to protect users' personal information. This investigation was triggered by concerns regarding how third-party applications accessed users' personal information and the level of consent obtained by Facebook for this access. The OPC's findings led to recommendations for changes in Facebook's practices to achieve compliance with PIPEDA, demonstrating the potential scale and impact of such investigations (https://priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-complaints-and-enforcement-process/)

GDPR

Legal mechanisms behind the GDPR

The General Data Protection Regulation (GDPR), effective from May 25, 2018, is a significant regulation in the field of data privacy. It applies across the European Union (EU) and affects non-EU organizations that process personal data of individuals in the EU (affects collection of data from Canadians if collaborating with researchers in the EU). Below is a clearer and more detailed explanation of the GDPR, with citations to each article in the GDPR:

The GDPR is designed to harmonize data privacy laws across Europe, protecting the privacy of EU citizens in the increasingly digital era. It is applicable to organizations within the EU as well as those outside the region if they provide goods or services to, or monitor the behavior of EU data subjects, as stated in Article 3.

Under the GDPR, “personal data” is defined as any information relating to an identifiable person, which can range from names and ID numbers to online identifiers and various factors tied to the individual's identity, as detailed in Article 4(1).

Article 6 outlines the legal grounds for processing personal data, including situations such as with consent, for contract necessity, to fulfill legal obligations, to protect vital interests, for public interest, and for legitimate interests.

The principles governing data processing are explicitly mentioned in Article 5, which calls for lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability.

The rights of data subjects have been significantly strengthened by the GDPR, affording individuals rights such as being informed, accessing data, rectifying inaccuracies, erasure (the right to be forgotten), restricting processing, portability of data, objecting to processing, and protections against automated decision-making and profiling, as laid out in Articles 12 through 22.

Article 83 of the GDPR sets out the penalties for non-compliance, which can lead to fines of up to €20 million or 4% of the annual global turnover, whichever is greater.

Certain organizations are required by Article 37 to appoint a Data Protection Officer (DPO) to oversee compliance with the GDPR.

In the event of a privacy breach, organizations must report the incident to the appropriate authority and, in some situations, to the individuals affected, as per Articles 33 and 34.

Articles 44 through 50 restrict the transfer of personal data outside the EU to ensure an adequate level of protection is maintained.

Organizations are mandated by Articles 24, 25, and 35 to demonstrate their compliance with the GDPR, which may include implementing data protection policies and conducting impact assessments.

Finally, enforcement of the GDPR is managed by a particular countries national data protection authorities, with coordination by the European Data Protection Board to ensure consistent application across the EU, as described in Articles 51 through 59.

GDPR: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Mechanisms for user reporting

To file a complaint regarding a possible violation of the General Data Protection Regulation (GDPR), a citizen of the European Union (EU) or European Economic Area (EEA) should indeed follow several steps:

1. **Identifying the National Data Protection Authority (DPA):** It is crucial to identify the DPA in the relevant EU/EEA member state. Each member state has established their own DPA, which serves as a national body responsible for protecting personal data in accordance with Article 8(3) of the Charter of Fundamental Rights of the EU, and these are tasked with enforcing the GDPR within their jurisdiction.
2. **Submitting the Complaint:** The complaint is typically filed online, by email, or by post to the relevant DPA. It should include detailed information about the issue, personal details, the nature of the complaint, and any supporting evidence. This step involves specifying how the GDPR has been breached, adhering to the guidelines provided by the GDPR itself.
3. **Awaiting Response:** After submission, the DPA reviews the complaint and decides on the next course of action. This could include an investigation into the organization accused of violating the GDPR.
4. **Resolution:** Based on their findings, the DPA may take actions like issuing warnings, imposing fines, or ordering changes in data processing practices. The GDPR stipulates substantial fines for violations – up to €20 million or 4% of the total worldwide annual turnover, depending on the nature of the breach.

Case Example

A notable case example of GDPR enforcement is the fine imposed on Google by France's data regulator CNIL in 2019. This case involved complaints about Google's data consent policies and their control over user information. CNIL's decision to impose a €50 million fine on Google was a significant action under the GDPR, emphasizing the importance of clear consent mechanisms and transparent data processing information as mandated by the GDPR. (https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en)

Sources

- https://iapp.org/
- https://gdpr-info.eu/art-77-gdpr/
- https://commission.europa.eu/index_en
- https://gdpr.eu/
- https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

CCPA

Mechanisms for user reporting

The CCPA provides a comprehensive framework for consumers to understand, manage, and protect their personal information, setting a precedent for privacy laws nationwide. For California citizens, navigating the complexities of the CCPA to address privacy concerns involves a series of actionable steps. From identifying the core privacy issue to directly engaging with businesses, and, if necessary, escalating complaints to the California Attorney General's Office, the process is designed to enforce accountability and ensure compliance with the law. This introductory guide aims to demystify the steps a California citizen can take to file a privacy complaint under the CCPA, reflecting the law's intent to empower individuals in the digital age.

For a California Citizen to file a privacy complaint under the CCPA, the following steps must be taken:

1. Identify the Concern: First, the individual should clearly understand and identify their specific privacy concern. This could be related to unauthorized access to personal data, failure of a business to disclose data collection practices, refusal to delete personal data upon request, or any other issue that violates the CCPA.
    a. https://www.oag.ca.gov/privacy/ccpa
2. Contact the Business Directly: Before escalating the matter to a governing body, the individual should contact the business directly. Under the CCPA, businesses are required to provide a method for consumers to submit requests regarding their personal data. This is usually done through a designated email address, a form on the company's website, or a toll-free number.
    a. https://www.consumer-action.org/modules/articles/CCPA-Privacy-Rights

3. Submit a Request or Complaint (to the business): The individual should submit a detailed request or complaint to the business, specifying their concerns and citing the relevant provisions of the CCPA. They should keep records of this communication.
    a. https://www.consumer-action.org/modules/articles/CCPA-Privacy-Rights
4. Wait for a Response: Businesses are required to respond to consumer requests within specific timeframes under the CCPA (usually within 45 days). The resident should wait for the business to respond and resolve the issue.
    a. https://www.consumer-action.org/modules/articles/CCPA-Privacy-Rights
5. Escalate if Necessary: If the business fails to respond adequately or within the required timeframe, or if the individual is not satisfied with the response, they can escalate the issue. This can be done by filing a complaint with the California Attorney General's Office.
    a. https://www.oag.ca.gov/privacy/ccpa
6. File a Complaint with the California Attorney General: The California Attorney General's Office enforces the CCPA. The individual can file a complaint online through the Attorney General's website or by mail. The complaint should include all relevant details about the issue and any correspondence with the business.
    a. https://oag.ca.gov/contact/consumer-complaint-against-business-or-company
7. Follow Up on the Complaint: After filing the complaint, the individual may need to provide additional information if requested by the Attorney General's Office. They should follow up periodically to check the status of their complaint.
    a. https://www.oag.ca.gov/privacy/ccpa
8. Understand Possible Outcomes: The outcome of a complaint can vary. The Attorney General's Office may investigate the complaint, which could lead to legal action against the business if a violation of the CCPA is found. In some cases, the office may provide guidance or mediation to resolve the issue.
    a. https://www.reedsmith.com/en/perspectives/2022/10/california-attorney-generals-most-recent-ccpa-enforcement-activities

Legal mechanisms behind the CCPA

The legal mechanisms behind the California Consumer Privacy Act (CCPA) and its amendment, the California Privacy Rights Act (CPRA), are quite comprehensive and provide a range of rights and obligations. Below is an overview of the key legal aspects we can mention in our article:

- **Consumer Rights:** The CCPA grants consumers several rights concerning their personal information. These include the right to know what personal information a business collects, the right to delete personal information, the right to opt-out of the sale of personal information, and non-discriminatory treatment for exercising these rights. The CPRA further extends these rights to include the right to correct inaccurate personal information and the right to limit use and disclosure of sensitive personal information.
- **Personal Information:** The CCPA defines personal information broadly to include any information that identifies, relates to, or could be linked with a consumer or household. This encompasses a wide range of data, including names, social security numbers, email

addresses, internet browsing history, geolocation data, biometric information, and inferences drawn from such information.

- **Business Obligations**: Businesses covered by the CCPA must inform consumers at or before the point of personal information collection about the types of data being collected and its intended use. They are also required to update their privacy policies annually with detailed disclosures about their data practices.
- **Enforcement and Remedies:** The California Attorney General enforces the CCPA, with the ability to take legal action against non-compliant entities. Under certain conditions, such as a data breach involving unencrypted and nonredacted personal information, consumers may initiate a private lawsuit against a business. For other CCPA violations, enforcement is primarily the responsibility of the Attorney General or the California Privacy Protection Agency.
- **Special Provisions:** The CCPA has specific provisions for different types of information and entities. For instance, it does not apply to medical information covered by other laws like HIPAA, nor does it completely cover employee personal information. The application to business-to-business transactions and website cookies is also nuanced.

Sources

1. California Department of Justice - Office of the Attorney General: https://www.oag.ca.gov/privacy/ccpa
2. Bloomberg Law - California Consumer Privacy Laws: https://pro.bloomberglaw.com/california-consumer-privacy-laws/
3. Jackson Lewis - California Consumer Privacy Act FAQs for Covered Businesses: https://www.jacksonlewis.com/publication/california-consumer-privacy-act-faqs-covered-businesses.

Legislation protecting users from privacy dark patterns

Introduction

Each of these legislative frameworks incorporates specific provisions aimed at curtailing the use of dark patterns by establishing clear, enforceable guidelines for the transparent and fair processing of personal data. By focusing on the mechanisms within PIPEDA, the CCPA, and the GDPR that combat obfuscation (the practice of hiding or distorting information to confuse users), obstruction (making the process of exercising privacy rights difficult), and pressure (pushing users into consenting to practices they might not otherwise agree with), we can understand how these laws protect personal privacy and help individuals make informed decisions about their data. This introduction sets the stage for a deeper exploration of the legislative tools at our disposal to combat privacy dark patterns.

PIPEDA

https://laws-lois.justice.gc.ca/PDF/P-8.6.pdf

Obstruction

Obstruction: "The site increases the effort that users must exert to make a privacy-friendly choice (i.e., by requiring more actions)" (Kelly & Burkell, Under Review, 2024a; 2024b).

Principle 4.3 – Consent

PIPEDA requires organizations to obtain informed consent for the collection, use, or disclosure of personal information. Principle 4.3.2 states that organizations must obtain "knowledge and consent" from individuals. They are required to clearly inform individuals about the purposes for which their information will be used, ensuring the explanation is understandable, thereby making the consent informed and meaningful. Furthermore, Principle 4.3.3 states organizations must not make users consent to unnecessary data collection, use, or disclosure as a precondition for receiving a product or service. They should only require consent for information needed for specific, legitimate purposes.

Principle 4.4 – Limiting Collection

Principle 4.4.1 establishes that organizations can only collect personal information that is necessary for the purposes they have identified. This limits the scope of data collection and helps prevent the unnecessary accumulation of personal data, which could lead to privacy risks. Principle 4.4.2 mandates that the collection of personal information is done fairly and lawfully, prohibiting organizations from misleading or deceiving individuals about the purpose of collection, ensuring consent is not acquired through deceit.

Principle 4.8 – Openness

Principle 4.8 establishes that organizations must provide individuals with easy access to detailed information about their personal information management policies and practices. Principle 4.8.1 states that Organizations must be transparent about their personal information management policies and practices. This includes providing clear information about their policies for handling personal information, which must be readily accessible and in plain language, thus preventing obfuscation.

Obfuscation

Obfuscation: "The site obscures, hides, or omits relevant information and options, with the intent of confusing or misleading the user into making a privacy-invasive choice" (Kelly & Burkell, Under Review, 2024a; 2024b).

Principle 4.1 – Accountability

Principle 4.1 establishes that organizations are responsible for personal information in their possession and must designate individual(s) who are accountable for compliance with PIPEDA. Principle 4.1.4 states organizations are required to establish policies and practices that uphold the principles by:

a) creating procedures to safeguard personal information.
b) setting up processes for handling complaints and inquiries.
c) educating and informing staff about the organization's policies and practices; and
d) producing materials to clarify the organization's policies and procedures to its users.

Principle 4.2 – Identifying Purposes

Principle 4.2 sets out that Organizations must specify the reasons for collecting personal information at or before the time of collection. Principle 4.2.2 sets out that specifying the reasons for collecting personal information at or before the time of collection helps organizations identify the necessary data needed to fulfill these reasons. According to the Limiting Collection principle (Clause 4.4), an organization is required to collect only the information essential for the identified purposes.

Principle 4.3 – Consent

Section 4.3.2 establishes that organizations must obtain "knowledge and consent" by making a conscientious effort to inform individuals about the purposes for using their information. For consent to be valid, these purposes must be communicated clearly enough for individuals to comprehend how their information will be utilized or shared.

Principle 4.4 – Limiting Collection

Principle 4.4.1 establishes that organizations are required to collect personal information selectively, restricting the quantity and kind of data gathered to what is essential for the stated purposes. They must clearly define the types of information they will be collecting within their information management policies and practices, adhering to the Openness principle (Clause 4.8).

Principle 4.8 – Openness

As mentioned above, PIPEDA establishes that organizations must be open about its policies and practices with respect to the management of personal information. This is to the benefit of the user and their decision-making capacity. Also as previously set out, Principle 4.1.4 states organizations are required to establish:

a) procedures to safeguard personal information.
b) processes for handling complaints and inquiries.
c) education for staff about the organization's policies and practices; and
d) materials to clarify the organization's policies and procedures to its users.

Principle 4.9 – Individual Access

Principle 4.9.1 states that upon request, an organization must disclose to an individual if it possesses personal information about them and is "*encouraged*" to reveal the source of this information. The individual must be granted access to their information, though sensitive medical details may be provided via a medical practitioner. Furthermore, the organization must detail how this information has been or is being used and list any third parties to whom it has been disclosed. This information on usage and disclosure could help a user make a more informed privacy choice.

Notes

These principles collectively ensure that organizations must not hide or obscure important information about the use of a user's personal data. For instance, Principle 3 on consent necessitates that individuals are adequately informed in a manner that they can understand, which directly counters obfuscation. Principle 8's requirement for openness obligates organizations to be clear and transparent about their data management practices. Principle 9's right of individual access allows individuals to see and verify the accuracy of their personal information, which can help identify any misleading practices.

Pressure

Pressure: "The site actively encourages the user to make a privacy-invasive choice by presenting the privacy-invasive choice positively, and/or presenting the privacy-friendly choice negatively, through language and visuals" (Kelly & Burkell, Under Review, 2024a; 2024b).

Principle 4.3 – Consent

This principle is central to protecting users from pressure. As stated above—Principle 4.3.2 states that organizations must obtain "knowledge and consent" from individuals. They are required to clearly inform individuals about the purposes for which their information will be used, ensuring the explanation is understandable, thereby making the consent informed and meaningful. Furthermore, Principle 4.3.3 states organizations must not make users consent to unnecessary data collection, use, or disclosure as a precondition for receiving a product or service. They should only require consent for information needed for specific, legitimate purposes.

Principle 4.4 – Limiting Collection

As stated above, Principle 4.4.1 establishes that organizations can only collect personal information that is necessary for the purposes they have identified. This protects users from making a privacy-invasive choice that would otherwise take their information without their knowing. This also limits the scope of data collection and helps prevent the unnecessary accumulation of personal data, which could lead to privacy risks. Principle 4.4.2 mandates that the collection of personal information is done fairly and lawfully, prohibiting organizations from misleading or deceiving individuals about the purpose of collection, ensuring consent is not acquired through deceit.

Principle 4.8 – Openness

As mentioned above, PIPEDA establishes that organizations must be open about its policies and practices with respect to the management of personal information. Ideally, this would prevent organizations from pressuring users into making harmful privacy choices, and users will be able to see and fully understand where their personal information is going/being used for.. Also as previously set out, Principle 4.1.4 states organizations are required to establish:

a) procedures to safeguard personal information.
b) processes for handling complaints and inquiries.

c) education for staff about the organization's policies and practices; and
d) materials to clarify the organization's policies and procedures to its users.

Notes

While PIPEDA does not explicitly mention "pressure" as a concept, these principles collectively work to create an environment where consent must be informed and voluntary, reducing the efficacy of pressure tactics designed to encourage privacy-invasive choices. For enforcement and specific applications, the Office of the Privacy Commissioner of Canada (OPC) would investigate, and address complaints related to such practices under these principles.

CCPA

https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

Obstruction

Obstruction: "The site increases the effort that users must exert to make a privacy-friendly choice (i.e., by requiring more actions)" (Kelly & Burkell, Under Review, 2024a; 2024b).

Cal. Civ. Code § 1798.130

Section 1798.130 (a)(1)(A) of the CCPA mandates that businesses must provide two or more designated methods for submitting requests for information, including, at a minimum, a toll-free telephone number and a website address if the business maintains an internet presence. Ideally, this would simplify the process for consumers to make requests regarding their personal information, and lead to more privacy-friendly choices.

Section 1798.130 (a)(2)(A) asserts that businesses are required to respond to verifiable consumer requests within 45 days, helping to further ensure users are informed and if they have questions, organizations are providing answers. Furthermore, Section 1798.130 (2)(A) asserts that the information must be disclosed and provided free of charge. It should be in a format that is usable and can be transferred to another entity without hindrance.

Section 1798.130 (a)(3)(A) establishes that businesses must disclose any personal information it has collected about a consumer, whether directly or indirectly (including through service providers or contractors), upon receiving a verifiable consumer request (also pursuant to sections 1798.110 or 1798.115).

Section 1798.130 (a)(5) states that businesses must disclose specific information in its online privacy policy or policies and in any California-specific description of consumers' privacy rights. If the business does not have these policies, the required information should be posted on its internet website. This information must be updated at least once every 12 months.

Notes

This section ensures that consumers can easily exercise their rights regarding their personal information while requiring businesses to handle these requests in a transparent, timely, and

consumer-friendly manner. The provisions aim to prevent businesses from creating unnecessary hurdles or using obstructive practices that could deter consumers from managing their personal information.

Cal. Civ. Code § 1798.120

Section 1798.120 establishes that businesses cannot discriminate against consumers who opt out of the sale of their personal information or exercise any other CCPA rights. This includes not denying goods or services, not altering prices, not providing a different quality of service, and not making suggestions that opting out will result in unfavorable treatment.

Section 1798.120 (a) states that consumers have the right to instruct businesses not to sell or share their personal information with third parties at any time, known as the right, to opt-out of sale or sharing.

Section 1798.120 (b) asserts Businesses that sell or share consumers' personal information must inform consumers that their information may be sold or shared and that they have the right to opt-out of this sale or sharing.

Section 1798.120 (c) states Businesses cannot sell or share the personal information of consumers under 16 years of age without affirmative authorization: from the consumer if they are between 13 and 16 years of age, or from a parent or guardian if the consumer is under 13. Businesses that ignore a consumer's age are considered to have knowledge of that consumer's age.

Obfuscation

Obfuscation: “The site obscures, hides, or omits relevant information and options, with the intent of confusing or misleading the user into making a privacy-invasive choice” (Kelly & Burkell, Under Review, 2024a; 2024b).

Cal. Civ. Code § 1798.135

Section 1798.135 (A)(1) establishes that businesses must inform consumers of their rights to opt-out of the sale of personal information and provide a clear and conspicuous "Do Not Sell My Personal Information" link on their homepage, which must direct them to a webpage that enables them to opt-out easily.

Like the "Do Not Sell My Personal Information,” Section 1798.135 (A)(2) asserts businesses must provide a clear link titled “Limit the Use of My Sensitive Personal Information” on their homepage. This enables consumers to restrict the use or disclosure of their sensitive personal information to those uses that are authorized by the law.

Section 1798.135 (A)(3) states Businesses have the option to use a single link that combines the opt-out options for both the sale/sharing of personal information and the use of sensitive personal information, as long as it is easy for consumers to use.

Under Section 1798.135 (A)(4), If a business informs consumers about a charge for a product or service following an opt-out request, it must disclose any financial incentive that applies for the retention, use, sale, or sharing of personal information.

Cal. Civ. Code § 1798.100

Section 1798.100(a)(1) states that at or before the point of collecting personal information, businesses must inform consumers about the categories of personal information they are collecting and the purposes for which they will use it. This includes whether the information is sold or shared. Businesses cannot collect additional personal information or use it for purposes that are not compatible with those disclosed without informing the consumer.

Similar requirements apply specifically to sensitive personal information (Section 1798.100(a)(2)). Businesses must disclose the categories of such information they collect and the purposes for collection and use, including any sale or sharing.

Notes

By setting these requirements, this legislation ensures that businesses are clear and upfront about their data practices, thereby giving consumers the information, they need to make informed choices and prevent businesses from hiding or obscuring how they handle personal data.

Pressure

Pressure: "The site actively encourages the user to make a privacy-invasive choice by presenting the privacy-invasive choice positively, and/or presenting the privacy-friendly choice negatively, through language and visuals" (Kelly & Burkell, Under Review, 2024a; 2024b).

Cal. Civ. Code § 1798.120

As mentioned above:

Section 1798.120 establishes that businesses cannot discriminate against consumers who opt out of the sale of their personal information or exercise any other CCPA rights. This includes not denying goods or services, not altering prices, not providing a different quality of service, and not making suggestions that opting out will result in unfavorable treatment.

Section 1798.120 (a) states that consumers have the right to instruct businesses not to sell or share their personal information with third parties at any time, known as the right, to opt-out of sale or sharing.

Section 1798.120 (b) asserts Businesses that sell or share consumers' personal information must inform consumers that their information may be sold or shared and that they have the right to opt-out of this sale or sharing.

Section 1798.120 (c) states Businesses cannot sell or share the personal information of consumers under 16 years of age without affirmative authorization: from the consumer if they are between 13 and 16 years of age, or from a parent or guardian if the consumer is under 13.

Businesses that ignore a consumer's age are considered to have knowledge of that consumer's age.

Notes

These provisions collectively provide consumers with a straightforward and clear process to exercise their right to opt-out, free from pressure that businesses might otherwise use to discourage opting out, such as complicated procedures or misleading information.

Cal. Civ. Code § 1798.125

Preamble

California Civil Code Section 1798.125 aims to protect consumers from being penalized for exercising their privacy rights under the CCPA. Below is a breakdown of its key dark pattern protections:

1798.125 (a)(1) features a Non-Discrimination Clause. It states that Businesses are prohibited from discriminating against consumers who exercise their rights under the CCPA. This means a business cannot:

1. Deny goods or services.
2. Charge different prices or rates, including through discounts or penalties.
3. Provide a different level or quality of goods or services.
4. Suggest that a consumer will receive a different price or quality of goods or services.
5. Retaliate against an employee or contractor for exercising their rights under the CCPA.

These protections ensure that consumers don't feel pressured to choose between their privacy rights and potential negative consequences.

1798.125 (a)(3) discusses Loyalty Programs. It states that Businesses are allowed to offer loyalty, rewards, or club card programs, which may have different terms for consumers who have opted out of data sale/sharing.

Regarding Financial Incentives 1798.125 (b)(1) states that Businesses may offer financial incentives for the collection, sale, or retention of personal information. However, these incentives must be clearly disclosed and cannot be unjust or coercive. Building on this, 1798.125 (b)(3) states any financial incentive program requires clear, affirmative opt-in consent from the consumer, and consumers must have the ability to revoke their consent at any time. 1798.125 (b)(4) states financial incentive practices must not be unjust, unreasonable, coercive, or usurious.

Notes

This section of the legislation ensures that consumers can make privacy decisions without facing undue pressure, financial penalties, or degraded service from businesses, thereby fostering a fair and respectful marketplace.

Cal. Civ. Code § 1798.130:

As discussed above, 1798.130 establishes businesses must provide information about consumer rights and the collection of personal data in a manner that is understandable and accessible, thus countering obfuscation through design or language.

Cal. Civ. Code § 1798.185(a)(3)(B)

Section 1798.185(a)(3)(B) states that the Attorney General is tasked with establishing rules and regulations that require businesses to use clear and understandable language when providing required notices and information, which helps prevent misleading or pressuring language that could influence user decisions.

GDPR

https://gdpr-info.eu/

Obstruction

Obstruction: "The site increases the effort that users must exert to make a privacy-friendly choice (i.e., by requiring more actions)" (Kelly & Burkell, Under Review, 2024a; 2024b).

Articles 15-22

Preamble

The GDPR confers numerous rights to users, regarding their personal data. These rights empower data subjects under GDPR with control over their personal data, including access, correction, deletion, and limiting how their data is processed, ensuring data privacy, protection, and an almost complete control over what happens with user personal data.

Article 15 – Right of Access by the Data Subject

Data subjects have the right to confirm if their personal data is being processed, access their data, and receive details on processing purposes, data categories, recipients, storage duration, and rights concerning data processing. They're entitled to information on data origins not directly collected from them, automated decision-making processes, including profiling, and safeguards for data transferred internationally. Subjects can request a copy of their data, with possible fees for additional copies, provided in electronic format upon request, while respecting others' rights and freedoms.

Article 16 – Right to Rectification

Additionally, they can have inaccurate or incomplete personal data rectified promptly, ensuring the integrity of their personal information.

Article 17 – Right to Erasure ("Right to be Forgotten")

Data subjects can have their data erased under certain conditions, such as data no longer being necessary, withdrawal of consent, objections to processing, unlawful processing, compliance with legal obligations, or data collected for information society services.

Article 18 – Right to Restriction of Processing

Data subjects can request the restriction of processing under certain conditions, such as disputes over data accuracy, unlawful processing, when data is no longer needed for processing purposes but is required for legal claims or pending an objection to processing.

Restricted data can only be processed with consent or for specific purposes like legal claims or public interest. Data subjects will be informed before lifting a restriction on processing.

Article 19 – Notification Obligation Regarding Rectification or Erasure of Personal Data or Restriction of Processing

Data controllers must inform all recipients of personal data about any rectification, erasure, or restriction of processing in accordance with Articles 16, 17(1), and 18, unless it's impossible or requires disproportionate effort.

Article 20 – Right to Data Portability

Data subjects have the right to receive their personal data in a structured, commonly used, and machine-readable format. They can transfer data to another controller without hindrance where processing is based on consent or a contract and carried out by automated means. This right allows for direct transmission of data between controllers where technically feasible.

Article 21 – Right to Object

Data subjects can object to processing of their personal data based on specific grounds (Articles 6(1)e or f), including profiling. Processing must stop unless the controller demonstrates compelling legitimate grounds that override the interests, rights, and freedoms of the data subject or for legal claims. Outlined in Article 12(2) and (3) specifically, The data subject has the right to object at any time to the processing of their personal data for direct marketing, including related profiling. Upon objection, such data shall not be processed for direct marketing purposes.

For processing for scientific, historical research, or statistical purposes, subjects can object on personal grounds unless it's necessary for public interest tasks.

Article 22 – Automated Individual Decision-making, Including Profiling

Data subjects have the right not to be subject to decisions based solely on automated processing (including profiling) that have legal or similarly significant effects on them. Exceptions include necessity for contract performance, law authorization, or explicit consent.

In permitted cases, suitable measures must protect the data subject’s rights, including a right to human intervention, to express viewpoints, and to contest decisions.

Decisions must not be based on special categories of personal data unless stringent conditions are met and protections in place.

Notes

Obstructive practices that make it more difficult for users to exercise these rights would be in violation of the GDPR. These rights collectively ensure businesses and organizations are

maximizing user ability to make privacy friendly choices. This is exclusive to the GDPR, and there is nothing comparable to it found in either the CCPR or PIPEDA.

Consent (Article 7): The conditions for consent are reinforced under the GDPR. Consent must be freely given, specific, informed, and unambiguous. There must be a clear affirmative action by the data subject. Pre-ticked boxes or inactivity should not constitute consent. This means that users should not be led through unnecessary steps to avoid or opt-out of data processing.

Data Protection by Design and by Default (Article 25): Requires that data protection measures are designed into the development of business processes for products and services. Privacy-friendly settings should be the default condition.

Obfuscation

Obfuscation: "The site obscures, hides, or omits relevant information and options, with the intent of confusing or misleading the user into making a privacy-invasive choice" (Kelly & Burkell, Under Review, 2024a; 2024b).

Article 12 – Transparency

Article 12 of the GDPR focuses on Transparency. Under Article 12.1, data controllers must ensure that any information and communications about data processing provided to individuals, as specified in Articles 13, 14, and communications under Articles 15 to 22 and 34, are delivered in a manner that is clear, transparent, understandable, and easily accessible, employing straightforward language, especially when addressing children. This information should be conveyed in writing or through other methods, including digital formats, if suitable. Additionally, upon the individual's request, information may be given verbally if the individual's identity is verified by other means.

Under Article 12.2, Controllers are required to support individuals in exercising their rights as outlined in Articles 15 to 22. In situations mentioned that are discussed in Article 11(2), controllers cannot deny a request from an individual to exercise their rights under Articles 15 to 22, unless the controller can prove that identifying the individual is not possible.

Article 13 – Information to be Provided

Article 13(1) and (2) outlines the information that must be provided to data subjects at the time personal data is obtained. This includes the purposes of processing, the legal basis for processing, the recipients of the personal data, and other necessary information to ensure fair and transparent processing.

Under Article 13(1) When personal data is collected directly from data subjects, controllers must provide the following information at the time of collection:

1. Controller's Identity and Contact Details: The name and contact information of the controller and, if applicable, their representative.
2. Data Protection Officer (DPO) Contact Details: If applicable, the contact details of the DPO.

3. Processing Purposes and Legal Basis: The purposes for processing the personal data and the legal basis for the processing.
4. Legitimate Interests: If processing is based on legitimate interests (Article 6(1)(f)), the specifics of these interests for the controller or a third party.
5. Recipients of Data: The recipients or categories of recipients of the personal data, if any.
6. International Transfers: If the data will be transferred to a third country or international organization, information about the transfer, including the presence or absence of an adequacy decision by the Commission, or reference to appropriate safeguards and how to obtain a copy or where they have been made available.

Additionally, to ensure fair and transparent processing, under Article 13(2), the following information must also be provided:

1. Data Retention Period: The duration personal data will be stored, or if not determinable, the criteria used to determine this period.
2. Rights of Data Subjects: The rights to access, rectify, erase personal data, restrict processing, object to processing, and data portability.
3. Right to Withdraw Consent: If processing is based on consent, the right to withdraw consent at any time without affecting the legality of processing before withdrawal.
4. Complaints to Supervisory Authority: The right to lodge a complaint with a supervisory authority.
5. Data Provision Requirements: Whether providing personal data is a statutory or contractual requirement, or necessary to enter into a contract, the obligation of the data subject to provide the data, and possible consequences of not providing the data.
6. Automated Decision-Making: Information on the existence of automated decision-making, including profiling, as referred to in Article 22(1) and (4), and meaningful information about the logic involved, as well as the significance and envisaged consequences for the data subject.

Article 7 – Conditions for Consent

Article 7(1) and (2) assert that when processing personal data based on consent, data controllers must be able to prove that the data subject has agreed to the processing of their personal data. If consent is requested as part of a document addressing other matters, the consent request must be clearly distinguishable, presented in a straightforward and accessible way, using clear and simple language. Any part of the declaration that violates this regulation is not enforceable.

Article 7(3) states that fata subjects have the right to withdraw their consent at any time, and this withdrawal does not affect the legality of any data processing that occurred before the consent was withdrawn. They must be informed about their right to withdraw consent before giving it, and withdrawing consent should be as easy as giving it.

Article 7(4) asserts that in determining whether consent was freely given, significant consideration is given to whether the execution of a contract, including the provision of a service, is made conditional on consent to process personal data that is not necessary for fulfilling that contract.

Article 22 – Automated Individual Decision Making

As mentioned above, Article 22 provides individuals the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them. Transparent information about the logic involved and the significance and envisaged consequences of such processing for the data subject must be provided.

Pressure

Pressure: "The site actively encourages the user to make a privacy-invasive choice by presenting the privacy-invasive choice positively, and/or presenting the privacy-friendly choice negatively, through language and visuals" (Kelly & Burkell, Under Review, 2024a; 2024b).

Article 7 – Conditions for Consent

As mentioned in more detail above, the GDPR requires that consent must be freely given, specific, informed, and unambiguous. This means that any form of pressure or influence that detracts from the user's ability to make an informed and voluntary choice is not compliant. As aforementioned, Article 7(3) also requires that the data subject has the right to withdraw consent as easily as it was given, which means that any pressure not to withdraw consent would be against the regulation.

Articles 12 and 13 – Transparency

As outlined above in greater detail, these two Articles require that any information and communication relating to the processing of personal data be easily accessible and understandable, and that clear and plain language is used. This means that under this act, an organization cannot use language or visuals that unfairly pressure or deceive an individual into giving consent or accepting certain privacy terms.

Article 35 – Data Protection Impact Assessment

Article 35 requires a data protection impact assessment to be carried out when the processing is likely to result in a high risk to the rights and freedoms of natural persons. If the use of pressure tactics or misleading designs could affect the rights of the individuals, this would need to be assessed and mitigated.

Article 35(1) states that when engaging in types of processing that, especially through new technologies and considering the nature, scope, context, and purposes, pose a high risk to the rights and freedoms of individuals, controllers are mandated to conduct a Data Protection Impact Assessment (DPIA) before beginning such processing. This assessment can cover a group of similar processing activities with comparable high risks.

Under Article 35(1), Controllers must consult their Data Protection Officer (DPO) during the DPIA process. DPIAs are specifically required when processing involves:

- Systematic and extensive evaluation of personal aspects based on automated processing, including profiling, leading to significant decisions about individuals.
- Large-scale processing of special categories of data or data relating to criminal convictions and offences.
- Large-scale systematic monitoring of publicly accessible areas.

Article 21(2) and (3) – Right to Object

Specifically addressing the concern of protecting users from being coerced into making privacy-invasive decisions, Article 12(2) and (3) stipulates that when personal data are processed for direct marketing purposes, individuals possess an unequivocal right to object at any point. This right extends to any profiling linked to direct marketing. In practice, this means that once an objection is raised, the processing of personal data for these purposes must immediately halt, thereby safeguarding individuals from unwarranted intrusion and potential pressure to acquiesce to privacy-invasive choices.

Note on Article 21(2) and (3)

Digital marketing and targeted ads are one of the largest ways personal data is used by dark patterns to manipulate user ads, often without their consent. This Article allows the user to avoid pressure, by always being in control of their personal data and having the right to opt out of these manipulative practices.

Conclusion

In conclusion, PIPEDA, the CCPA, and the GDPR represent significant strides in the global effort to protect personal privacy in the digital age. By specifically addressing the challenges posed by dark privacy patterns, these laws underscore the necessity of transparent, fair, and accessible mechanisms for individuals to safeguard their personal information and navigate the complexities of the digital world with confidence. The proactive measures embedded within PIPEDA, the CCPA, and the GDPR to combat obfuscation, obstruction, and pressure demonstrate a commitment to not only responding to privacy breaches but also preventing them. As digital technologies continue to evolve, so too must our legislative frameworks adapt to ensure they remain effective in protecting individuals against the ever-changing tactics that threaten personal privacy. This analysis of PIPEDA, the CCPA, and the GDPR provides a foundational understanding of how current legislation addresses the intricate issue of dark privacy, paving the way for future discourse on enhancing and expanding protections to meet the needs of an increasingly interconnected society.

Acknowledgements

This project has been funded by the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the author(s) and do not necessarily reflect those of the OPC.

References

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., & Wilson, S. (2017). Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys*, *50*(3), 1-41. https://doi.org/10.1145/3054926

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economics Literature*, *54*(2), 442–492. https://doi.org/http://dx.doi.org/10.1257/jel.54.2.442

Barocas, S., & Nissenbaum, H. (2014). Big data's end run around anonymity and consent. *Privacy, big data, and the public good: Frameworks for engagement*, *1*, 44-75. https://doi.org/10.1017/CBO9781107590205.004

Bhoot, A. M., Shinde, M. A., & Mishra, W. P. (2020). Towards the identification of dark patterns: An analysis based on end-user reactions. *IndiaHCI '20: Proceedings of the 11th Indian Conference on Human-Computer Interaction*, 24-33. https://doi.org/10.1145/3429290.342929

Bill C-27, *Digital Charter Implementation Act*, 1st Sess, 44th Parl, 2021-2022.

Bösch, C., Erb, B., Kargl, F., Kopp, H., & Pfattheicher, S. (2016). Tales from the dark side: Privacy dark strategies and privacy dark patterns. *Proceedings on Privacy Enhancing Technologies*, *2016*(4), 237-254. https://doi.org/10.1515/popets-2016-0038

Brignull, H. (2010). *Dark patterns*. https://www.darkpatterns.org/

Cal. Civ. Code § 1798.100 (2020).

Cal. Civ. Code § 1798.105 (2020).

Cal. Civ. Code § 1798.198 (2020).

Cal. Civ. Code § 1798.140 (2020).

Cal. Civ. Code § 1798.145 (2020).

Cal. Civ. Code § 1798.135 (2020).

Cal. Civ. Code § 1798.155 (2020).

Cal. Civ. Code § 1798.199.10 (2020).

Cal. Civ. Code § 1798.199.40 (2020).

Cal. Civ. Code § 1798.199.60 (2020).

Christl, W. (2017). *How companies use personal data against people: Automated disadvantage, personalized persuasion, and the societal ramifications of the commercial use of personal information*. https://crackedlabs.org/en/data-against-people

Commission Nationale de l'Informatique et des Libertés. (2019). *Shaping choices in the digital world.* https://linc.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf

The Consumer Policy Research Centre. (2022). *Duped by design – Manipulative online design: Dark patterns in Australia.* https://cprc.org.au/dupedbydesign/

Di Geronimo, L., Braz, L., Fregnan, E., Palomba, F., & Bacchelli, A. (2020). UI dark patterns and where to find them: A study on mobile applications and user perception. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1-14. https://doi.org/10.1145/3313831.3376600

European Data Protection Board. (2022). *Dark patterns in social media platforms: How to recognise and avoid them*. https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en

Forbrukerrådet. (2018). *Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy*. fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

Fritsch, L. (2017). Privacy dark patterns in identity management. *Open Identity Summit 2017: Proceedings*, 93-104.

General Data Protection Regulation, EU 2016/679, [online], available at gdpr-info.eu (last accessed 3 March 2024).

Government of Canada. (2022). *Bill C-27 Summary: Digital Charter Implementation Act, 2022*. https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter/bill-summary-digital-charter-implementation-act-2020

Hansen, P. G., & Jespersen, A. M. (2013). Nudge and the manipulation of choice: A framework for the responsible use of the nudge approach to behaviour change in public policy. *European Journal of Risk Regulation*, *4*(1), 3-28. https://www.jstor.org/stable/24323381

Hausner, P., & Gertz, M. (2021). Dark patterns in the interaction with cookie banners. *CHI Conference on Human Factors in Computing Systems*, 1-5. https://dbs.ifi.uni-heidelberg.de/files/Team/phausner/publications/Hausner_Gertz_CHI2021.pdf

Johnson, E. J., & Goldstein, D. (2003). Do defaults save lives? *Science*, *302*(5649), 1338-1339. https://doi.org/10.1126/science.1091721

Kahneman, D. (2013). *Thinking, fast and slow*. Anchor Canada.

Kelly, D. & Rubin, V. L. (2022). Dark pattern typology: How do social networking sites deter disabling of user accounts? *12th International Conference on Social Media & Society*, July 18 - 19, Toronto, Canada. https://easychair.org/publications/preprint/GD6S

Kelly, D., & Rubin, V. L. (2024). Identifying dark patterns in user account disabling interfaces: Content analysis results. *Social Media + Society*, *10*(1). https://doi.org/10.1177/20563051231224269

Kelly, D., & Burkell, J. (Accepted, 2024). "Every time you tried to make an objectively good decision for your privacy, it tried to persuade you out of it": How teens perceive privacy dark patterns on social media. *2024 International Conference on Social Media and Society, London, England, July 16-18, 2024.*

Kelly, D., & Burkell, J. (Under Review, 2024a). Documenting privacy dark patterns: How social networking sites influence users' privacy choices.

Kelly, D., & Burkell, J. (Under Review, 2024b). Disclosure by design: How dark patterns reduce users' social privacy.

Kirkman, D., Vaniea, K., & Woods, D. W. (2023). DarkDialogs: Automated detection of 10 dark patterns on cookie dialogs. *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*, Delft, Netherlands, 847-867. https://doi.org/10.1109/EuroSP57164.2023.00055

Kroll, T., & Stieglitz, S. (2019). Digital nudging and privacy: Improving decisions about self-disclosure in social networks. *Behaviour & Information Technology*, 1-19. https://doi.org/10.1080/0144929X.2019.1584644

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*, *110*(15), 5802-5805. https://doi.org/10.1073/pnas.1218772110

Luguri, J., & Strahilevitz, L. J. (2021). Shining a light on dark patterns. *Journal of Legal Analysis*, *13*(1), 43-109. https://doi.org/10.1093/jla/laaa006

Lukoff, K., Hiniker, A., Gray, C. M., Mathur, A., & Chivukula, S. S. (2021). What can CHI do about dark patterns? *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems* (*CHI EA '21*), 1-6. https://doi.org/10.1145/3411763.3441360

Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11k shopping websites. *Proceedings of the ACM Human-Computer Interaction*, *3*(81), 1-32. https://doi.org/10.1145/3359183

Mirsch, T., Lehrer, C., & Jung, R. (2017). Digital nudging: Altering user behavior in digital environments. *13th International Conference on Wirtschaftsinformatik, February 12-15, 2017, St. Gallen, Switzerland*, 634-648.

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (*CHI '20*), 1-13. https://doi.org/10.1145/3313831.3376321

Personal Information Protection and Electronic Documents Act S.C. 2000, c. 5

Rossi, A., & Bongard-Blanchy, K. (2021). All in one stroke? Intervention spaces for dark patterns. *Conference on Human Factors in Computing System (CHI'21)*, 1-5. https://doi.org/10.48550/arXiv.2103.08483

Schaffner, B., Lingareddy, N. A., & Chetty, M. (2022). Understanding account deletion and relevant dark patterns on social media. *Proceedings of the ACM Human-Computer Interaction*, *6*(CSCW2), 1-43. https://doi.org/10.1145/3555142

Simon, H. A. (2000). Bounded rationality in social science: Today and tomorrow. *Mind & Society*, *1*, 25-39.

Soe, T. H., Santos, C. T., & Slavkovik, M. (2022). Automated detection of dark patterns in cookie banners: how to do it poorly and why it is hard to do it any other way. *ArXiv,* https://doi.org/10.48550/arXiv.2204.11836

Solove, D. J. (2007). *The future of reputation: Gossip, rumor, and privacy on the Internet*. Yale University Press.

Stavrakakis, I., Curley, A., O'Sullivan, D., Gordon, D., & Tierney, B. (2021). A framework of web-based dark patterns that can be detected manually or automatically. *International Journal on Advances in Internet Technology*, *14*(1&2), 36-45. http://dx.doi.org/10.21427/20g8-d176

Susser, D., Roessler, B., & Nissenbaum, H. (2019a). Online manipulation: Hidden influences in a digital world. *Georgetown Law Technology Review*, *4*(1), 1-39. https://dx.doi.org/10.2139/ssrn.3306006

Susser, D., Roessler, B., & Nissenbaum, H. (2019b). Technology, autonomy, and manipulation. *Internet Policy Review*, *8*(2), 1-22. https://doi.org/10.14763/2019.2.1410

Thaler, R. H., & Sunstein, C. R. (2008). *Nudge: Improving decisions about health, wealth, and happiness*. Penguin Books.

Thaler, R. (2018). Nudge, not sludge. *Science*, *361*(6401), 431. https://doi.org/10.1126/science.aau9241

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science, 185*(4157), 1124-1131.

Tversky, A., & Kahneman, D. (1986). Rational choice and the framing of decisions. *The Journal of Business, 59*(4), S251-S278.

Voigt, C., Schlögl, S., & Growth, A. (2021). Dark patterns in online shopping: On sneaky tricks, perceived annoyance and respective brand trust. In F. FH. Nah, & K. Siau (Eds.), *HCII 2021: HCI in Business, Government and Organizations*. Lecture Notes in Computer Science. https://doi.org/10.48550/arXiv.2107.07893

Waldman, A. E. (2020). Cognitive biases, dark patterns, and the 'privacy paradox.' *Current Opinion in Psychology, 31*, 105-109. https://doi.org/10.1016/j.copsyc.2019.08.025

Wang, Y., Norcie, G., Komanduri, S., Acquisti, A., Leon, P. G., & Cranor L. F. (2011). "I regretted the minute I pressed share": A qualitative study of regrets on Facebook. *Proceedings of the Seventh Symposium on Usable Privacy and Security* (*SOUPS '11*), 1-16. https://doi.org/10.1145/2078827.2078841

Yeung, K. (2017). 'Hypernudge': Big data as a mode of regulation by design. *Information, Communication & Society*, *20*(1), 118-136. https://doi.org/10.1080/1369118X.2016.1186713