The PANOPTIC™Privacy Threat Model

Samantha Katcher*▷, Ben Ballard*▷, Cara Bloom*, Katie Isaacson*, Julie McEwen*,
*Dr. Stuart Shapiro**, *Shelby Slotter**, *Mark Paes**, *Ryan Xu**
+ **MITRE Corporation;* ▷ *Tufts University*

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.

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 [11]. 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" [14]. Threat modeling varies depending on its context of use – modeling physical threats to a building differs from modeling cyber threats to a system. Privacy threat modeling 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. Privacy scholars cannot agree on a basic definition for the concept of "privacy" [9, 12], 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 is one a common language across industries like some cybersecurity threat models [7, 13]. PANOPTIC™ is intended to address this gap.

Threat models are one of the three legs of the risk model "stool" along with vulnerabilities and adverse consequences. Accounting for threats may elevate a risk model from looking at flaws in systems (vulnerability-centric model) to exploring which flaws are exploitable (threat-informed defense) [10]. Each component 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.

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 [12], while Calo's dichotomy characterizes consequences as objective and subjective harms [4]; there are privacy vulnerability models, for example Nissenbaum's Contextual Integrity Theory [9] and the National Institute of Standards and Technology (NIST) Problematic Data Actions [3]. Privacy risk assessment methodologies such as FAIR-P [6] and the NIST Privacy Risk Assessment Methodology (PRAM) [3] 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 [2, 5].

The only published threat model for privacy attacks (that we identified in our literature review) is LINDDUN [15], 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 transition from a compliance-oriented to a risk-oriented mindset, but with

privacy we have yet to see such a transition [10].

Despite numerous high-profile privacy incidents over the last decade, the contrast between privacy and cybersecurity is stark. Calls for a risk-based approach to privacy notwithstanding, privacy generally remains firmly mired in a compliance-based mode. Aside from other contributing factors, 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 [9] 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 [15], along with most privacy vulnerability [1, 2, 5, 8] and consequence models [4, 12]) 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.

2 PANOPTIC Taxonomy

The PANOPTIC Taxonomy is based on the attack stories from the seed dataset and consists of Privacy Threat Actions 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., aggregation).

Mapping an Attack: Nomi Technologies Systems of interest, threat landscapes, and individual attacks can be mapped to the PANOPTIC Taxonomy to gain understanding of the threat(s). The following mapping of an attack, Nomi Technologies, is 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) and others occurred due to physical surveillance (PC01.02). Nomi shared the aggregate data with the specific retailer from whose store the original data had been collected (PC02.02), but it also indicated whether customers had visited other chain locations as well (PC02.03). Individuals did not need to interact directly with Nomi to be involved in the attack (PC03.01.01) but the individual's phone, which is a proxy for the individual, was tracked while in range of Nomi's sensors (PC03.02.02). 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).

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. The online notice was misleading/false (PA01.06). While Nomi did provide an online opt-out mechanism, there was no in-store provision, therefore consent was out of sequence (PA02.01) and the promised opt-out was unavailable (PA02.06). Data collection occurred via tracking (PA03.03) and sniffing (PA03.04) because Nomi collected data about individuals' physical movements and emanations from their mobile devices. Nomi identified individuals by hashing their phone MAC address, which is a constructed identifier (PA05.02.01). Nomi created individual profiles (PA08.01.01) as well as aggregate views of store customers (PA08.02.01). Nomi derived aggregate shopping information (PA09.01.02) and performed behavioral analysis (PA09.02). They shared aggregate data with each retailer (PA10), but no specific threat actions apply. Nomi failed to comply with their stated policy (PA13.02). There were no insecurity, quality assurance, manageability, or retention and destruction-related privacy threat actions in this attack.

This mapping 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.

References

[1] Richard Ayers and Wayne Jansen. PDA forensic tools: An overview and analysis. *National Institute of Standards and Technology*, 2004.

[2] Reuben Binns. Data protection impact assessments: A meta-regulatory approach. *International Data Privacy Law*, 7(1):22–35, 2017.

[3] Sean Brooks, Ellen Nadeau, Michael Garcia, Naomi Lefkovitz, and Suzanne Lightman. Privacy risk management for federal information systems. *National Institute of Standards and Technology*, 8062, 2015.

[4] Ryan Calo. The Boundaries of Privacy Harm. *Indiana Law Journal*, 86(3), 2011.

[5] Roger Clarke. Privacy impact assessment: Its origins and development. *Computer law & security review*, 25(2):123–135, 2009.

[6] R. Jason Cronk and Stuart S. Shapiro. Quantitative privacy risk analysis. In *2021 IEEE European Symposium on Security and Privacy Workshops (EuroSPW)*, pages 340–350, 2021.

[7] Michael Muckin and Scott C Fitch. A threat-driven approach to cyber security. *Lockheed Martin Corporation*, 2014.

[8] Helen Nissenbaum. Privacy as Contextual Integrity. *Wash. L. Rev.*, 79:119, 2004.

[9] Helen Nissenbaum. *Privacy in Context*. Stanford University Press, 2009.

[10] Stuart S Shapiro. Time to Modernize Privacy Risk Assessment. *Issues in Science and Technology*, 38(1):20–22, 2021.

[11] Adam Shostack. *Threat Modeling: Designing for security*. John Wiley & Sons, 2014.

[12] Daniel J. Solove. A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3), 2006.

[13] Blake E Strom, Andy Applebaum, Doug P Miller, Kathryn C Nickels, Adam G Pennington, and Cody B Thomas. MITRE ATT&CK: Design and philosophy. *The MITRE Corporation*, 2018.

[14] Anton V Uzunov and Eduardo B Fernandez. An extensible pattern-based library and taxonomy of security threats for distributed systems. *Computer Standards & Interfaces*, 36(4):734–747, 2014.

[15] Kim Wuyts, Riccardo Scandariato, and Wouter Joosen. LINDDUN privacy threat tree catalog. *Department of Computer Science, KU Leuven*, 2014.

A Appendix: 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

ID	Contextual Domain / Element	Definition
PC01	**ENVIRONMENT**	**The contextual domain in which a data action occurs**
PC01.01	Digital	Data action in a digital environment
PC01.02	Physical	Data action in a physical environment
PC02	**DISTRIBUTION**	**How many entities with which the information holder shares information**
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
PC03	**INTERACTION**	**The extent to which an individual or their proxy interact with the entity or their proxy**
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, including once, 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's proxy does not directly interact at all with the entity or their proxy
PC03.02.02	Discrete interaction	Individual's proxy interacts a discrete number of times, including once, with the entity or their proxy
PC03.02.03	Ongoing interaction	Individual's proxy interacts with the entity or their proxy on an ongoing basis
PC03.02.04	Indeterminate interaction	It is unclear with what frequency the individual's proxy interacts with the entity or their proxy

Table A1: PANOPTIC Taxonomy Structure & Definitions – Privacy Contextual Domains

ID	Contextual Domain / Element	Definition
PC04	**ENGAGEMENT**	**Targeted subpopulations with which the entity or their proxy interact**
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 identity
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

ID	Contextual Domain / Element	Definition
PC05	**DATA TYPE**	**Classes of data upon which data actions are performed**
PC05.01	Location	Data that serve as an 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
PC05.04.01	Audio	Sound recording of the voice of individual(s) and associated metadata if applicable
PC05.04.02	Image	A single instance of a visual representation relating to individual(s) and associated metadata if applicable
PC05.04.03	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 exists 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

ID	Contextual Domain / Element	Definition
PC05.13	Psychographic	Psychological and cognitive attributes of an individual that reveal their beliefs, values, and goals
PC05.13.01	Preferences	Information pertaining to an individual's interests or 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 direct identifier	A consistent identifier that one can be reasonably confident directly associates data with an individual, such as a name
PC05.15.02	Persistent 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

Table A2: PANOPTIC Taxonomy Structure & Definitions – Privacy Activities

ID	Activity/Threat Action	Definition
PA01	**NOTICE**	**Informing an individual or their proxy of one or more data actions**
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
PA02	**CONSENT**	**Assent from an individual or their proxy to one or more defined data actions**
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-out/in	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

ID	Activity/Threat Action	Definition
PA03	**COLLECTION**	**The gathering or extraction of information**
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 an individual 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

ID	Activity/Threat Action	Definition
PA04	**INSECURITY**	**Insufficient data protection controls**
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
PA05	**IDENTIFICATION**	**How information is associated with an individual**
PA05.01	Implicit identification	Inferring an individual's identity from a collection of data points
PA05.01.01	Re-identification	Re-associating data with 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
PA06	**QUALITY ASSURANCE**	**Implementing policies or processes to ensure quality throughout privacy-related activities**
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

ID	Activity/Threat Action	Definition
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
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	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 control of information disclosure	Individual or their proxy cannot control how or with whom their information is shared
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

ID	Activity/Threat Action	Definition
PA08	**AGGREGATION**	**Assembling data from multiple sets of data**
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
PA09	**PROCESSING**	**Extracting and developing value and utility from information**
PA09.01	Deriving new information	Determining or extracting novel information by analyzing 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 analyzing information
PA09.01.03	Deriving sensitive information	Determining or extracting novel sensitive information by analyzing information
PA09.01.04	Deriving derogatory information	Determining or extracting novel derogatory information by analyzing information
PA09.02	Behavioral analysis	Leveraging information to determine or infer the behavior 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
PA10	**SHARING**	**Making information available to another entity**

Table A2: PANOPTIC Taxonomy Structure & Definitions – Privacy Activities

ID	Activity/Threat Action	Definition
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	Doxing	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
PA11	**USE**	**Leveraging information to achieve a goal**
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
PA12	**RETENTION & DESTRUCTION**	**Actions that affect the persistence of information**
PA12.01	Data not destroyed after use	Information has not been disposed of at the conclusion of its lifecycle
PA12.02	Data improperly destroyed	Information remains at least partially recoverable despite attempts to destroy it
PA13	**DEVIATIONS**	**Data action diverges from established limits bounding the data action in question**
PA13.01	Deviating from usage restrictions	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