

MITRE

# The PANOPTIC™ Privacy Threat Model

Sponsor: MITRE Independent Research and Development (IR&D) Program

The views, opinions, and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

Approved for Public Release. Distribution Unlimited. Public Release Case Number 23-4353.

© 2023 The MITRE Corporation. All Rights Reserved.

**Bedford, MA**

Stuart Shapiro, Cara Bloom, Ben Ballard, Shelby Slotter, Mark Paes, Julie McEwen, Ryan Xu, Samantha Katcher

December 2023

This page intentionally left blank.

# Abstract

Threat modeling is a process which can be used to understand potential attacks or adversaries and is essential for holistic risk modeling. As privacy moves from a compliance- to a risk-based orientation, threat-informed defense will be crucial for organizations' privacy management as it has already become for their cybersecurity management. Yet, privacy lacks a shared threat language and commonly used threat model. This paper describes one effort to address this gap, the development of the Pattern and Action Nomenclature Of Privacy Threats In Context (PANOPTIC™). The model's scope is broader than a cybersecurity threat model by necessity, including both actions and inactions, benign as well as malicious intent, and recognizes the system of concern as a potential threat agent in addition to adversaries outside the system itself. This paper defines a privacy attack – the foundation of the PANOPTIC Privacy Threat Model – and describes the model itself; how it was developed; use cases for the model, such as privacy threat assessments, privacy risk modeling, and privacy red teaming; and future work expanding and enhancing the model.

This page intentionally left blank.

# Table of Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Background</b>	<b>3</b>
2.1	From privacy compliance to privacy risk management	3
2.2	Current state of privacy threat modeling	3
2.3	Current state of security threat modeling	4
2.4	Distinguishing privacy and cybersecurity threat models	4
<b>3</b>	<b>Philosophy and Scope</b>	<b>5</b>
<b>4</b>	<b>Data Generation</b>	<b>8</b>
<b>5</b>	<b>PANOPTIC Taxonomy</b>	<b>11</b>
5.1	Method	11
5.2	Structure and Contents	12
5.3	Mapping an Attack: Nomi Technologies	13
5.4	Critical Choices	16
<b>6</b>	<b>Constraints</b>	<b>18</b>
<b>7</b>	<b>Discussion</b>	<b>19</b>
<b>8</b>	<b>Applications</b>	<b>20</b>
8.1	Privacy Threat Assessment	20
8.2	Privacy Risk Management	20
8.3	Privacy Red Teaming	21
<b>9</b>	<b>Future Work</b>	<b>21</b>
<b>10</b>	<b>Conclusion</b>	<b>22</b>
<b>11</b>	<b>References</b>	<b>23</b>

<b>Appendices</b> . . . . .	<b>27</b>
<b>A Appendix A: PANOPTIC Definitions</b> . . . . .	<b>27</b>
<b>Appendices</b> . . . . .	<b>38</b>
<b>A Appendix B: System Privacy Threat Assessment</b> . . . . .	<b>38</b>

## List of Figures

1	Relationship between privacy risks and cybersecurity risks [1]	5
2	Solove’s Taxonomy of Privacy [2]	6
3	Privacy Attacks in our seed dataset by year	8
4	PANOPTIC Taxonomy Structure	11

## List of Tables

1	PANOPTIC Taxonomy Contents – Privacy Contextual Domains	13
2	PANOPTIC Taxonomy Contents – Privacy Activities	14
A1	PANOPTIC Taxonomy Structure & Definitions – Privacy Contextual Domains	28
A1	PANOPTIC Taxonomy Structure & Definitions – Privacy Contextual Domains	29
A1	PANOPTIC Taxonomy Structure & Definitions – Privacy Contextual Domains	30
A1	PANOPTIC Taxonomy Structure & Definitions – Privacy Contextual Domains	31
A2	PANOPTIC Taxonomy Structure & Definitions – Privacy Activities	32
A2	PANOPTIC Taxonomy Structure & Definitions – Privacy Activities	33
A2	PANOPTIC Taxonomy Structure & Definitions – Privacy Activities	34
A2	PANOPTIC Taxonomy Structure & Definitions – Privacy Activities	35
A2	PANOPTIC Taxonomy Structure & Definitions – Privacy Activities	36
A2	PANOPTIC Taxonomy Structure & Definitions – Privacy Activities	37

This page intentionally left blank.



# 1 Introduction

Threat modeling enables professionals to anticipate the kinds of attacks against which systems or processes need to be guarded and has become an accepted practice of risk management in multiple domains, including cybersecurity [3]. While no definition of threat modeling is all encompassing, Uzunov and Fernandez offer a widely accepted definition, describing threat modeling as “a process that can be used to analyze potential attacks or threats, and can be supported by threat libraries or attack taxonomies” [4]. Threat modeling varies depending on its context of use – modeling physical threats to a building differs from modeling cyber threats to a system – and privacy threat modeling is no different. Privacy threat modeling brings with it the inherent complexity of privacy itself and seeks to identify the ways privacy threat agents can exploit vulnerabilities in digital, physical, and social systems. Given the increasing number of privacy incidents online and offline, it is a reasonable next step for privacy defenses to be threat informed.

Privacy threat modeling begins with a usable definition and scope for privacy to bound the model. Yet privacy scholars cannot agree on a basic definition for the concept of “privacy” [2, 5], partially explaining why there are few existing privacy threat models today. No existing privacy threat model is used as a common standard across organizations, nor has one served as a common language across industries the way some cybersecurity threat models have [6, 7]. PANOPTIC™ is intended to address this gap.

Threat models are just one of the three legs of the risk model “stool” along with vulnerabilities and adverse consequences. Accounting for threats has the potential to elevate a risk model from simply looking at flaws in systems (vulnerability-centric models) to exploring which flaws are the most exploitable (threat-informed defense) [8]. Each of the three components involves its own modeling exercise: a risk model can be thought of as the combination of a threat model, vulnerability model, and adverse consequences model where each model has some alignment with the other models.

The modeling mindset has created some strong privacy consequence and vulnerability models, yet privacy threat modeling lags behind. For instance, Solove’s Taxonomy of Privacy (Harms) organizes 16 specific privacy adverse consequences into four categories [2], while Calo’s dichotomy characterizes consequences as objective and subjective harms [9]; there are privacy vulnerability models, for example Nissenbaum’s Contextual Integrity Theory [5] and the National Institute of Standards and Technology (NIST) Problematic Data Actions [10]. Privacy risk assessment methodologies such as FAIR-P [11] and the NIST Privacy Risk Assessment Methodology (PRAM) [10] similarly incorporate vulnerabilities and adverse consequences while leaving out threats. Even the ubiquitous Privacy Impact Assessments and Data Protection Impact Assessments can be thought of as two-legged risk stools, including vulnerability and adverse consequences components while leaving the concept of threat modeling out [12, 13].

The only published threat model for privacy attacks (that we identified in our literature review) is LINDDUN [14], which breaks the privacy threat landscape down into seven types of privacy threats. In cybersecurity the inclusion of threat modeling has greatly facilitated the industry’s (still incomplete) transition from a compliance-oriented to a risk-oriented mindset, but with privacy we have yet to see such a transition [8].

Despite numerous high-profile privacy incidents over the last decade, the contrast between privacy and cybersecurity in this regard is stark. Calls for a risk-based approach to privacy notwithstanding,

privacy generally remains firmly mired in a compliance-based mode. Aside from any other contributing factor, the paucity of supports for privacy threat modeling in terms of attacks has seriously impeded the ability of privacy professionals to move toward a fully-realized risk-oriented approach. This paper describes one effort to address this gap, the development of the Pattern and Action Nomenclature Of Privacy Threats In Context (PANOPTIC). The motivation, methodology, and resulting taxonomy are discussed, along with projected use of PANOPTIC and plans for its continued development.

PANOPTIC diverges from cybersecurity threat models in a number of ways, re-enforcing the contextual nature of privacy [5] and the numerous differences between cybersecurity and privacy (lack of a shared definition being only one). Perhaps the most essential divergence is that the PANOPTIC model (like LINDDUN [14], along with most privacy vulnerability [15, 16, 12, 13] and consequence models [2, 9]) considers threats to individual people, not threats to information technology and software systems or the organizations responsible for them. This means that the adverse consequences caused by the privacy threat agent are not reputational or regulatory damage to organizations, but the real and sometimes intangible privacy harms done to individuals and groups of people as a result of the actions or inactions of the privacy threat agent.

Like any taxonomy, PANOPTIC is a structured vocabulary. This vocabulary consists of two distinct parts: *Contextual Domains* and *Privacy Activities*. The former reflect various aspects of the socio-technical environment while the latter relate to the different types of potential privacy attack components. Both the contextual domains and the privacy activities are categories under which more granular contextual elements and threat actions respectively are specified. Describing a privacy threat using PANOPTIC consists of selecting the particular threat actions that constitute the attack together with its relevant contextual elements.

The remainder of the paper proceeds as follows: in Section 2 we review background material on privacy threat modeling, in Section 3 we discuss the philosophy behind and scope of PANOPTIC, in Section 4 we detail our data generation process, in Section 5 we describe and show the PANOPTIC Taxonomy, in Section 6 we discuss some constraints that currently apply to PANOPTIC, in Section 7 we review the benefits and limitations of our approach, in Section 8 we discuss the three primary PANOPTIC use cases, in Section 9 we describe our future work plans, and in Section 10 we briefly summarize this paper.

## 2 Background

### 2.1 From privacy compliance to privacy risk management

Historically, organizational privacy efforts have taken an overwhelmingly compliance-oriented approach. While this has been particularly the case in the US, with its patchwork of sector-specific statutes (e.g., [17, 18]), it has also been true of broader privacy regimes, including the EU’s Data Protection Directive (DPD) [19], the predecessor to the General Data Protection Regulation (GDPR) [20]. Compliance-oriented approaches, including compliance with organizational policies, encourage a checklist mentality and a one-size-fits-all presumption [8] that have increasingly run into the realities of complex socio-technical systems.

Growing recognition of these deficiencies over the last decade, mirroring earlier developments in security (e.g., [21, 22]), has produced movement toward an explicit risk management approach. These moves are reflected in the work of, for example, NIST [23], executive agency guidance issued by the White House Office of Management and Budget [24], the California Consumer Privacy Act (CCPA) [25], and the GDPR [20].

At the core of any risk management approach is a risk model that defines the relevant universe of threats, vulnerabilities those threats might exploit, and the adverse consequences that could result. While modeling of privacy consequences and vulnerabilities have benefited from a number of developments (e.g., Solove’s Taxonomy [2] and Nissenbaum’s Contextual Integrity Theory [5]), privacy threat modeling has been notably less generative when it comes to describing privacy attacks, as opposed to threat actors.

### 2.2 Current state of privacy threat modeling

For some time, the only well-known privacy threat model has been the LINDDUN framework [14]. Inspired by the STRIDE security threat model (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) developed at Microsoft as part of its Security Development Lifecycle [26], LINDDUN aims to categorize system privacy threats in a similar manner. To that end, LINDDUN defines attacks related to Linkability, Identifiability, Non-repudiation, Detectability, (information) Disclosure, (content) Unawareness, and Non-compliance. Like STRIDE, LINDDUN construes these threats broadly and situates them in terms of system architecture – processes, data stores, data flows, and external entities.

While LINDDUN is a useful model of threats, it is grounded in potential vulnerabilities, making it a hybrid vulnerability-threat model. Rather than focusing on threat agents, like models such as Persona-non-Grata or on the threats themselves such as Security Cards, STRIDE [26], or the ATT&CK framework [6], LINDDUN is about the opportunity to execute an attack; for example, the possibility of attributing data to an identity – which may or may not be exploited – is more like a vulnerability than a threat. LINDDUN takes steps back towards threat-centric modeling by providing attack trees that break down the seven different types of threats in the LINDDUN model [27] and LINDDUN, beneficially, also provides some guidance on translating threats into risks. LINDDUN can be limited though – it only focuses on software systems rather than including potential privacy threats that can be realized in physical or social systems such as spying or stalking.

It is also a top-down model rather than a bottom-up, data-driven one, meaning that the model may be leaving some threats out of its scope.

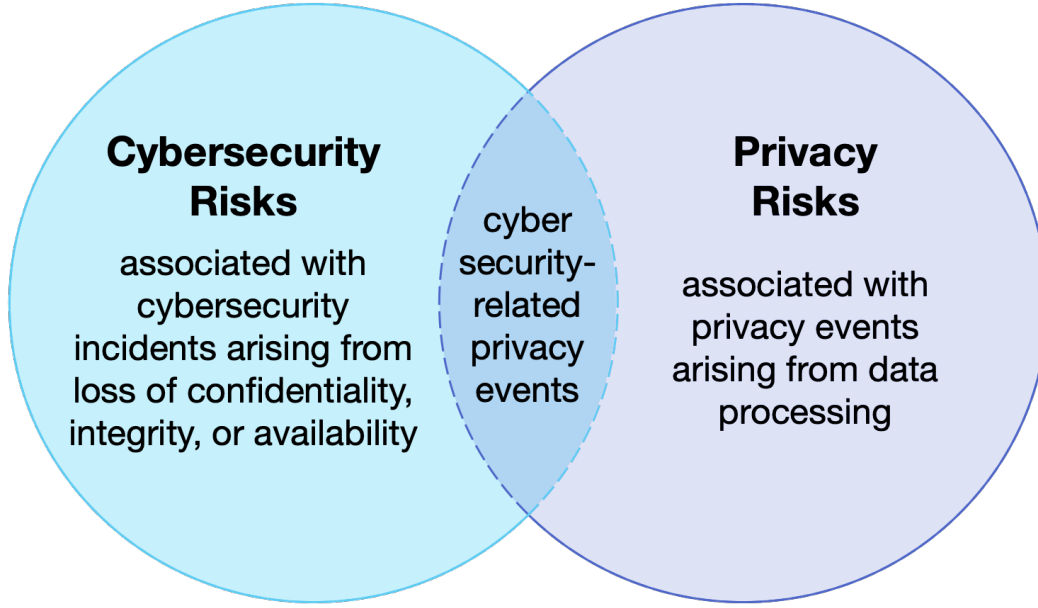
## 2.3 Current state of security threat modeling

While STRIDE is useful for projecting and understanding threat agent goals and general behaviors, it is less useful for projecting and understanding the more specific stepwise actions of an attacker. Addressing this was the motivation behind the development of MITRE ATT&CK®, Adversarial Tactics, Techniques, and Common Knowledge [6]. ATT&CK exhibits several important characteristics, including bottom-up empirical development, a phased sequential structure similar to that of the Lockheed Martin Cyber Kill Chain® [28], and hierarchical categorization of techniques under tactics. Much like LINDDUN took inspiration from STRIDE, PANOPTIC takes its inspiration from ATT&CK, but leverages a larger dataset using a more systematic method. Analogous to ATT&CK, PANOPTIC provides a more granular, stepwise basis for privacy threat modeling built from empirical data.

## 2.4 Distinguishing privacy and cybersecurity threat models

Confidentiality is where privacy and cybersecurity intersect. Moreover, privacy is frequently erroneously equated solely with confidentiality. It is therefore not surprising that the privacy attacks which attract the most attention are data breaches. However, precisely because data breaches typically amount to gross confidentiality failures (i.e., unauthorized accessing of information), they’re best understood in their initial form as cybersecurity rather than privacy attacks (though they may enable downstream privacy attacks). Owing to this, cybersecurity threat modeling appears largely capable of addressing these kinds of attacks [10].

Privacy threat modeling should focus instead on potential attacks against aspects of privacy beyond those that are strictly against confidentiality (e.g., attacks that repurpose personal information for unforeseen purposes). This raises the challenging question of how to systematically identify such non-breach privacy attacks. Garfinkel and Theofanos [29] employed Solove’s well-known Taxonomy of Privacy [2] as a means to this end and we have adapted their approach. In general, we consider these non-breach privacy attacks to be those that result in one or more privacy harms as described by Solove’s Taxonomy (Figure 2).



**Figure 1. Relationship between privacy risks and cybersecurity risks [1]**

### 3 Philosophy and Scope

The PANOPTIC Privacy Threat Model gains external and internal validity from the core philosophies of its creation: all attacks in the *seed dataset* must be found in the wild and all components of the PANOPTIC Taxonomy must be derived from the data themselves. We follow the method from Garfinkel and Theofanos [29], searching for closed US Federal Trade Commission (FTC) and US Federal Communications Commission (FCC) privacy cases that fit our definition of a *privacy attack* and including these cases in our dataset.

We modify the “privacy event” definition from Garfinkel and Theofanos [29] to form our definition of a privacy attack. In this model, a privacy attack is defined as any action or inaction not solely involving cybersecurity violations that could be perceived by affected individuals to cause a privacy harm. If an entity’s action (or inaction) could reasonably cause an individual to perceive that they have experienced one of the harms in Solove’s Taxonomy, we consider it to be a privacy attack so long as it is not solely the result of compromised security.

We determined that if data breaches were included in the model they would overwhelm it and the model would be focused almost exclusively on confidentiality of personally identifiable information (PII) cyber attacks, the overlap section of the Venn diagram in Figure 1. Models such as STRIDE and ATT&CK adequately cover these attacks, so we focus on non-data breaches (the right side of the Venn diagram, not including the overlap) because these complex and heavily contextual cases are under-studied and under-modeled in cyber risk modeling literature.

The PANOPTIC Privacy Threat Model focuses on the attacks themselves, not the threat agents (the groups or individuals capable of carrying out the threat) [30]. In this way PANOPTIC is entirely threat agent-agnostic, differentiating it from agent-focused models such as Persona-non-Grata [26] as well as from cybersecurity threat models, which assume that the system of concern is being attacked by outside actors. In the PANOPTIC model, outside actors are considered in addition

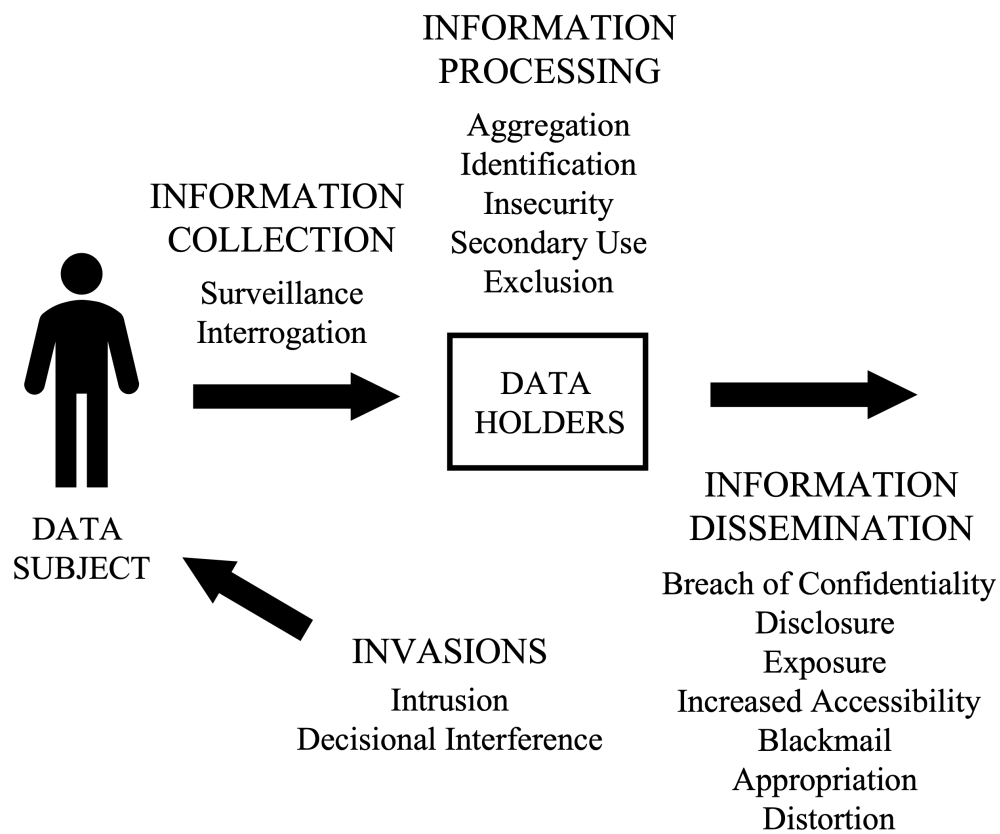


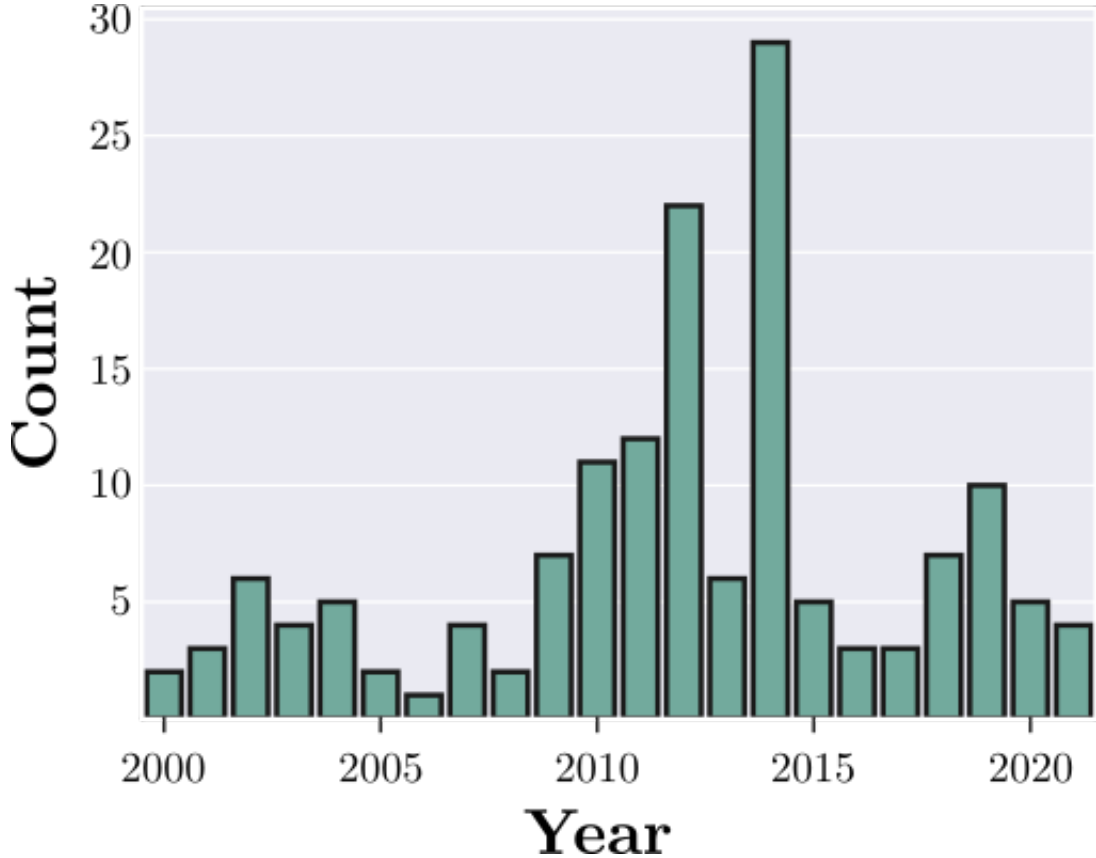
Figure 2. Solove's Taxonomy of Privacy [2]

to the system of concern itself because either can cause privacy harms to individuals engaging with the system. In cybersecurity, issues with the system are vulnerabilities, not exploits, while in privacy the system itself may be responsible for causing harms to individuals. For instance, a social media platform (e.g., Facebook) should consider outside threats (e.g., Cambridge Analytica) as well as the potential threats caused by the platform itself (e.g., Facebook’s emotional contagion study, described in Section 4). In our model, perceived “bad guys” (such as advanced persistent threat actors and other hacking groups) as well as perceived “good guys” (such as companies or government entities that provide useful services) can be a privacy threat agent if they cause a perceived privacy harm through their actions or inactions. PANOPTIC is attack-oriented, threat agent-agnostic, and data-driven, features that arise from the attack definition itself and from the seed dataset.

The seed dataset was used to generate the initial PANOPTIC model. The cases were manually reviewed to ensure they fit our definition of a privacy attack. The final seed dataset consists of 153 privacy attacks taking place from 2000 to 2021. The dataset was enriched with metadata that included details about the progression of the attack. Attacks were then broken down into those component events to create the PANOPTIC Taxonomy, which describes the actions and inactions that make up a privacy attack. We plan to perform clustering analysis on the underlying dataset to generate a typology of privacy attacks that describes common attack patterns – the PANOPTIC Patterns – or generic kill chains of events that differentiate a particular type of attack from other attacks. PANOPTIC is intended to sufficiently describe privacy attacks so as to be usable for privacy threat assessment and privacy threat modeling efforts.

Furthermore, we anticipate that PANOPTIC will be a useful tool for privacy red teaming, a concept highlighted at Black Hat 2022 by Meta [31]. The concept of red teaming is to emulate the behavior of a threat agent to test whether systems and processes can defend against the attack. Organizations can use PANOPTIC to identify which threats are most relevant to their system so they can emulate these attacks and identify potential outcomes. Privacy red teaming, unlike cybersecurity red teaming, will involve emulating both actions (and inactions) from outside the system of concern and potential actions (and inactions) within the system itself.





**Figure 3. Privacy Attacks in our seed dataset by year**

## 4 Data Generation

We assembled a seed dataset to be used for development of the taxonomy-based threat model. We started by following the method from Garfinkel and Theofanos [29] to assemble the seed dataset (introduced in Section 3), expanding the total number of cases from the earlier paper by over one hundred privacy attacks. We then diverged significantly and went beyond [29] by structuring attack components and relevant meta data into a privacy threat model.

For the attacks in the seed dataset we used the keyword “privacy” to search for closed cases referencing privacy from 2000 to 2021 on the FTC and FCC websites, then manually reviewed the down-selected cases to determine if they fit our definition of a privacy attack. Garfinkel and Theofanos included some cases that were identified by experts in addition to those found by searching the FTC and FCC websites and some cases in their dataset were general descriptions of a type of case (e.g., revenge porn), rather than specific instances of that type of attack. All specific cases from the [29] dataset are included in the PANOPTIC seed dataset except those occurring before 2000 and the general cases. The resulting seed dataset includes 153 cases, 122 from the FTC (including 14 identified by both our search and [29]), 10 from the FCC (including 6 identified by both our search and [29]), and 41 from the [29] set only. The latter type of cases did not refer to closed FTC or FCC cases, rather privacy attacks that involved lesser regulatory actions or those without any regulatory action. Privacy attacks in our seed dataset are reported by year in Figure 3.

As stated in our privacy attack definition, each attack had to cause (or be reasonably perceived by



affected individuals to cause) at least one harm from Solove’s Taxonomy. If the only harm was “Insecurity” then the attack was not included in the final seed dataset because it was exclusively a cybersecurity incident with no further privacy harms. Attacks where data were inadvertently made available to unintended entities, such as those recorded in the Privacy Rights Clearinghouse Database [32], are not considered cybersecurity-only breaches, and were therefore included in the seed dataset. Although the Privacy Rights Clearinghouse Database was considered as source material for the PANOPTIC seed dataset, it was excluded because it only describes one type of privacy attack, which was already included in our dataset of FTC, FCC, and [29] attacks.

Metadata were recorded about each privacy attack including: year, type and number of individuals or groups affected, data types, groups or entities involved in the attack, relevant harms from Solove’s Taxonomy, and the attack story, an approximately one paragraph summary description of the attack.

Privacy attack definition compliance and inclusion in the seed dataset were determined by one researcher and verified by an independent researcher. Disagreements and unclear cases were brought to the entire team of seven researchers for discussion. Each member of the team read the attack story; if needed, additional information was gathered and appended. While almost all cases brought to the entire team were decided by consensus, occasionally cases were included or excluded in the seed dataset by majority vote.

Two examples of the 153 attacks included in the seed dataset are given below:

**Privacy Attack Name:** Nomi Technologies

**Privacy Attack Story:** In 2014, Nomi Technologies provided retailers with a technology that could log consumers' movements at their stores. These sensors collected the MAC addresses of consumer mobile devices and other data (device type, date and time the device was observed, and device signal strength) without consumers' awareness [33]. The MAC addresses were hashed, but since it is unique to a consumer's mobile device, it could still be tracked over time. Nomi collected data from individuals inside and outside their stores. Nomi aggregated the data and gave reports to clients about consumer behavior such as how long consumers stayed in the store, how many individuals were repeat customers, and how many customers visited another of the chain's locations [34]. Nomi policy said it allowed consumers to opt out of Nomi's service in-store and online, but there was no mechanism for in-store opt out. Consumers were not informed of tracking in stores. The FTC subsequently issued a complaint and settled deception charges against Nomi [33].

**Solove Harms:** Surveillance (Collection), Secondary Use (Processing), Disclosure (Dissemination)

**Privacy Attack Name:** Facebook Emotional Contagion

**Privacy Attack Story:** In 2012, Facebook partnered with Cornell researchers to perform an experiment on 689,003 of the platform's users to find evidence of "emotional contagion," a phenomenon in which people transfer positive or negative emotions to others without their awareness. The company curated the users' news feeds with more positive or negative posts to measure the effect on the content of each targeted user's posts [35]. Facebook and the researchers failed to obtain consent from or provide notice to users involved in the experiment, leaving users with no ability to opt out from the emotional manipulation [36]. The study cited users' acceptance of Facebook's Data Use Policy, which included no reference to "research" until four months after the study took place, as informed consent. Publication of the experiment's methods and findings prompted significant public backlash for not providing users an opportunity to opt out of the study, as well as for potentially causing harms to users by increasing negative emotions [37].

**Solove Harms:** Decisional Interference (Invasion)

Privacy Contextual Domains						Privacy Activities												
PC01	PC02	PC03	PC04	PC05		PA01	PA02	PA03	PA04	PA05	PA06	PA07	PA08	PA09	PA10	PA11	PA12	PA13
PC01.01	PC02.01	PC03.01	PC04.01	PC05.01	PC05.09	PA01.01	PA02.01	PA03.01	PA04.01	PA05.01	PA06.01	PA07.01	PA08.01	PA09.01	PA10.01	PA11.01	PA12.01	PA13.01
PC01.02	PC02.02	PC03.02	PC04.02	PC05.02	PC05.10	PA01.02	PA02.02	PA03.02	PA04.02	PA05.02	PA06.02	PA07.02	PA08.02	PA09.02	PA10.02	PA11.02	PA12.02	PA13.02
	PC02.03		PC04.03	PC05.03	PC05.11	PA01.03	PA02.03	PA03.03	PA04.03	PA05.03	PA06.03	PA07.03		PA09.03	PA10.03	PA11.03		PA13.03
	PC02.04			PC05.04	PC05.12	PA01.04	PA02.04	PA03.04	PA04.04		PA06.04	PA07.04		PA09.04		PA11.04		PA13.04
				PC05.05	PC05.13	PA01.05	PA02.05	PA03.05	PA04.05		PA06.05	PA07.05		PA09.05		PA11.05		
				PC05.06	PC05.14	PA01.06	PA02.06	PA03.06			PA06.06	PA07.06				PA11.06		
				PC05.07	PC05.15		PA02.07	PA03.07			PA06.07	PA07.07						
				PC05.08	PC05.16			PA03.08			PA06.08	PA07.08						
								PA03.09			PA06.09							
								PA03.10			PA06.10							

**Figure 4. PANOPTIC Taxonomy Structure**

## 5 PANOPTIC Taxonomy

Version 1 of the PANOPTIC Taxonomy is based on the attack stories from the seed dataset and consists of Privacy Threat Actions organized under different Privacy Activities. Privacy Threat Actions are individual actions taken or not taken by an entity that can be perceived to, in combination with other privacy threat actions, cause a privacy harm. Threat Actions are grouped into Privacy Activities, which are categories of actions an entity can take in relation to a privacy attack (e.g., collection, aggregation, processing, and sharing).

### 5.1 Method

Creation of the PANOPTIC Taxonomy began by structuring all of the 153 attack stories from the seed dataset into specific, discrete sub-events, such as “individuals were tracked using unique identifiers captured via Bluetooth.” Patterns/commonalities were identified across the dataset of sub-events. As we identified those common elements, we coded them with descriptive phrases, like “data collected via tracking” and “sensitive data were inferred” that we designated Privacy Threat Actions.

During this process, higher level categories were labeled Privacy Activities and new Privacy Threat Actions were added to applicable Privacy Activities. The structuring effort was performed collectively within the group of seven researchers. As the effort continued with new privacy attacks, proceeding iteratively through the seed dataset, the Activities and Threat Actions were renamed and reorganized and new Activities and Threat Actions were added.

Once a taxonomic structure emerged, we began a series of iterative mapping exercises where randomly selected privacy attacks from the seed dataset were mapped to the PANOPTIC Taxonomy by an individual researcher, who brought unclear Privacy Activity and Privacy Threat Action mappings and potential new Activities and Threat Actions to the group for discussion. Consensus determinations were made for adding, removing, merging, separating, and renaming Activities and Threat Actions. This process continued until half of the 153 attacks in the seed dataset had been mapped to the Taxonomy. It was important to perform this process randomly because technological development and FTC and FCC priorities change from year to year, with different types of cases

becoming more and less common over time. Rather than checking for inter-coder agreement, a subset of cases were mapped by the entire group, which served as a calibration exercise; the rest were mapped by individual team members. Any questions or issues arising from the individual mappings were discussed and resolved by the whole team.

The process of defining the Privacy Activities and Privacy Threat Actions brought up new discussions and led to additional changes to the PANOPTIC Taxonomy. During this effort the group decided collectively on final names and definitions for each Activity and Threat Action. Occasionally Privacy Threat Actions were found to be overlapping with other Threat Actions or were entirely subsumed by them, in which case the Threat Actions were either merged or separated, and some Privacy Threat Sub-actions were created. For each decision, applicable cases were brought to bear and discussed in the context of the decision at hand.

In parallel with this effort, the team identified Privacy Contextual Domains, or groupings of Privacy Contextual Elements that define the contextual environment of a privacy attack. Privacy Contextual Domains include important non-threat actions such as the data type(s), affected population(s), and types of interaction(s) between the threat agent and the individual harmed. This is something that distinguishes PANOPTIC from a cybersecurity model such as ATT&CK and is reflective of the importance of context in privacy. While these Contextual Domains are based on the same foundational assumption about privacy as Nissenbaum’s Contextual Integrity parameters [5] (that privacy is contextual) and function similarly, they are not the parameters themselves.

## 5.2 Structure and Contents

The PANOPTIC Taxonomy includes two related taxonomies: the socio-technical environment with Privacy Contextual Domains and Privacy Contextual Elements and the attack path with Privacy Activities and Privacy Threat Actions. In Tables 1 and 2 each Privacy Contextual Domain and Privacy Activity is listed with its identification number,<sup>1</sup> name, definition, and component Privacy Contextual Elements or Privacy Threat Actions. Contextual elements within a given Contextual Domain and Threat Actions within a given Privacy Activity are almost never mutually exclusive. Privacy Contextual Sub-elements and Privacy Threat Sub-actions are not included in the table but can be found in the Appendix along with the definitions of all components of the Taxonomy.

The use of two component taxonomies is essential given the generally recognized importance of context for privacy. This context can be crucial to understanding an attack and, in some cases, may be instrumental in distinguishing a privacy attack from an otherwise benign set of actions. In the Nomi attack, for example, the fact that location (PC05.01 Data type: Location) tracking (PA03.03 Collection: Tracking and Affording Tracking) took place in a specific physical environment (PC01.02 Environment: Physical) while the opt-out mechanism was only available online created a disconnect (PA01.06 Notice: Misleading/false). The Nomi attack is analyzed in greater detail in the next section. In the Facebook emotional contagion attack, the curation

---

<sup>1</sup>Privacy Contextual Domains and Contextual Elements are denoted PC<Contextual Domain Number>.<Contextual Element Number>.<Contextual Sub-element Number> followed by the Contextual Domain, Contextual Element, and Contextual Sub-Element names separated by colons (e.g., the data type PC05.13.01 Data Type: Psychographic: Preferences). Privacy Activities and Threat Actions are denoted PA<Activity Number>.<Threat Action Number>.<Threat Sub-action Number> followed by the Activity, Threat Action, and Sub-threat Action names separated by colons (e.g., the use PA11.03.01 Use: Reprisal).

**Table 1. PANOPTIC Taxonomy Contents – Privacy Contextual Domains**

<b>ID</b>	<b>Contextual Domain</b>	<b>Definition</b>	<b>Contextual Elements</b>
PC01	Environment	The contextual domain in which a data action occurs	PC01.01 Digital, PC01.02 Physical
PC02	Distribution	How many entities with which the information holder shares information	PC02.01 No distribution, PC02.02 One to one, PC02.03 One to many, PC02.04 One to everyone
PC03	Interaction	The extent to which an individual or their proxy interact with the entity or their proxy	PC03.01.01 Individual interaction, PC03.01.02 Proxy Interaction
PC04	Engagement	Targeted subpopulations with which the entity or their proxy interact	PC04.01 Populations with sensitive characteristics, PC04.02 Specific individuals, PC04.03 Biased population samples
PC05	Data Type	Classes of data upon which data actions are performed	PC05.01 Location, PC05.02 Demographic, PC05.03 Biometric, PC05.04 Recording, PC05.05 Credentials, PC05.06 Contact information, PC05.07 Health, PC05.08 Financial, PC05.09 Employment, PC05.10 Social/personal network, PC05.11 Criminal, PC05.12 Social media, PC05.13 Psychographic, PC05.14 Behavior, PC05.15 Identity, PC05.16 Other sensitive information

of user news feeds (PA03.07 Collection: Interception) aimed to evoke changes (PA11.03 Use: Manipulation) in their emotional state (PC05.16 Data type: Other sensitive), which differentiated it from, for instance, typical A/B testing.

### 5.3 Mapping an Attack: Nomi Technologies

Systems of interest, threat landscapes, and individual attacks can be mapped to the PANOPTIC Taxonomy to gain a better understanding of the threat(s). We include the following mapping of a single attack, Nomi Technologies (described in Section 4), as an example of the explanatory capacity of PANOPTIC. Nomi Technologies is a company that works with retailers to develop customer insights by tracking individuals inside and outside retail establishments via bluetooth sensors.

Systems of interest, threat landscapes, and individual attacks can be mapped to the PANOPTIC Taxonomy to gain a better understanding of the threat(s). We include the following mapping of a single attack, Nomi Technologies (described in Section 4), as an example of the explanatory capacity of PANOPTIC. Nomi Technologies is a company that works with retailers to develop customer insights by tracking individuals inside and outside retail establishments via bluetooth sensors.

The Nomi privacy attack occurred in both digital and physical environments because some potential interactions between Nomi and individuals occurred virtually (PC01.01 Environment: Digital) and

**Table 2. PANOPTIC Taxonomy Contents – Privacy Activities**

<b>ID</b>	<b>Activity</b>	<b>Definition</b>	<b>Privacy Threat Actions</b>
PA01	Notice	Informing an individual or their proxy of one or more data actions	PA01.01 Out of sequence, PA01.02 Unclear, PA01.03 Imprecise, PA01.04 Absent, PA01.05 Insufficient, PA01.06 Misleading/false
PA02	Consent	Assent from an individual or their proxy to one or more defined data actions	PA02.01 Out of sequence, PA02.02 Imprecise, PA02.03 Absent, PA02.04 Insufficient, PA02.05 Misleading, PA02.06 No opt in/out, PA02.07 Inherited
PA03	Collection	The gathering or extraction of information	PA03.01 Application or device use, PA03.02 Registration, PA03.03 Tracking and affording tracking, PA03.04 Sniffing and affording sniffing, PA03.05 Pretexting, PA03.06 External appropriation, PA03.07 Interception, PA03.08 Soliciting and affording soliciting, PA03.09 Recording, PA03.10 Transaction
PA04	Insecurity	Insufficient data protection controls	PA04.01 Insufficient access controls, PA04.02 Insufficient encryption, PA04.03 Undermining or interfering with authentication, PA04.04 Detection failure, PA04.05 Misconfigured permissions
PA05	Identification	How information is associated with an individual	PA05.01 Implicit identification, PA05.02 Identifier assignment, PA05.03 Compulsory self-identification
PA06	Quality Assurance	Implementing policies or processes to ensure quality throughout privacy-related activities	PA06.01 Age not verified, PA06.02 Unvetted data source, PA06.03 Unvetted data quality, PA06.04 Unvetted recipients, PA06.05 Unvetted downstream practices, PA06.06 Insufficient communication of downstream requirements, PA06.07 Data insufficiently de-identified, PA06.08 Data out of scope, PA06.09 Data action out of scope, PA06.10 Insufficient agreed usage restrictions
PA07	Manageability	Enabling an individual or their proxy to access, modify, copy, or destroy information about the individual	PA07.01 No individual access to information, PA07.02 No individual management of information, PA07.03 No individual deletion of information, PA07.04 No individual control over information disclosure, PA07.05 Privacy configurations compromised by outside forces, PA07.06 Confounded user controls, PA07.07 Bypass of user controls, PA07.08 Pre-emption of privacy settings
PA08	Aggregation	Assembling data from multiple sets of data	PA08.01 Profiling, PA08.02 Clustering
PA09	Processing	Extracting and developing value and utility from information	PA09.01 Deriving new information, PA09.02 Behavioral analysis, PA09.03 Introducing bias, PA09.04 Trawling datasets for information, PA09.05 Internal appropriation
PA10	Sharing	Making information available to another entity	PA10.01 Affording revelations, PA10.02 Exposure, PA10.03 Misrepresentation
PA11	Use	Leveraging information to achieve a goal	PA11.01 Implication, PA11.02 Targeting, PA11.03 Manipulation, PA11.04 Intrusion, PA11.05 Selling, PA11.06 Reprisal
PA12	Retention & Destruction	Actions that affect the persistence of information	PA12.01 Data not destroyed after use, PA12.02 Data improperly destroyed
PA13	Deviations	Data action diverges from established limits bounding the data action in question	PA13.01 Deviating from usage agreements, PA13.02 Deviating from stated policy or user agreements, PA13.03 Deviating from claimed certification conformance, PA13.04 Deviating from regulatory requirements

others occurred due to physical surveillance (PC01.02 Environment: Physical). Nomi shared the aggregate data with the specific retailer from whose store the original data had been collected (PC02.02 Distribution: One to one), but it also indicated whether customers had visited other chain locations as well (PC02.03 Distribution: One to many). Individuals did not need to interact directly with Nomi to be involved in the attack (PC03.01.01 Interaction: Individual interaction: No interaction) but the individual's phone, which is a proxy for the individual, was tracked while in range of Nomi's sensors (PC03.02.02 Interaction: Proxy interaction: Discrete interaction). Because Nomi was not specifically engaging with a certain population (they tracked any individuals within range, regardless of identity-related factors) no specific engagement contextual elements were selected. The data types Nomi collected were location (PC05.01), behavior (PC05.14), and MAC address, which is a persistent pseudo-identifier (PC05.15.02).

Moving on to Privacy Activities, because Nomi provided notice of store tracking online, but not, contrary to its online claim, within stores, notice was out of sequence (PA01.01) since customers were unlikely to have seen the notice prior to visiting a store. By the same token, the online notice was misleading/false (PA01.06). Similarly, while Nomi did provide an online opt-out mechanism, there was no such in-store provision (again contrary to the online notice), therefore consent was also out of sequence (PA02.01) and the promised opt-out was unavailable (PA02.06 Consent: No opt-out/in). Data collection occurred via tracking (PA03.03 Collection: Tracking and affording tracking) and sniffing (PA03.04 Collection: Sniffing and affording sniffing) because Nomi collected data about individuals' physical movements and collected emanations from their mobile devices. Nomi identified individuals by hashing their phone MAC address, which is a constructed identifier (PA05.02.01 Identification: Identifier assignment: Fingerprinting). Nomi created individual profiles (PA08.01.01 Aggregation: Profiling: Single source) as well as aggregate views of store customers (PA08.02.01 Aggregation: Clustering: Single source). Nomi derived aggregate shopping information (PA09.01.02 Processing: Deriving new information: Deriving aggregate information) and performed behavioral analysis (PA09.02 Processing: Behavioral analysis). They shared aggregate data with each retailer (PA10: Sharing), but no specific threat actions apply. Nomi failed to comply with their stated policy (PA13.02 Deviations: Deviating from stated policy or user agreement). There were no insecurity, quality assurance, manageability, or retention and destruction-related privacy threat actions in this attack.

This mapping codifies and explains the attack story in which Nomi Technologies surveilled shoppers. Using PANOPTIC, multiple attacks can be mapped, leading to a heat map that describes a threat environment, or individual attacks can be mapped for greater explainability and understanding of the context and activities of the attack. Systems of interest can also be mapped to PANOPTIC, identifying which threat actions are afforded by the system itself. In this way, PANOPTIC can be used both retroactively, to explain an attack, and proactively, to identify potential future attacks.

## 5.4 Critical Choices

While cybersecurity threat models can be used to simulate attacks on systems, privacy threat models – at least PANOPTIC and LINDDUN – are about threats to people. This is a fundamental shift in the threat modeling mindset. Instead of harm to an organization’s reputation or regulatory risk, PANOPTIC focuses on actions or inactions that cause a perceived privacy harm to individuals or groups. In privacy regulatory, reputational, and financial risks to organizations stem from risks to people. If the organization is not first threatening people, it is unlikely that the second order organizational risks will be realized.

Due to their focus on harms to individuals and the complex nature of privacy, privacy threat models must cover a wider threat space than cybersecurity threat models. Cybersecurity threat models (with the notable exception of insider threat models) need only cover malicious actions taken by an entity from outside the system itself. But privacy harms can arise not only from malicious actions but also benign actions and malicious or benign inactions, both from outside agents and the system of concern itself.

In the PANOPTIC Taxonomy, Privacy Activities are neither malicious nor benign – they are neutral privacy activities – but Privacy Threat Actions cannot be exclusively benign. This was a difficult decision by the team: some argued for including benign actions to create a complete picture of a privacy attack (for example including opt-in separately from opt-out), while others proposed that the model would not be a true threat model if you could model entirely benign activities with it. If there were an exclusively benign action in every Activity, then if each were selected the resulting kill chain might not be a privacy attack, since no actions caused harm. The latter group prevailed and it was decided that actions that can be either harmful or benign would be included, for example PA03.02 Collection: Registration, as well as actions that are exclusively or almost exclusively malicious such as PA10.02.01 Sharing: Exposure: Doxxing, but that purely benign actions would be excluded.

While these are overarching decisions about the focus of the PANOPTIC Privacy Threat Model, numerous lower-level decisions were made that impact the Taxonomy and its component Privacy Activities and Privacy Threat Actions. Three such decisions were the inclusions of PA04 Insecurity, PA13.04 Deviations: Deviating from regulatory requirements, and PA11.02.01 Use: Targeting: Tailored Content.

We mirror many cybersecurity threat models which have one privacy-centric component (such as STRIDE’s Information Disclosure [26] by including a cybersecurity Activity in PANOPTIC. Insecurity in PANOPTIC is defined as “insufficient data protection controls” and captures the component of a privacy attack where a cybersecurity mechanism is insufficiently protecting personal information or individuals. When mapping individual attacks from the seed dataset to the Taxonomy, there were only five types of cybersecurity issues that were relevant to the attacks (e.g., PA04.02 Insecurity: Insufficient encryption and PA04.05 Insecurity: Misconfigured Permissions) and these issues were central to the attack. Not including them would have meant that the PANOPTIC Taxonomy did not fully capture the nuances of the attack.

While PANOPTIC is not a regulatory compliance model, we did decide to include PA13.04 Deviations: Deviating from Regulatory Requirements, defined as “an entity is violating a specific regulation that applies to it.” We find that the inclusion of this Threat Action reflects the nature of



the seed dataset: we sought out privacy attacks that rose to the level of FTC or FCC regulatory action (except for the attacks identified by experts in [29]). Our seed dataset is regulatory-focused and includes many cases where the Children’s Online Privacy Protection Act (COPPA) [38] or the now defunct US-EU Safe Harbor [39] framework were violated by an entity. This Threat Action was included to capture cases where a regulation is violated because such violations lead to the perception or actuality of harms to individuals. The regulations afford certain rights and protections to individuals, therefore violations of these regulations are an infringement on the rights and protections of the individual, which can constitute a privacy harm.

Some Threat Actions include Threat Sub-actions. Sub-actions are specific types of Privacy Threat Actions, and – unlike Privacy Threat Actions – may not cover the entire action space of the Threat Action itself. For instance, PA11.02 Use: Targeting has one Sub-action (PA11.02.01 Use: Targeting Tailored Content) though there are certainly other types of Targeting in our dataset. Tailored Content was a particularly prevalent type of Targeting, so we found it helpful to include it in the PANOPTIC Taxonomy. It refers to specific cases of distinguishing an individual for particularized treatment (Targeting) where the content a user sees is manipulated (Tailored Content). There were many cases of targeted advertisements in our seed dataset which fall under Tailored Content, as well as privacy attacks like Facebook’s launch of the “Year In Review” feature, where individuals were shown a highlights reel of posts from the previous year which sometimes included painful memories such as the death of a loved one or another traumatic experience [40]. While these practices are now commonplace [41, 42, 43], at the time this change in application behavior violated privacy norms and was seen as harmful by individuals, leading to FTC action.

## 6 Constraints

PANOPTIC Version 1 can only reliably generalize to FTC and FCC privacy cases, since these are the sources for the attacks in the seed dataset. Our seed dataset is therefore biased towards the United States’ regulatory environment. We have mapped a second dataset to the Taxonomy that we have generated by searching the *New York Times* and the [reddit.com/r/privacy](https://www.reddit.com/r/privacy) online forum for privacy attacks that fit our definition. The resulting dataset includes around 150 recent privacy attacks and is much broader: attacks from multiple (mostly English speaking) nations are included as well as attacks that did not involve regulatory action but nonetheless caused privacy harms. The iterative mapping of this second dataset has helped alleviate some of the biases in the seed dataset and the resulting Version 2 of PANOPTIC will be a more holistic and robust model.

While a powerful tool for breaking down and describing privacy attacks, PANOPTIC currently lacks a method by which a user can differentiate between a threat action that potentially contributes to a privacy harm and a threat action that does not. When modeling a series of actions using PANOPTIC it is possible for a combination of Privacy Threat Actions to lead to no privacy harms, if each of the Threat Actions is benign (recall that completely benign actions are not included, but actions that can be either benign or harmful are included). It may also be possible that a series of actions or inactions, which are each individually harmless, are harmful in combination. More commonly, a combination of Privacy Threat Actions leads to a privacy harm because one or more of the Threat Actions were harmful individually. For instance, some Threat Actions within PA03 Collection, such as the registration of a new user on a website, are generally harmless while others, such as the surveillance in the Nomi case (Section 5.3) are harmful. Just as in our attack definition, the existence of a privacy adverse consequence matters.

Yet some privacy consequences can be considered adverse by one individual and neutral or harmless by another – they are subjective. When a combination of Privacy Threat Actions leads to a subjective outcome, PANOPTIC does not provide a method to determine if a privacy harm has actually occurred. Our definition includes any case where there is a perception of privacy adverse consequences, but whose perception? Nissenbaum argues that privacy is “provided by appropriate flows of information” where “appropriate information flows are those that conform with contextual information norms” [5]. Following this logic, the contextual group of people affected determine whether a privacy harm has been perceived to have taken place.

While there are few data-driven methods for identifying contextual privacy norms, [44] and [45] offer a potential solution based on crowdsourcing norms from representative samples using Contextual Integrity Theory. Privacy norms are both ethical and temporal – they are based in perceptions of right and wrong that change over time [5]. However, the violation of a societal norm is not required for the perception of harm by an individual, and harms can be perceived on an individual or group level even if society at large disagrees that a norm was broken. The population affected is itself contextual and “society” may mean different groups of people in different cases. Threat modeling by its nature is intended to have broad scope, though, and is not intended to identify perceived threats against any specific individual.

## 7 Discussion

Privacy threat modeling (and privacy risk modeling generally) does not take place in a vacuum. How it happens and why will be invariably affected by the characteristics of the surrounding environment. Some of these are specific to organizations and applications while others reside at the regulatory and societal level. Different organizations will employ different development life cycles and there will be no one-size-fits-all recipe for integrating privacy threat modeling into those processes, other than to note that a threat model will need to evolve throughout the life cycle to account for changing context. That context will have multiple dimensions that may shift over the course of time – including system boundaries, affected individuals and other stakeholders, anticipated adversaries, and the relevant consequence model – and have implications for scoping decisions. A crucial and easily overlooked dimension are the attributes of the threat modelers themselves and how these shape their perspectives; a degree of self-awareness is in order. [46]

More broadly, making privacy threat modeling work within the plethora of regulatory compliance regimes could present challenges. Privacy threat modeling could become simply another element of performative compliance and tactics for preventing this come with their own drawbacks. Even a good-faith attempt to employ privacy threat modeling could, as a result of narrow focus, end up just replicating compliance measures by other means. Any proposed foundational privacy threat model must be developed and used with an awareness of these issues.

While PANOPTIC is intended to have wide applicability, there are important limitations that merit user awareness. PANOPTIC does not address data breaches and therefore would not directly contribute to data breach prevention. It is important, therefore, that security threat modeling (which should account for data breaches in principle) address them in practice. Additionally, PANOPTIC reflects one particular adverse privacy consequences model, Solove’s Taxonomy of Privacy [2], which is widely recognized but not necessarily the appropriate model for all contexts. Users of any privacy threat model must recognize the possibility of a potential mismatch between the threat model itself and the domain of application.

PANOPTIC is also not intended to facilitate compliance. While specific compliance requirements would constitute their own model, to the limited extent that PANOPTIC addresses compliance, it is by the means of particular threat actions (e.g., PA06.01 Age not verified (for regulations such as COPPA that protect children), PA13.04 Deviating from regulatory requirements). However, using PANOPTIC as intended could help satisfy some of the new regulatory requirements for the inclusion of privacy risk assessments [20, 25], as well as demonstrate a commitment to active privacy risk management and, by extension, Privacy by Design [47].

The benefits to a range of stakeholders from a common structure and language for describing privacy threats are apparent when one considers the myriad benefits to the cybersecurity domain from the widespread adoption of ATT&CK [6]. Practitioners can communicate more effectively both within and across organizations, organizations can more effectively implement threat-informed defense, risk management tools can interoperate effectively, and the public can enjoy a higher level of protection. As such, PANOPTIC represents an important step in the evolution toward comprehensive privacy risk models that supply all three principal components: threats, vulnerabilities, and adverse consequences. While privacy threat modeling suffers the largest gap amongst these three components, all three components are necessarily constituents of privacy risk models. Fully formed privacy risk models will facilitate more systematic identification and assessment of privacy

risks, which is increasingly crucial in an age of increasingly complex socio-technical systems.

## 8 Applications

PANOPTIC can be leveraged for multiple operational use cases. To be of more than academic interest, a threat model must be usable and provide value in real-world environments and processes, a quality exemplified by ATT&CK. We envision three principal use cases for PANOPTIC: stand-alone privacy threat assessment, privacy risk management, and privacy red teaming. None of these are mutually exclusive; indeed, they can be mutually supportive.

### 8.1 Privacy Threat Assessment

There are two distinct aspects to threat assessment, environmental and system or process specific. All systems and processes operate in some larger environment that presents a constantly changing set of potential threats. Understanding that environment is essential to establishing and maintaining appropriate risk postures. PANOPTIC can be used to represent general attack trends and thereby prompt responses in the form of alterations to existing configurations and policies as part of the maintenance activity within life cycles (i.e., informing privacy continuous monitoring) and to requirements and design guidance addressing those life-cycle facets. In particular, PANOPTIC can be used to profile specific threat agents based on empirical data, enabling general measures to be identified and implemented which counter the threats represented by those profiles. Those profiles, as well as the PANOPTIC Patterns, can also be employed at the system or process level to identify relevant threats, including those posed by the system or process itself, by looking for intersecting activities and actions. The results may motivate specific changes to the requirements or design of an artifact under development or specific modifications of an existing one. Further, as outlined in Appendix B, if a system and its associated processes can be described using PANOPTIC then that description can be analyzed independently to identify potential attack paths. Both modes of threat assessment support threat-informed defense, at the organizational level in one case and at the system level in the other.

### 8.2 Privacy Risk Management

As previously noted, threat models are just one dimension of a complete risk model that addresses vulnerabilities and consequences as well. The risk assessment process effectively looks for system or process-specific alignments between threats, vulnerabilities, and consequences. Where one or even two of these dimensions are absent, they must be imputed – not necessarily in any systematic manner – to enable risk determinations. PANOPTIC can supply the threat dimension of privacy risk models. This bolsters the privacy risk management process by explicitly defining a privacy threat space. Relevant threats can then be specified and connected to the vulnerabilities they could exploit and/or the resulting privacy consequences. Such alignments will identify privacy risks that should be managed by either mitigation, remediation, transfer, or acceptance. Exactly when risk management takes place will be dependent on the specifics of a given life cycle, but it can potentially occur during requirements definition, design, and maintenance (in the case of continuous monitoring). Arguably, it should take place during all three of these activities. In all cases, though,

privacy risk management that utilizes a risk model which explicitly includes threats will be more robust than when a threat model is missing.

## 8.3 Privacy Red Teaming

Red teaming aims to evaluate the preparedness and protections of systems, processes, and people by conducting mock outsider attacks. (It is broader than penetration testing, which traditionally concerns itself with just systems, including networks.) Red teaming has a long history in cybersecurity but has only recently begun to gain significant traction in privacy [31]. Owing to its holistic perspective (attacking the enterprise as opposed to just its systems), red teaming tends to be scenario based. As a result, it can benefit enormously from the availability of an appropriate threat model. This is even more the case for privacy than for security, given the importance of context for privacy and the possibility of the systems and processes themselves posing potential privacy threats. PANOPTIC, then, can provide the basis for constructing attack scenarios that a privacy red team can use to guide their efforts (as well as report their results) in conjunction with actor-based threat modeling. Depending on the nature of the exercise, specific scenarios may be of particular concern, either as a function of the environment or due to specific sensitivities or obligations.

## 9 Future Work

We are currently finalizing PANOPTIC Version 2, the result of mapping a second, broader dataset with approximately 150 additional attacks identified by searching the *New York Times* and the [reddit.com/r/privacy](https://www.reddit.com/r/privacy) online forum. As part of this iteration we introduced a quantitative metric to track taxonomy rate of change and also employed "regression testing" using a small set of attacks from the seed dataset. This has produced a more holistic and robust model.

Once PANOPTIC Version 2 has been released, we intend to use clustering algorithms to identify major types of privacy attacks in our dataset that share similar Taxonomy mappings. These will be represented through the PANOPTIC Taxonomy as generic kill chains designated PANOPTIC Patterns. We intend to integrate this into a web-based tool currently under development that, in addition to facilitating system and environmental mappings, will indicate matching Patterns and suggest mitigations that break the Patterns. Related to this, we are developing mitigating interventions for specific Privacy Threat Actions. We are also currently testing PANOPTIC in multiple organizational environments with different use cases and developing procedural documentation on how to use PANOPTIC for different purposes – threat assessments, privacy risk management, and privacy red teaming.

## 10 Conclusion

This paper presented the PANOPTIC Privacy Threat Model, the philosophies and scoping decisions that define it, how it was developed, and future work to develop it into a fully holistic and robust model. PANOPTIC takes a data-driven, threat agent-agnostic, attack-oriented approach to privacy threat modeling, including within its scope both actions and inactions from within and without the system of concern so long as the combination of events leads to a perceived privacy harm. It approaches privacy as an inherently context-driven domain and incorporates privacy contextual elements into the model. PANOPTIC, and privacy threat models in general, enable privacy threat assessments, holistic risk management, privacy red teaming, and privacy threat-informed defense. PANOPTIC's Privacy Activities and Privacy Threat Actions have the potential to become a common language with which to discuss privacy threats, moving the privacy community from compliance-oriented to risk- and threat-informed privacy management.

## 11 References

- [1] K. R. Boeckl and N. B. Lefkowitz, “NIST Privacy Framework: A tool for improving privacy through enterprise risk management, Version 1.0,” *National Institute of Standards and Technology*, 2020.
- [2] D. J. Solove, “A taxonomy of privacy,” *University of Pennsylvania Law Review*, vol. 154, no. 3, 2006. [Online]. Available: <https://ssrn.com/abstract=667622>
- [3] A. Shostack, *Threat Modeling: Designing for security*. John Wiley & Sons, 2014.
- [4] A. V. Uzunov and E. B. Fernandez, “An extensible pattern-based library and taxonomy of security threats for distributed systems,” *Computer Standards & Interfaces*, vol. 36, no. 4, pp. 734–747, 2014.
- [5] H. Nissenbaum, *Privacy in Context*. Stanford University Press, 2009.
- [6] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, “MITRE ATT&CK: Design and philosophy,” *The MITRE Corporation*, 2018.
- [7] M. Muckin and S. C. Fitch, “A threat-driven approach to cyber security,” *Lockheed Martin Corporation*, 2014.
- [8] S. S. Shapiro, “Time to Modernize Privacy Risk Assessment,” *Issues in Science and Technology*, vol. 38, no. 1, pp. 20–22, 2021.
- [9] R. Calo, “The Boundaries of Privacy Harm,” *Indiana Law Journal*, vol. 86, no. 3, 2011. [Online]. Available: <https://ssrn.com/abstract=1641487>
- [10] S. Brooks, E. Nadeau, M. Garcia, N. Lefkowitz, and S. Lightman, “Privacy risk management for federal information systems,” *National Institute of Standards and Technology*, vol. 8062, 2015.
- [11] R. J. Cronk and S. S. Shapiro, “Quantitative privacy risk analysis,” in *2021 IEEE European Symposium on Security and Privacy Workshops (EuroSPW)*, 2021, pp. 340–350.
- [12] R. Clarke, “Privacy impact assessment: Its origins and development,” *Computer law & security review*, vol. 25, no. 2, pp. 123–135, 2009.
- [13] R. Binns, “Data protection impact assessments: A meta-regulatory approach,” *International Data Privacy Law*, vol. 7, no. 1, pp. 22–35, 2017.
- [14] K. Wuyts, R. Scandariato, and W. Joosen, “LINDDUN privacy threat tree catalog,” *Department of Computer Science, KU Leuven*, 2014.
- [15] R. Ayers and W. Jansen, “PDA forensic tools: An overview and analysis,” *National Institute of Standards and Technology*, 2004.
- [16] H. Nissenbaum, “Privacy as Contextual Integrity,” *Wash. L. Rev.*, vol. 79, p. 119, 2004.
- [17] O. for Civil Rights, “Summary of the HIPAA privacy rule,” *U.S. Department of Health and Human Services*, 2003.

- [18] J. C. Cuaresma, “The Gramm-Leach-Bliley Act,” *Berkeley Tech. LJ*, vol. 17, p. 497, 2002.
- [19] J. M. Fromholz, “The European Union Data Privacy Directive (DPD),” *European Commission*, vol. 15, p. 461, 2000.
- [20] P. Voigt and A. Von dem Bussche, “The EU General Data Protection Regulation (GDPR),” *European Commission*, 2017.
- [21] M. Howard and S. Lipner, *The security development lifecycle*. Microsoft Press Redmond, 2006, vol. 8.
- [22] M. E. Mylrea, S. N. G. Gourisetti, M. Touhiduzzaman, M. D. Watson, and J. E. Castleberry, “Risk management framework process map,” Pacific Northwest National Lab.(PNNL), Tech. Rep., 2018.
- [23] S. Brooks, S. Brooks, M. Garcia, N. Lefkowitz, S. Lightman, and E. Nadeau, *An introduction to privacy engineering and risk management in federal systems*. US Department of Commerce, National Institute of Standards and Technology, 2017.
- [24] “Revision of OMB Circular No. A-130, “Managing Information as a Strategic Resource,”” *Office of Management and Budget, Executive Office of the President*, 2016. [Online]. Available: <https://www.federalregister.gov/documents/2016/07/28/2016-17872/revision-of-omb-circular-no-a-130-managing-information-as-a-strategic-resource>
- [25] “California Consumer Privacy Act,” *California State Legislature*, vol. 55, p. 375, 2018, cal. Legis. Serv. Ch. 55 (A.B. 375) (West).
- [26] N. R. Mead, F. Shull, K. Vemuru, and O. Villadsen, “A hybrid threat modeling method,” *Carnegie Mellon University-Software Engineering Institute*, 2018.
- [27] K. Wuyts and W. Joosen, “LINDDUN privacy threat modeling: A tutorial,” *CW Reports*, 2015.
- [28] E. M. Hutchins, M. J. Cloppert, R. M. Amin *et al.*, “Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains,” *Leading Issues in Information Warfare & Security Research*, vol. 1, no. 1, p. 80, 2011.
- [29] S. L. Garfinkel and M. Theofanos, “Non-breach privacy events,” *Technology Science*, 2018.
- [30] M. Goodwin, J. Gadsden, L. Reading, and A. Kokoroko, “OWASP Threat Dragon,” *OWASP Foundation*, 2016. [Online]. Available: <https://owasp.org/www-project-threat-dragon/>
- [31] S. Tenaglia, “Better Privacy Through Offense: How To Build a Privacy Red Team,” *Black Hat*, 2022.
- [32] Privacy Rights Clearinghouse, “Privacy rights clearinghouse chronology of data breaches,” 2023.
- [33] “Retail tracking firm settles FTC charges it misled consumers about opt out choices,” *Federal Trade Commission*, April 2015. [Online]. Available: <https://www.ftc.gov/news-events/news/press-releases/2015/04/retail-tracking-firm-settles-ftc-charges-it-misled-consumers-about-opt-out-choices>



- [34] C. Larose, “FTC takes action against retail tracking start-up NOMI Technologies,” *JD Supra*, April 2015. [Online]. Available: <https://www.jdsupra.com/legalnews/ftc-takes-action-against-retail-tracking-00076/>
- [35] A. D. Kramer, J. E. Guillory, and J. T. Hancock, “Experimental evidence of massive-scale emotional contagion through social networks,” *Proceedings of the National Academy of Sciences*, vol. 111, no. 24, pp. 8788–8790, 2014.
- [36] R. Meyer, “Everything we know about facebook’s secret mood-manipulation experiment,” June 2014. [Online]. Available: <https://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/>
- [37] M. N. Meyer, “Everything you need to know about facebook’s controversial emotion experiment,” June 2014. [Online]. Available: <https://www.wired.com/2014/06/everything-you-need-to-know-about-facebooks-manipulative-experiment/>
- [38] F. T. Commission, “Protecting children’s privacy under COPPA: A survey on compliance,” *July*, 2002.
- [39] M. A. Weiss and K. Archick, “US-EU Data Privacy: From safe harbor to privacy shield,” 2016.
- [40] A. Peterson, “Facebook’s ‘Year in Review’ app swings from merely annoying to tragic,” *The Washington Post*, Dec 2014. [Online]. Available: <https://www.washingtonpost.com/news/the-switch/wp/2014/12/26/facebook-year-in-review-app-swings-from-merely-annoying-to-tragic/>
- [41] K. Pau, “Spotify wrapped, unwrapped,” *Vox*, Dec 2021. [Online]. Available: <https://www.vox.com/culture/22814121/spotify-wrapped-2021-algorithm-data-privacy>
- [42] J. Constine, “Apple iOS 10 “Memories” turns old photos into editable mini-movies,” *TechCrunch*, June 2016. [Online]. Available: <http://tcrn.ch/1PphfCs>
- [43] S. Ben-Yair, “Your photos, your memories, your way,” <https://blog.google/products/photos/new-memories-features-look-back/>, May 2021.
- [44] C. Bloom and J. Emery, “Privacy expectations for human-autonomous vehicle interactions,” in *2022 31st IEEE International Conference on Robot and Human Interactive Communication (RO-MAN)*. IEEE, 2022, pp. 1647–1654.
- [45] Y. Shvartzshnaider, S. Tong, T. Wies, P. Kift, H. Nissenbaum, L. Subramanian, and P. Mittal, “Learning privacy expectations by crowdsourcing contextual informational norms,” in *Proceedings of the AAAI Conference on Human Computation and Crowdsourcing*, vol. 4, 2016, pp. 209–218.
- [46] C. Bloom, S. Shapiro, S. Slotter, M. Paes, R. Xu, and B. Ballard, “Themes in privacy threat modeling,” *PTM Workshop*, 2022. [Online]. Available: <https://ptmworkshop.gitlab.io/>
- [47] A. Cavoukian *et al.*, “Privacy by design: The 7 foundational principles,” *Information and Privacy Commissioner of Ontario, Canada*, vol. 5, p. 12, 2009.

- [48] R. H. Arpaci-Dusseau and A.-D. A. C., *Operating Systems: Three Easy Pieces*, 1st ed. Arpaci-Dusseau Books, LLC, 2015, <http://pages.cs.wisc.edu/~remzi/OSTEP/>.
- [49] C. A. Waldspurger, “Memory resource management in VMware ESX server,” in *USENIX Symposium on Operating System Design and Implementation (OSDI)*, 2002, pp. 181–194, <https://www.usenix.org/legacy/event/osdi02/tech/waldspurger/waldspurger.pdf>.
- [50] J. S. Hiller and R. S. Russell, “Privacy in crises: The NIST privacy framework,” *Journal of Contingencies and Crisis Management*, vol. 25, no. 1, pp. 31–38, 2017.
- [51] J. Schwartz, “Meta takes offensive posture with privacy red team,” Aug 2022. [Online]. Available: <https://www.darkreading.com/edge/meta-takes-offensive-posture-with-privacy-red-team>
- [52] Facebook, “2014 year in review,” 2014. [Online]. Available: <https://www.facebook.com/formedia/blog/2014-year-in-review>
- [53] “FTC approves final order in Nomi Technologies Case,” *Federal Trade Commission*, September 2015. [Online]. Available: <https://www.ftc.gov/news-events/news/press-releases/2015/09/ftc-approves-final-order-nomi-technologies-case>
- [54] J. Dev, B. Rashidi, and V. Garg, “Models of applied privacy (map): A persona based approach to threat modeling,” in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, ser. CHI ’23. New York, NY, USA: Association for Computing Machinery, 2023. [Online]. Available: <https://doi.org/10.1145/3544548.3581484>

## A Appendix A: PANOPTIC Definitions

The following tables include all Privacy Contextual Domains (PCs) and their constituent Privacy Contextual Elements and Sub-elements (Table A1), as well as all Privacy Activities (PAs) and their constituent Privacy Threat Actions and Sub-actions (Table A2). Each component is given with its identification number, name, and definition.

**Table A1. PANOPTIC Taxonomy Structure & Definitions – Privacy Contextual Domains**

<b>ID</b>	<b>Contextual Domain / Element</b>	<b>Definition</b>
<b>PC01</b>	<b>ENVIRONMENT</b>	<b>The contextual domain in which a data action occurs</b>
PC01.01	Digital	Data action in a digital environment
PC01.02	Physical	Data action in a physical environment
<b>PC02</b>	<b>DISTRIBUTION</b>	<b>How many entities with which the information holder shares information</b>
PC02.01	No distribution	Information holder does not share information
PC02.02	One to one	Information holder shares information with one other entity
PC02.03	One to many	Information holder shares information with a discrete number of other entities
PC02.04	One to everyone	Information holder shares information with the public
<b>PC03</b>	<b>INTERACTION</b>	<b>The extent to which an individual or their proxy interact with the entity or their proxy</b>
PC03.01	Individual interaction	Interaction by a natural person
PC03.01.01	No interaction	Individual does not directly interact at all with the entity or their proxy
PC03.01.02	Discrete interaction	Individual interacts a discrete number of times with the entity or their proxy
PC03.01.03	Ongoing interaction	Individual interacts with the entity or their proxy on an ongoing basis
PC03.01.04	Indeterminate interaction	It is unclear with what frequency the individual interacts with the entity or their proxy
PC03.02	Proxy interaction	Interaction by an intermediary that acts on behalf of a natural person
PC03.02.01	No interaction	Individual does not directly interact at all with the entity or their proxy
PC03.02.02	Discrete interaction	Individual interacts a discrete number of times with the entity or their proxy
PC03.02.03	Ongoing interaction	Individual interacts with the entity or their proxy on an ongoing basis
PC03.02.04	Indeterminate interaction	It is unclear with what frequency the individual interacts with the entity or their proxy

**Table A1. PANOPTIC Taxonomy Structure & Definitions – Privacy Contextual Domains**

<b>ID</b>	<b>Contextual Domain / Element</b>	<b>Definition</b>
<b>PC04</b>	<b>ENGAGEMENT</b>	<b>Targeted subpopulations with which the entity or their proxy interact</b>
PC04.01	Populations with sensitive characteristics	Individuals who, based on a differentiating characteristic, are within a contextually sensitive population
PC04.01.01	Age	Individuals who, based on the differentiating characteristic of age, are within a contextually sensitive population
PC04.01.02	Race & ethnicity	Individuals who, based on the differentiating characteristic of race and/or ethnicity, are within a contextually sensitive population
PC04.01.03	Political opinion	Individuals who, based on the differentiating characteristic of political opinion, are within a contextually sensitive population
PC04.01.04	Religious and philosophical beliefs	Individuals who, based on the differentiating characteristic of religious and/or philosophical belief, are within a contextually sensitive population
PC04.01.05	Sexual orientation & gender identity	Individuals who, based on the differentiating characteristic of sexual orientation & gender identity, are within a contextually sensitive population
PC04.01.06	Sex life	Individuals who, based on the differentiating characteristic of sex life, are within a contextually sensitive population
PC04.01.07	Genetics	Individuals who, based on the differentiating characteristic of genetics, are within a contextually sensitive population
PC04.01.08	Other context-specific populations	Individuals who, based on the differentiating characteristic of another context-specific population, are within a contextually sensitive population
PC04.02	Specific individuals	Only specific individuals are threatened based on their actions
PC04.03	Biased population samples	The system, application, or service employs a skewed understanding of the population with which it interacts

**Table A1. PANOPTIC Taxonomy Structure & Definitions – Privacy Contextual Domains**

<b>ID</b>	<b>Contextual Domain / Element</b>	<b>Definition</b>
<b>PC05</b>	<b>DATA TYPE</b>	<b>Classes of data upon which data actions are performed</b>
PC05.01	Location	Data that serve as a indication or representation of location
PC05.02	Demographic	Socio-physical characteristics of individuals, e.g., education level, ethnicity, religion
PC05.03	Biometric	Measurable physical characteristics or personal behavioral traits used to identify or verify the claimed identity of an individual
PC05.04	Recording	A physical or digital artifact capturing some aspect related to the individual, e.g., a likeness or screenshot
PC05.04	Audio	Sound recording of the voice of individual(s) and associated metadata if applicable
PC05.04	Image	A single instance of a visual representation relating to individual(s) and associated metadata if applicable
PC05.04	Video	Moving visual images relating to a individual(s) and associated metadata if applicable subject
PC05.05	Credentials	Evidence attesting to one's right to credit, authority, or other attribute such as identity
PC05.06	Contact information	Information including the identity of, and the means to communicate with, the individual(s) associated with the data set or information resource
PC05.07	Health	Information pertaining to an individual's health status or use of health-related products or services
PC05.08	Financial	Information pertaining to an individual's financial status, e.g., credit ratings and history, income, bank accounts
PC05.09	Employment	Information pertaining to an individual's relationship with their employer
PC05.10	Social / personal network	Personal relationships in some context, including but not limited to social media networks
PC05.11	Criminal	Information pertaining to activity that can be interpreted as violating the law or is related to the criminal justice system
PC05.12	Social media	Information that exist within forms of electronic communication, including websites and applications, that enable users to create and share content or to participate in social networking

**Table A1. PANOPTIC Taxonomy Structure & Definitions – Privacy Contextual Domains**

<b>ID</b>	<b>Contextual Domain / Element</b>	<b>Definition</b>
PC05.13	Psychographic	Psychological and cognitive attributes of a individual that reveal their beliefs, values, and goals
PC05.13.01	Preferences	Information pertaining to an individual's inclination toward one alternative over another
PC05.13.02	Personality	The combination of characteristics or qualities that form an individual's distinctive character
PC05.14	Behavior	Information about an individual's actions
PC05.15	Identity	Information pertaining to who an individual is
PC05.15.01	Persistent Identifier	A consistent identifier that one can be reasonably confident directly associates data with an individual, such as a name
PC05.15.02	Persistent identifier      Pseudo-identifier	An identifier that enables data to be repeatedly associated with the same individual(s) or their proxy without knowing their identity, such as a username or a MAC address
PC05.16	Other sensitive information	Any otherwise unspecified data type that could result in adverse consequences for an individual or group

<b>Table A2. PANOPTIC Taxonomy Structure &amp; Definitions – Privacy Activities</b>		
<b>ID</b>	<b>Activity/Threat Action</b>	<b>Definition</b>
<b>PA01</b>	<b>NOTICE</b>	<b>Informing an individual or their proxy of one or more data actions</b>
PA01.01	Out of sequence	User is not notified of potential data actions before they are performed
PA01.02	Unclear	A privacy notice is difficult for the user to find or understand
PA01.03	Imprecise	Key data actions that are not presented clearly to the user, in a confusing manner
PA01.04	Absent	Applicable notice is not provided
PA01.05	Insufficient	Significant context is missing from the notice
PA01.06	Misleading/false	The notice includes erroneous or deceptive statements
<b>PA02</b>	<b>CONSENT</b>	<b>Assent from an individual or their proxy to one or more defined data actions</b>
PA02.01	Out of sequence	Consent is requested after the data action in question has been performed
PA02.02	Imprecise	Key data actions that are not presented clearly enough to constitute informed consent
PA02.03	Absent	Applicable consent is not requested
PA02.04	Insufficient	Significant context for consent is not provided
PA02.05	Misleading	Consent is based on erroneous or deceptive statements.
PA02.06	No opt in/out	There is no way to opt out or opt in
PA02.06.01	No overall opt in/out	There is no way to opt out with a single action
PA02.06.02	No granular opt in/out	There is no way to opt out of specific elements
PA02.07	Inherited	Consent is inherited from a prior consent though the new data action is outside the original scope and context



**Table A2. PANOPTIC Taxonomy Structure & Definitions – Privacy Activities**

<b>ID</b>	<b>Activity/Threat Action</b>	<b>Definition</b>
<b>PA03</b>	<b>COLLECTION</b>	<b>The gathering or extraction of information</b>
PA03.01	Application or device use	Information collected or generated through routine actions that are intrinsic to the application or device usage
PA03.02	Registration	Information collected or created during registration for a system, application, or service
PA03.03	Tracking & affording tracking	Information collected or generated about an individual's actions that is extrinsic to the actions themselves and/or making available facilitating functionality
PA03.04	Sniffing & affording sniffing	Collecting information from device broadcast signals and/or making available facilitating functionality
PA03.05	Pretexting	Collecting information by using false pretenses to manipulate data subjects into divulging information
PA03.06	External appropriation	Presumptively using personal information legitimately collected within others' functional contexts for some unrelated purpose
PA03.07	Interception	Collecting information flows in transit between their source and destination
PA03.08	Soliciting & affording soliciting	Individuals are prompted to provide information and/or making available facilitating functionality
PA03.08.01	2nd party solicits 1st party	Information custodian entices individuals to disclose more personal information than they otherwise might and/or enables others to do the same
PA03.08.02	3rd party solicits 2nd party	Information recipient entices an information custodian to disclose more personal information of an individual than they otherwise might and/or enables others to do the same
PA03.08.03	3rd party solicits 1st party	Information recipient entices individuals to disclose additional personal information and/or enables others to do the same
PA03.09	Recording	Capturing a physical or digital artifact capturing the aspect or likeness of the individual
PA03.10	Transaction	Logging information pertaining to monetary transactions

**Table A2. PANOPTIC Taxonomy Structure & Definitions – Privacy Activities**

<b>ID</b>	<b>Activity/Threat Action</b>	<b>Definition</b>
<b>PA04</b>	<b>INSECURITY</b>	<b>Insufficient data protection controls</b>
PA04.01	Insufficient access controls	Operational constraints for managing access to personal information are insufficient or flawed
PA04.02	Insufficient encryption	Appropriate encryption is not implemented, or is weak or otherwise poorly implemented
PA04.03	Undermining or interfering with authentication	Intervening in authentication processes such that chains of trust are disrupted or other operational assumptions are invalidated
PA04.04	Detection failure	Relevant system events are not captured and/or identified
PA04.05	Misconfigured permissions	System, application, or service data handling permissions allow unauthorized handling
<b>PA05</b>	<b>IDENTIFICATION</b>	<b>How information is associated with an individual</b>
PA05.01	Implicit identification	Inferring an individual's identity from a collection of data points
PA05.01.01	Re-identification	Re-associating data with identifiable individuals that had been treated to remove those associations
PA05.02	Identifier assignment	Assigning a pseudo-identifier
PA05.02.01	Fingerprinting	Constructing a device, system, or application pseudo-identifier based on a unique set of properties
PA05.03	Compulsory self-identification	Requiring an individual to identify themselves
<b>PA06</b>	<b>QUALITY ASSURANCE</b>	<b>Implementing policies or processes to ensure quality throughout privacy-related activities</b>
PA06.01	Age not verified	Age of the user is not checked before performing data actions
PA06.02	Unvetted data source	Source of the data is not considered when performing data actions
PA06.03	Unvetted data quality	Quality of the data is not considered when performing data actions
PA06.03.01	Bias of data not evaluated	Data action potentially adversely influenced by bias
PA06.03.02	Unvetted data accuracy	Accuracy of the data is not considered when performing data actions
PA06.04	Unvetted recipients	The legitimacy and/or trustworthiness of downstream data recipients has not been assessed
PA06.05	Unvetted downstream practices	The legitimacy and/or trustworthiness of downstream data processes have not been assessed

**Table A2. PANOPTIC Taxonomy Structure & Definitions – Privacy Activities**

<b>ID</b>	<b>Activity/Threat Action</b>	<b>Definition</b>
PA06.06	Insufficient communication of downstream responsibilities	The legitimacy and/or trustworthiness of downstream data stewardship responsibilities has not been assured
PA06.07	Data insufficiently de-identified	Insufficient data processing to prevent identification of the individual
PA06.08	Data out of scope	Action leverages data types outside of limits established by any relevant source
PA06.09	Data action out of scope	Data action exceeds limits bounding that action established by any relevant source
PA06.09.01	Data collection out of scope	Collection exceeds limits bounding that action established by any relevant source
PA06.09.02	Data processing out of scope	Data processing exceeds limits bounding that action established by any relevant source
PA06.09.03	Data sharing out of scope	Data sharing exceeds limits bounding that action established by any relevant source
PA06.10	Insufficient agreed usage restrictions	Data use agreement for downstream data recipients is insufficient or absent
<b>PA07</b>	<b>MANAGEABILITY</b>	<b>Enabling an individual or their proxy to access, modify, copy, or destroy information about the individual</b>
PA07.01	No individual access to information	Individual or their proxy cannot obtain or view their collected personal data
PA07.02	No individual management of information content	Individual or their proxy cannot transform (e.g., move, copy, edit) their collected personal data
PA07.03	No individual deletion of information	Individual or their proxy cannot delete their collected personal data
PA07.04	No individual deletion of information	Individual or their proxy cannot delete their collected personal data
PA07.05	Privacy configurations compromised by outside forces	Individual's privacy settings are compromised by dependencies on the settings of others
PA07.06	Confounded user controls	User controls are opaque or ineffective, including frustrating individuals' attempts to utilize controls
PA07.07	Bypass of user controls	Defeating or ignoring a privacy control within or outside a functional context
PA07.08	Pre-emption of privacy settings	Preventing individuals from influencing an action or event by initiating or executing it before they have an opportunity to affect it

**Table A2. PANOPTIC Taxonomy Structure & Definitions – Privacy Activities**

<b>ID</b>	<b>Activity/Threat Action</b>	<b>Definition</b>
<b>PA08</b>	<b>AGGREGATION</b>	<b>Assembling data from multiple sets of data</b>
PA08.01	Profiling	Assembling and organizing data points regarding specific individuals
PA08.01.01	Single source profiling	Assembling and organizing data points about specific individuals from a single source
PA08.01.02	Multi-source profiling	Assembling and organizing data points about specific individuals from multiple sources
PA08.02	Clustering	Assembling and organizing data points regarding groups of people
PA08.02.01	Single source clustering	Assembling and organizing data points regarding groups of people from a single source
PA08.02.02	Multi-source clustering	Assembling and organizing data points regarding groups of people from multiple sources
<b>PA09</b>	<b>PROCESSING</b>	<b>Extracting and developing value and utility from information</b>
PA09.01	Deriving new information	Determining or extracting novel information by analysing information
PA09.01.01	Deriving information about individuals	Determining or extracting novel information about an individual by analyzing information
PA09.01.02	Deriving aggregate information	Determining or extracting novel aggregate information by analysing information
PA09.01.03	Deriving sensitive information	Determining or extracting novel sensitive information by analysing information
PA09.01.04	Deriving derogatory information	Determining or extracting novel derogatory information by analysing information
PA09.02	Behavioral analysis	Leveraging information to determine or infer the behaviour of an individual or group
PA09.03	Introducing bias	Data action is adversely influenced by bias
PA09.04	Trawling datasets for information	Reviewing aggregated collections or streams of information for items of interest
PA09.05	Internal appropriation	Presumptively using information legitimately collected within a functional context for some unrelated purpose
<b>PA10</b>	<b>SHARING</b>	<b>Making information available to another entity</b>

**Table A2. PANOPTIC Taxonomy Structure & Definitions – Privacy Activities**

<b>ID</b>	<b>Activity/Threat Action</b>	<b>Definition</b>
PA10.01	Affording revelations	Making available information that enables the discovery of further information
PA10.02	Exposure	Information that should be protected are made generally discoverable and accessible
PA10.02.01	Doxxing	Disseminating information for purposes of harassment, in terms of the release itself and/or its exploitation by others
PA10.03	Misrepresentation	Information is made generally available without context necessary for proper interpretation
<b>PA11</b>	<b>USE</b>	<b>Leveraging information to achieve a goal</b>
PA11.01	Implication	Establishing a particularized derogatory suspicion or accusation regarding an individual
PA11.02	Targeting	Distinguishing individuals for particularized treatment
PA11.02.01	Tailored content	Customizing the information presented to an individual
PA11.03	Manipulation	Leveraging information to exploit, control, or inappropriately influence an individual
PA11.03.01	Extortion	Coercing an individual to derive some benefit
PA11.04	Intrusion	Invasions or incursions into an individual's life
PA11.05	Selling	Information is sold to other entities in a commercial transaction
PA11.06	Reprisal	Leveraging information to retaliate against an individual
<b>PA12</b>	<b>RETENTION &amp; DESTRUCTION</b>	<b>Actions that affect the persistence of information</b>
PA12.01	Data not destroyed after use	Information has not been disposed at the conclusion of its lifecycle
PA12.02	Data improperly destroyed	Information remains at least partially recoverable despite attempts to destroy it
<b>PA13</b>	<b>DEVIATIONS</b>	<b>Data action diverges from established limits bounding the data action in question</b>
PA13.01	Deviating from stated policy or user agreements	Downstream data recipients are in violation of usage agreements
PA13.02	Deviating from stated policy or user agreements	Data action deviates from stated policies or user agreements
PA13.03	Deviating from claimed certification conformance	An entity does not actually hold a claimed certification or is not actually adhering to a claimed standard
PA13.04	Deviating from regulatory requirements	An entity is violating a specific regulation that applies to it

## A Appendix B: System Privacy Threat Assessment

Conducting a system privacy threat assessment helps identify potential privacy attacks against a system. Interventions can then be considered at appropriate points to disrupt privacy threat actions.

A system privacy threat assessment using PANOPTIC consists of the following steps:

**Define assessment target** Before a threat assessment can be carried out, the system must be scoped to bound the assessment. While this may seem straightforward, it can be complicated by component integration and system of systems architectures. While applications may appear at first glance to be self-contained entities, the environments in which they execute could prove germane as attacks may involve the underlying operating system. Similarly, systems that are one component of a larger system of systems may be treatable as standalone systems, but their connections to other component systems and the data that flow across those connections may call for extending the target boundary.

Once the assessment target is scoped, sufficient descriptive information must be compiled. Consistent with PANOPTIC's structure, this information must address both context and privacy activities. Contextual information relates to the use case(s) of the system, pertaining to its intended purpose(s), interactions with users, and data. Privacy activities relate to system operation, including supporting business processes. Various artifacts can furnish the necessary information, including architectural diagrams, data flow diagrams, UML sequence diagrams, user guides, and concept of operations. If the target is an existing system, a privacy impact assessment, if available, can provide useful details regarding both the use case(s) and operation of the system.

**Construct scenarios** Scenarios establish contexts for potential privacy attacks. They can take a number of different orientations, depending on the structure of the system or the nature of concerns. For example, distinct scenarios could be developed for different sets of assumptions or preconditions. These could involve external environmental factors, particular internal states, or specific user stories. Scenarios can also be developed based on known or projected threat actors and their motives and capabilities. Scenarios provide a starting point for thinking through possible attacks. Without this grounding and the direction it provides, the assessment would be effectively arbitrary.

Scenarios can be described in a variety of ways that are highly dependent on the type. They do not need to be extremely detailed or extensively documented and in most cases can be represented as a simple table. They just need to provide enough information to constrain or shape thinking about relevant possible attacks. For example, the position and resources of a particular threat actor relative to the target may draw attention to particular architectural locations while discounting others as potential points of attack. This, in turn, will shape mapping of possible attack paths.

### **Map potential attacks**

For each scenario, relevant PANOPTIC contextual elements and threat actions should be selected. Depending on the characteristics of the target and those of the scenarios, the contextual elements may be largely or wholly static across scenarios. It therefore may be worth starting from the previous scenario's contextual elements and modifying these as appropriate.

Note that because the assessment target itself can constitute the privacy threat, a potential attack may arise from characteristics of the system. Therefore, it could be useful to initially select relevant

potential threat actions based on the description of the target and use this as the starting point for each scenario, selecting and deselecting threat actions as necessary.

Mapping possible attacks is an exercise of the imagination within the constraints imposed by a given scenario; posing and attempting to answer certain questions can facilitate the process:

- Where are the most likely points of attack in terms of architectural or data flow location or of function?
- What data is likely to be involved?
- What population is likely to be affected?
- What information life cycle stages are implicated?
- What Fair Information Practice Principles are implicated?
- What privacy activities or threat actions can be interpolated from others?
- What privacy activities or threat actions can be extrapolated from others?

Note that some mappings may include points at which an attack chain splits into divergent potential chains based on the presence or absence of a particular threat action.

**Validate attacks** Ultimately, a potential attack is only an attack if an affected individual could reasonably feel subjected to adverse privacy consequences, however defined. While PANOPTIC was developed using Solove's Taxonomy of Privacy as its consequence model for this purpose, nothing prevents an assessment from leveraging a different model. Regardless of the specifics, it is important to validate that a possible attack actually qualifies as an attack, as context could potentially render it moot.

A privacy consequence model should be explicitly identified for this purpose. It should then be used to establish whether each distinct potential attack chain in each scenario actually constitutes a privacy attack. Where this is not the case, contextual elements and threat actions can be de-selected if they are not part of some other attack. Alternatively, this step can be performed immediately following each scenario mapping rather than waiting until all scenarios have been mapped.

### **Analyze attacks**

The final step of the system privacy threat assessment is to analyze the set of valid attacks across the scenarios. Are there patterns that suggest common attack (i.e., privacy failure) modes? These could prompt reconsideration of relevant design choices. Are there common elements across attacks? These might present opportunities for maximally effective intervention at those points.