A Reactive Approach for Use-Based Privacy*

Eleanor Birrell Fred B. Schneider

Department of Computer Science
Cornell University
Ithaca, NY 14853
{eleanor, fbs}@cs.cornell.edu

November 24, 2017

Abstract

Use-based privacy views privacy in terms of authorized uses, a philosophy well-suited for data collection and data analysis applications that arise in networked information systems. This work takes a first step toward investigating the technical feasibility of use-based privacy. We identify requirements for a feasible, expressive, use-based privacy regime. A user-study with 100 Amazon Turkers gives evidence for the validity of these requirements. And the approach is instantiated through *avenance policies*, whose expressiveness is assessed by formulating HIPAA and the Facebook privacy policies.

1 Introduction

Privacy is often defined in terms of access control, a view dating back to Warren and Brandeis' seminal paper [45] and embodied in the design of many privacy languages [2, 14, 26, 23]. This view, however, is poorly suited to a world where data sharing is pervasive and information is often collected and used without user awareness (e.g., security cameras, smartphone sensors, online tracking). Our work explores an alternate view, sometimes called *use-based privacy* [10, 11, 31]. Use-based privacy is not just concerned with keeping certain information secret. It also concerns restricting how information is used. Privacy is achieved only when data handlers comply with specified use restrictions.

Use-based privacy subsumes a broad range of extant privacy definitions:

- The Warren-Brandeis definition is fundamentally about secrecy (the authors believed that the right to privacy ceases after consensual publication), but it can be viewed as a special case of use-based privacy wherein a single type of use (i.e., publication) is either permitted or prohibited.

*Supported in part by AFOSR grants F9550-16-0250 and grants from Microsoft.

- Contextual integrity [32, 33] defines privacy in terms of uses relative to an *appropriate context*. Whether a context is appropriate might depend on time, location, purpose, and/or participating principals. Contextual integrity thus distinguishes different types of uses (those for which the current context is appropriate versus those for which it is not) and, therefore, can be described naturally as a form of use-based privacy.

- Differential privacy [16] classifies a response to a database query as a privacy violation unless the algorithm used to generate the response satisfies a specific statistical property (viz., ε-differential privacy). Under this definition, each response-generating algorithm can be considered a use, and uses can be classified according to the level of differential privacy they satisfy. Uses permitted by the privacy policy of the data owner would be the set of ε-differentially private algorithms, for some choice of ε.

As part of an investigation into the inherent feasibility of use-based privacy, this paper identifies characteristics of a language well-suited to expressing use-based privacy policies. Drawing on examples from data-use contracts, existing privacy policies, and U.S. regulations, we identify four requirements: (1) policies must be human-readable and legally interpretable, (2) policies must be able to specify both sticky and jurisdictional restrictions, (3) policies must be able to describe permissions as well as obligations, and (4) policies must be allowed to depend on the history of events that have occurred, a characteristic termed *reactive* [25]. These requirements are discussed in Section 2.

To determine whether these requirements accurately capture end-user demands for use-based privacy, we undertook a study with 100 Mechanical Turk users. Respondents were asked about their privacy preferences in general and about their comfort with various proposed privacy policies. The survey results confirmed that the four requirements identified above are critical to a successful use-based privacy regime. Section 3 discusses this.

Having established requirements for specifying use-based privacy, we then suggest one possible instantiation, *avenance policies*, which express use-based authorizations in terms three characteristics: (1) who is using the data, (2) the type of use (i.e., which operation accesses the data), and (3) the purpose of that use. All three characteristics are defined in human-readable terms that have legally interpretable definitions. The manner in which an avenance policy's authorizations change is encoded as a *privacy automaton*, a finite state automata defined over events inspired by RIF automata [25]. Privacy automata enable avenance policies to express both sticky and jurisdictional use restrictions, to express both permissions and obligations, and to be reactive. The semantics for avenance policies is described in Section 4.

Finally, we explore expressiveness of avenance policies by demonstrating how they can be used to specify real-world privacy policies. Two common sources of use-based privacy policies are privacy regulations and corporate privacy policies. So we encoded the full set of privacy requirements defined by two representative example use cases—the Health Information Portability and Accountability Act (HIPAA) [22] and Facebook's site privacy policy [18]—as avenance policies. Our experience is discussed in Section 5.

The jury is out on whether use-based privacy is a viable. This work constitutes one piece in an ongoing effort to resolve this question. Here, we take the first step by determining whether it is even feasible to express use-based privacy policies. Avenance policies, which can fully encode real-world privacy policies, constitute evidence for feasibility. A full ecosystem for use-based privacy will require more than just a language. It will also require an effective enforcement regime, including an efficient mechanism for associating policies with data. Automated enforcement mechanisms are the subject of a companion paper [6] and are the focus of our ongoing work.

2 Requirements for Use-based Privacy

To define a privacy policy, it is necessary to have some notion of *authority*, which determines the principals allowed to impose those policies. A common approach is to assert that data handlers are policy authorities for data they store; data handler-defined policies might implement contractual agreements with business partners, internal corporate policies, industry standards, or legal requirements. However, a system that relies exclusively on data handler-defined policies would resemble the current "notice and consent" privacy regime. It would give the *data subject* a single all-or-nothing choice: decline to use the system or consent to the privacy policy for their data offered by the data handler. Like "notice and consent," this approach would presume that an informed decision is made separately for each data handler with which a data subject interacts. For someone who interacts with many services, reading and understanding each policy is likely to be infeasible [15, 28, 9, 44].[1] Additionally, in order to read all the relevant site privacy policies, data subjects must know which service providers might receive their data; embedded content, URL redirects, and undisclosed business relations make this infeasible. So we are driven to a regime that allows people to be policy authorities for data about themselves.

A regime in which people define policies must ensure these people understand policies they define. A policy that describes exactly how data will be used, in all cases, at a level of implementation detail that can be automatically enforced, is unlikely to be comprehensible to humans. A policy that specifies data uses intensionally and in human-readable language, however, will necessarily employ uninterpreted natural language that might elide or ambiguously specify relevant details, precluding enforcement by existing automated tools.

We resolve the tension between human-readability and automated enforcement by appealing to existing non-technical solutions. Our society long ago evolved institutions for handling violations to the spirit of a law (and cases where explicitly specifying a formal policy is infeasible). These institutions have people interpret and judge whether a violation has occurred. Human judges view evidence of circumstances associated with some action, and these judges—invoking common sense as well as knowledge of norms—decide whether some action is a violation. A use-based privacy regime can incorporate these institutions by relying on human judges (aided by experts) to determine whether a program segment constitutes a particular type of use (where the type of use is described in human-readable, legally-interpretable natural language). Human interpretation can either occur in advance of the use (enabling automated runtime enforcement) or after the fact (creating an audit-based compliance regime that relies on deterrence through accountability). So we have:

[1] By one estimate [30], it would take the average American Internet user 244 hours to read the site privacy policies for all service providers with which they interact in a single year.

> **Policy Transparency Requirement.** *A use-based privacy regime must express its restrictions in a human-readable, legally-interpretable language.*

Many use restrictions are broadly applicable. For example, the policy "Date of birth may not be used to target ads" is probably not restricted to particular companies or jurisdictions. So a use-based privacy regime must be able to support *sticky policies*—policies that are associated with a value and that apply to all uses of this value as it flows through the system. In some cases, restrictions might apply only within a specific context. For example, EU law imposes retention and deletion requirements on service providers operating within the EU. Any service provider operating in the EU should associate these use-restrictions with data they receive, but these restrictions do not apply to service providers operating in other jurisdictions. So an expressive language should also admit *local policies*, which do not propagate use restrictions to third parties. In summary:

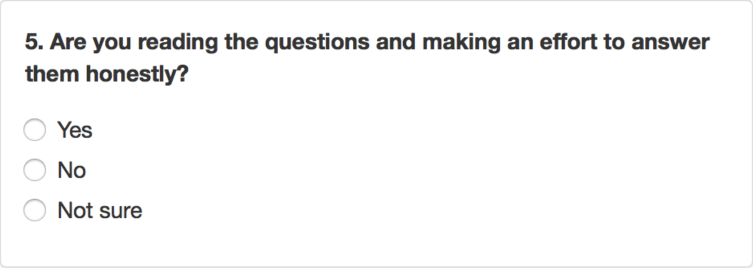
> **Policy Scope Requirement.** *A use-based privacy regime must be able to express both sticky policies and local policies.*

Use-based privacy policies are often expressed as permitted uses or prohibited uses, e.g., "email address may be used to send notifications" or "email address may not be used to send promotional offers." However, a language that only expresses permitted or prohibited uses is likely to be inadequate, because use-based policies might also be violated when no action is taken. For example, "Credit card information can be shared with third parties, but remote copies must be deleted within 90 days" requires a means to express *obligations*—time-limited mandatory uses. That leads us to conclude:

> **Restriction Type Requirement.** *A use-based privacy regime must be able to express permissions, prohibitions, and obligations.*

During program execution, information flows from values to derived values. A use-based privacy regime must, therefore, define policies for derived values. For example, a user who prohibits ads targeted based on their date of birth might still want to permit ads to depend on birthday ("Happy Birthday!"), even though birthday is derived from date of birth. Or, a user might prohibit specific details in a health record from being used for medical research, but might allow research using statistics derived from collections of health records. A policy might state that contact information may be shared with third parties only after opt-in authorization is received from the data subject. Or advertising might be allowed based on a single HTTP request (i.e., re-marketing) but might be prohibited based on values derived from the entire browsing history (i.e., targeted advertising). We conclude that policies are best defined as sets of restrictions that depend both on the use and on the provenance of the value, and these *reactive authorizations* must be propagated from initial values to derived values.

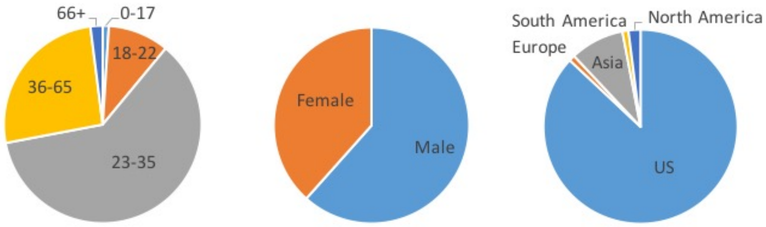
> **Reactive Requirement.** *A use-based privacy regime must support history-dependent policies.*



5. Are you reading the questions and making an effort to answer them honestly?

○ Yes
○ No
○ Not sure

Figure 1: Attention question



(a) Age (b) Gender (c) Location

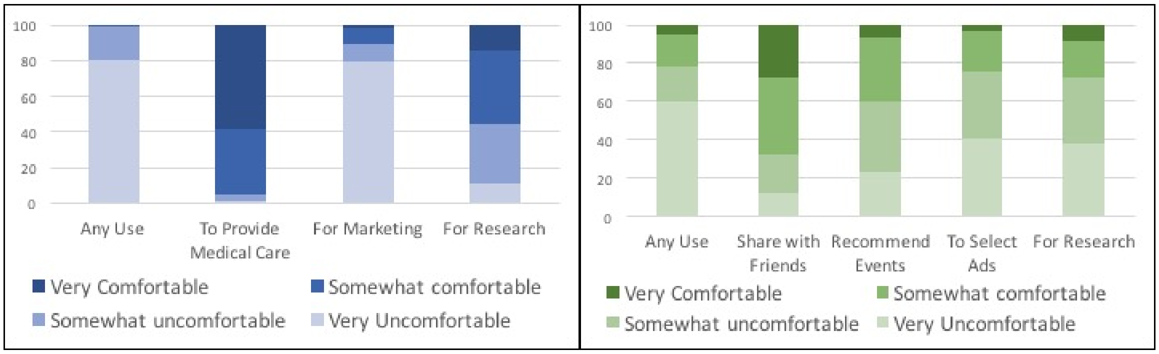
Figure 2: Study subject demographics

3 User Study

Collectively, the four requirements identified in Section 2 circumscribe an approach to use-based privacy. But this approach is only useful if it accurately reflects end-user preferences and priorities. To determine whether our four requirements are consistent with the privacy goals of actual users, we conducted a user study on Amazon Mechanical Turk.

A large body of prior work has employed user studies to understand user preferences and behaviors regarding information privacy [5, 20, 38, 29, 41, 27, 13]. These studies focus on identifying user preferences about data sharing. In our work, the goal is instead to understand user preferences about data use and to determine whether these preferences are consistent with the identified requirements. Our work has not considered the preferences of developers, who would ultimately implement these policies; though developer compliance might be compelled through regulation or contractual obligations. Instead, we focus here on determining whether the approach to use-based privacy characterized above accurately reflects end-user privacy preferences.

We surveyed 100 users using Amazon Mechanical Turk. Respondents were limited to those with at least 50 approved HITs and at least a 90% approval rate; each respondent was rewarded with 25 cents. The survey was posed as a sequence of multiple choice questions. Responses that failed the attention question (Figure 1), those with default answers (the first answer for all questions), and those with inconsistent answers (respondents who reported they were very comfortable with their information being used for any use but uncomfortable



(a) Medical Data

(b) Social Network Data

Figure 3: Subject preferences regarding data use

	Any Use	Medical	Marketing	Research
Any Use	1	$< .0001$	.1264	$< .0001$
Medical	$< .0001$	1	$< .0001$	$< .0001$
Marketing	.1264	$< .0001$	1	$< .0001$
Research	$< .0001$	$< .0001$	$< .0001$	1

(a) Medical Data

	Any Use	Share	Recommend	Ads	Research
Any Use	1	$< .0001$	$< .0001$	.1344	.0211
Share	$< .0001$	1	$< .0001$	$< .0001$	$< .0001$
Recommend	$< .0001$	$< .0001$	1	.0023	.0474
Ads	.1344	$< .0001$	.0023	1	.3493
Research	.0211	$< .0001$	.0474	.3493	1

(b) Social Network Data

Figure 4: p-Values for subject preferences regarding data use

with their information being used for particular uses) were dropped. The respondents were predominantly American (87%) and slightly over half were male (61%). Age varied, but most subjects were working-age adults. The median completion time for the full survey was 8.1 minutes. The survey is reproduced in Appendix A.‘

We began by surveying whether a use-based view of privacy actually reflects user privacy preferences. We asked each subject to imagine an organization that stored and used their data (a health care provider or a social network) was defining a new data use policy, and we queried how comfortable the subject would be to permit each of a set of specific proposed uses using a four-point Likert scale: very uncomfortable, somewhat uncomfortable, somewhat comfortable, or very comfortable. Reported comfort levels varied significantly with the type of use proposed. Users were more willing to authorize particular uses—e.g., medical purposes ($p < .0001$) or research ($p < .0001$) than to provide unrestricted access to data.

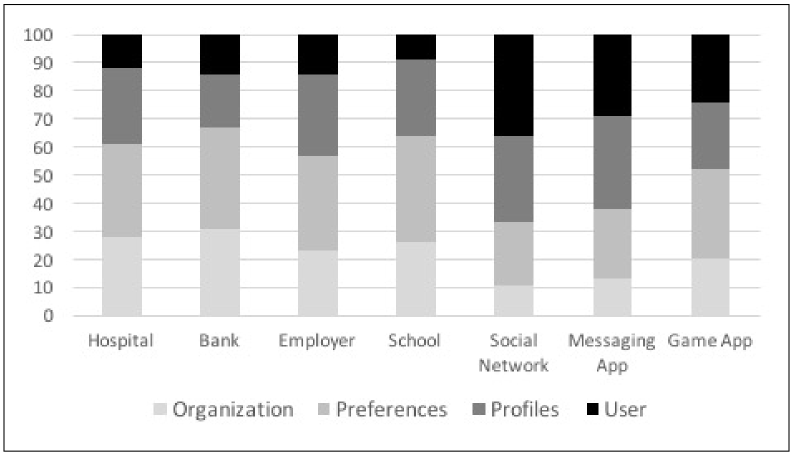


Figure 5: Subject preferences regarding policy authorities when interacting with various different types of organizations.

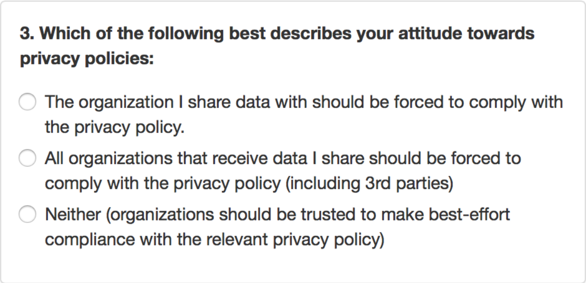
Preferences also depended on the type of use: medical purposes vs. marketing ($p < .0001$), medical purposes vs. research ($p < .0001$), marketing vs. research ($p < .0001$). Responses for selected uses are shown in Figure 3. p-values for the responses are given in Figure 4. We interpret these data as evidence that use-based privacy is an acceptable model of user privacy preferences.

We then asked a series of questions designed to determine whether users' general privacy preferences conformed with three of the requirements for use-based privacy identified in above: (1) Policy Transparency Requirement, (2) Policy Scope Requirement, and (3) Reactive Requirement. We did not ask about Restriction Type Requirement because that requirement is necessary to support existing privacy policies and does not depend on assumptions about user preferences.

Policy Transparency Requirement. Recall this requirement stems from our belief that a use-based privacy regime should allow users to act as policy authorities. To determine its soundness, we presented subjects with a set of questions designed to investigate user preferences about policy authorities—that is, questions about who should define data use restrictions. We offered four options: (1) the organization could define how data are used, (2) the organization could provide default use policies but allow the user to modify those defaults with their preference settings, (3) users could select from a set of preference profiles defined by third parties (e.g., privacy-oriented non-profits, governments, or trusted corporations), or (4) users could define their own data-use policies. We then asked users to select how they would prefer that privacy policies be defined for each of several types of organization: hospitals, banks, employers, schools, social networking sites, messaging apps, and game apps.

When interacting with trusted services (hospitals, banks, employers, schools), users were more willing to have the data-use policy defined by the organization (with or without preference settings).

When interacting with less-trusted services that handled sensitive data (social networks or messaging apps), users generally preferred to define their own policies. Detailed responses



3. Which of the following best describes your attitude towards privacy policies:

○ The organization I share data with should be forced to comply with the privacy policy.

○ All organizations that receive data I share should be forced to comply with the privacy policy (including 3rd parties)

○ Neither (organizations should be trusted to make best-effort compliance with the relevant privacy policy)

Figure 6: Example question asking about user preferences regarding policy scope

	Granularity	Anonymity	Aggregation	Time
Yes	48	66	58	23
Maybe	21	16	19	18
No	31	18	23	59

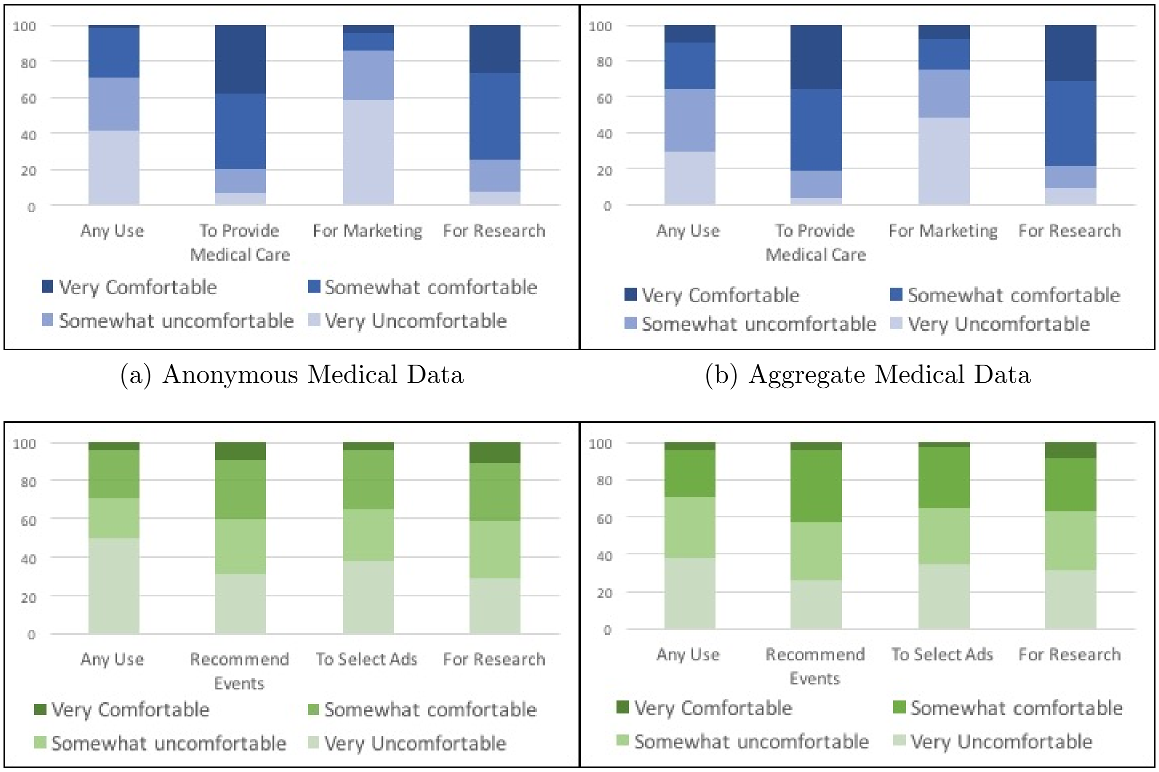
Figure 7: Factors influencing user data use preferences

are shown in Figure 5. For all services, a significant percentage of users wanted more control over the policies governing data use. Depending on how trusted the service was and how sensitive the handled data was, 33%-67% of respondents would prefer setting their own policies over policies defined by the service *even if the service allowed the user to set privacy preferences*. We view these responses as confirming that a use-based privacy regime should have users as policy authorities, which also reaffirms the requirement that a use-based privacy regime should express policies in a human-readable, legally-interpretable language.

Policy Scope Requirement. Local policies are needed for legal regulations; sticky policies are presumed to be needed for user preferences. So we surveyed our subjects to determine whether this presumption accurately reflects user privacy goals (Figure 6). We found that 67% of users thought that policies should be able to restrict behavior by third parties, a finding that confirms the policy scope requirement.

Reactive Requirement. We asked users whether they thought permitted uses might need to change for derived information: 48% thought their preferred policy would be depend on the granularity of the data, 66% thought their data use preferences would change if the data were anonymized, and 58% thought their data use preferences would change if their data were aggregated with that of other users. In addition, 41% of users thought their preference would or maybe would change after a period of time. These results reinforce our view that reactive policies are needed for representing user privacy preferences.

We further explored user preferences toward reactive policies by revisiting our hypothetical organizations (either a health care provider or a social network) that define a new data use policy. Each subject was queried about comfort with each of a new set of proposed policies, each of which changed its restrictions in concert with changes to the provenance of



(a) Anonymous Medical Data

(b) Aggregate Medical Data

(c) Anonymous Social Network Data

(d) Aggregate Social Network Data

Figure 8: User Preferences for Derived Data Use

the data (either anonymization or aggregation). The survey results support our belief that reactive policies are needed for expressing user preferences. Except for particular conditions that were deemed broadly acceptable under any circumstances (use by medical personnel, use for research with notification), preferences changed significantly when medical data is anonymized ($p = .004$ to $p = .02$, depending on use) or aggregated ($p < .0001$ to $p = .002$, depending on use). In general, users were less comfortable with various proposed uses for social network data (especially posts) than for medical data. However, some similar trends emerged. Users were more willing to authorize a particular use: recommending posts or events ($p < .0001$), recommending third party apps ($p = .02$), or research ($p = .02$). Users also distinguished between their intended use (sharing posts with friends) and other proposed uses ($p < .0001$ for recommending, advertising, and research uses). And users were significantly more likely to allow anonymized posts to be used to provide personalized recommendations ($p = .01$) or to conduct research ($p = .004$) and were more likely to allow aggregated information derived from their posts to be published ($p = .03$).

Overall, our survey results affirmed each of our assumptions about user preferences. This, in turn, suggests that a policy regime that satisfies these requirements could form the foundation for an acceptable implementation of use-based privacy.

Authorization Triples:	States:	Policy Rules:
$\mathsf{I} := \mathsf{invoker} \mid \mathsf{I} \cap \mathsf{I} \mid \mathsf{I} \cup \mathsf{I}$	$s := (\mathsf{I,P,E}) \mid s \wedge s \mid s \vee s$	$r := (\mathsf{transType}, S, s_0, T, s_v)$
$\mathsf{P} := \mathsf{purpose} \mid \mathsf{P} \cap \mathsf{P} \mid \mathsf{P} \cup \mathsf{P}$	$S := \{s_1, \ldots, s_n\}$	
$\mathsf{E} := \mathsf{useType} \mid \mathsf{E} \cap \mathsf{E} \mid \mathsf{E} \cup \mathsf{E}$		
Transition Types:	Transitions:	Policies:
$\mathsf{transType} := \mathsf{useType}\ \cup \mathsf{cEvent}$	$T:\ S \times \mathsf{transType} \rightarrow S$	$\rho := r \mid \rho \wedge \rho \mid \rho \vee \rho$

Figure 9: Avenance Policy Syntax.

4 An Instantiation of Use-based Privacy

To further explore the feasibility of use-based privacy, we developed one possible instantiation. *Avenance policies*[2] are predicates $P(u, h)$ associated with a value v that specify whether a use u of value v is prohibited or allowed after history h has transpired. So, for example, an avenance policy associated with a user's date of birth might not initially allow that value to be used for advertising, but after the year has been deleted, might allow the resulting value (the user's birthday) to be used for advertising.[3]

Avenance policies ρ are specified as conjunctions and disjunctions of *policy rules*

$$\rho := r \mid \rho \wedge \rho \mid \rho \vee \rho.$$

A policy rule r is represented as a *privacy automaton*—a finite state automaton that encodes history-dependent use-based authorizations. Formally, a policy rule is defined as a 5-tuple

$$r := (\mathsf{transType}, S, s_0, T, s_v)$$

where $\mathsf{transType}$ is the alphabet for transitions (i.e., the set of events in a history that might change the current set of authorized uses for a value), $S := \{s_0, \ldots, s_n\}$ is the set of states, s_0 is the initial state, T is the state-transition function

$$T:\ S \times \mathsf{transType} \rightarrow S,$$

and s_v is the violation state. Observe that unlike standard finite state automata, privacy automata do not explicitly define a set of accepting states; they instead specify a violation state s_v. A sequence of uses is *policy compliant* if each use is authorized by the current state at the time that use occurs and if it never enters the violation state s_v. The syntax for avenance policies is summarized in Figure 9.

A state s_i in a privacy automaton defines the set of permitted uses when the privacy automaton is in that state. This set of permitted uses is specified by conjunctions and disjunctions of *authorization triples*, predicates expressed as triples $(\mathsf{I,P,E})$, where I identifies an invoking principal, P denotes a purpose, and E is some executable binary.

$$s := (\mathsf{I,P,E}) \mid s \wedge s \mid s \vee s$$

[2] The term avenance is derived from the French word *avenir*, meaning future or yet to occur; the etymology is analogous to that of provenance (from *provenir*).

[3] For practical reasons, we restrict avenance policies to uses determined solely by the party currently holding the associated value and to histories that only depend on the provenance of the associated value.

I may be defined as a single principal or may be a role, P may be drawn from a hierarchy of purpose labels, and E may be specified by a binary hash or by a type drawn from a hierarchy of program labels. *Compound components* I, P, or E are constructed using unions and intersections.

$$\begin{aligned}
\mathsf{I} &:= \mathsf{invoker} \mid \mathsf{I} \cap \mathsf{I} \mid \mathsf{I} \cup \mathsf{I} \\
\mathsf{P} &:= \mathsf{purpose} \mid \mathsf{P} \cap \mathsf{P} \mid \mathsf{P} \cup \mathsf{P} \\
\mathsf{E} &:= \mathsf{useType} \mid \mathsf{E} \cap \mathsf{E} \mid \mathsf{E} \cup \mathsf{E}
\end{aligned}$$

Semantically, an authorization triple $(\mathsf{I}, \mathsf{P}, \mathsf{E})$ specifies a predicate that allows a use if it is in all three component sets; a state is interpreted as a predicate defined by conjunctions and disjunctions of authorization triples. Example policies demonstrating the use of authorization triples to define single-state privacy automata are given below.

Example 1. *Data may be viewed by medical personnel for the purpose of providing counseling or medical care:*

$$\{(\mathsf{doctors} \cup \mathsf{nurses}, \mathsf{medical\ care} \cup \mathsf{counseling}, \mathsf{view})\}$$

Example 2. *Data may be viewed by coaches and by researchers; researchers may use data to conduct research:*

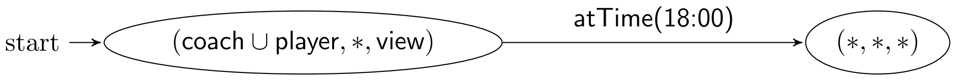
$$\{(\mathsf{coach} \cup \mathsf{researcher}, *, \mathsf{view}) \vee (\mathsf{researcher}, \mathsf{research}, *)\}$$

Transitions in a privacy automaton are triggered by events τ in the language $\mathsf{transType}$ that cause the automaton to change its state. We consider two classes of events: *contextual events* and *synthesis events.*

$$\mathsf{transType} := \mathsf{cEvent} \cup \mathsf{useType}$$

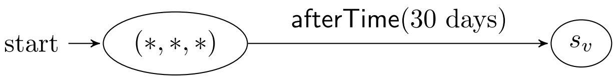
Contextual events are elements of a language cEvent. These might include *temporal events*—clock-triggered events that can be expressed either absolutely ($\mathsf{atTime}(t)$) or a relatively ($\mathsf{afterTime}(t)$)—or user actions (e.g., a change in a user's privacy settings). The mechanism responsible for enforcing policy compliance is responsible for updating the state of affected policy rules when contextual events occur.

Example 3. *Data may be viewed by coach and players; data becomes public after 18:00.*



Temporal events are handy for expressing obligations. To capture such obligations, we introduce a $\mathsf{violation}$ automata state s_v. If a privacy automaton enters the violation state s_v, that policy (i.e., the obligation) has been violated.

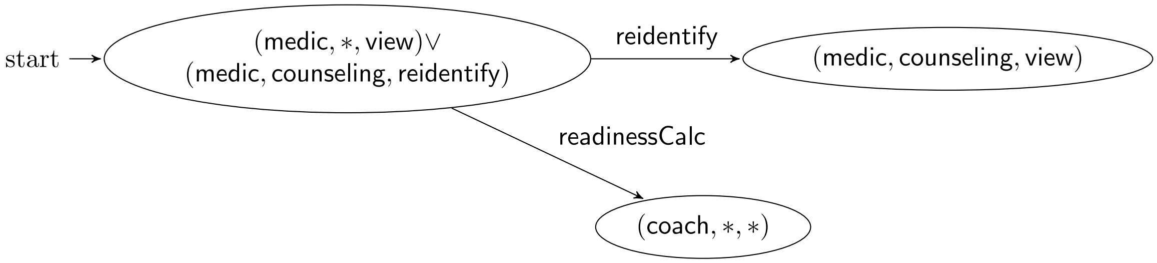
Example 4. *Data must be deleted within 30 days.*



Synthesis events correspond to the generation (synthesis) of new data values. These events are drawn from the language useType that was used to express permissions for executables. The policy associated with the output of a synthesis event is the conjunction of the policies associated with the tagged values that influence the new value according to standard information flow rules; this includes implicit information flows. The current state of each privacy automata (i.e., policy rule) in the derived policy is determined by matching the synthesis event against the transitions in each of the input automata.

So, for example, if a value (e.g., anonymous mood data) is associated with the policy shown in Example 5 and is then reidentified, the resulting derived data (i.e., the reidentified mood data) may be viewed by medics for the purpose of providing counseling. If the data used to reidentify the pseudo-anonymized mood data (e.g., a mapping between pseudonyms and identities) was also associated with an avenance policy, then the resulting identified mood data would be associated with the conjunction of two policies: one derived from the automaton associated with each of the two inputs.

Example 5. *Anonymous mood data may be viewed by medical personnel. Anonymous mood data may be re-identified and subsequently viewed by medical personnel for the purpose of providing counseling. Derived readiness score may be used by coaches.*



Avenance policies are parameterized by sets of labels role, purpose, useType, CEvent; these sets are defined by some namespace associated with the policy. We presume an agreed *interpretation* for each label—a legally-binding definition of the programs comprising that type (e.g., a specific natural-language explanation). Different namespaces could be defined by individual data stores, service providers, or established nonprofit organizations. One example namespace is given in Example 6.

Example 6. *PMSys is a mobile and web-based application developed at the University of Tromsø that performs physiological evaluation and training-load personalization for soccer players. PMSys collects data about player mood, sleep patterns, physical fitness, and injuries. These data are subject to data-use restrictions derived both from the data-use contract signed by the players (who all are members of elite clubs and national teams in Norway, Sweden, and Denmark). The following namespace was defined to support policies for the PMSys soccer application:*

$$\begin{aligned}
\mathsf{role} &:= \{\mathsf{medical,\ coach,\ player}\}\\
\mathsf{purpose} &:= \{\mathsf{prevention,\ diagnosis,\ care,\ intervention}\}\\
\mathsf{useType} &:= \{\mathsf{view,\ sendTo}(\cdot)\mathsf{,\ delete,\ average,}\\
&\qquad \mathsf{pseudonoymize,\ reidentify,\ readinessCalc,}\\
&\qquad \mathsf{rosterCalc}\}\\
\mathsf{cEvent} &:= \{\mathsf{atTime}(\cdot)\mathsf{,\ afterTime}(\cdot)\}
\end{aligned}$$

5 Evaluating Avenance Policy Expressiveness

Avenance policies have utility only if they are able to describe privacy policies that arise in practice. To evaluate that, we selected two applications: U.S. federal privacy regulations defined in the Health Information Portability and Accountability Act (HIPAA) [22] and Facebook's site privacy policy [18]. Each application is representative of a class of data use policies (privacy regulations and site privacy policies, respectively) that constitute common sources of use-based policies. So, for each, we determined whether and how the imposed use-restrictions might be expressed as avenance policies. Success with these example applications increases our confidence in the broad applicability of the avenance approach.

5.1 HIPAA

HIPAA regulates members of the health care industry. In addition to defining rules for information storage and security, it imposes limitations on how health providers or *covered entities* may use and disclose personal health information.

To encode HIPAA's data-use rules, we use a variant of Semantic Parameterization [7]. For each rule, we identify five properties constraining the use:

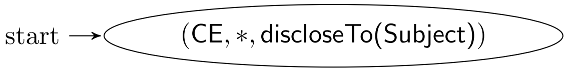
1. The *object* is the data to which the use restriction applies.
2. The *invoker* is the principal that invokes the use.
3. The *purpose* is the goal of the activity.
4. The *action* is the type of use covered by the rule.
5. The *condition* is a boolean expression indicating when the rule applies.

We analyzed §164.502-§164.528 of the HIPAA Privacy Rule—the sections describing restrictions on how data may be used—and extracted 95 data-use tuples. We then manually analyzed each of the resulting data-use tuples, and we formalized each tuple as an avenance policy rule. The full encoding is given in Appendix B.

Inspecting the resulting policies, we observed that invoker, purpose, and action defined a authorization triple (I, P, E) that could be expressed in the avenance language. Some data-use rules referred to a particular action (e.g., Example 7), but many restrict use according to purpose instead of by operation (e.g., Example 8).

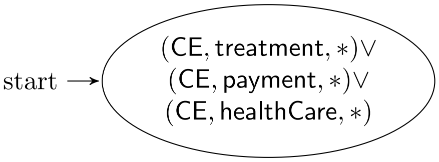
Example 7. HIPAA §164.502(a)(1)(i): *A covered entity is permitted to disclose protected health information to the individual.*

Object	Invoker	Purpose	Action	Condition
PHI	CE	$*$	discloseTo(Subject)	



Example 8. HIPAA §164.506(c)(1): *A covered entity may use or disclose protected health information (PHI) for its own treatment, payment, or health care operations.*

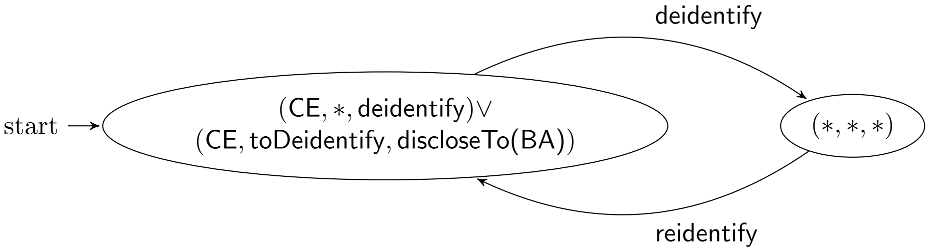
Object	Invoker	Purpose	Action	Condition
PHI	CE	treatment	$*$	
PHI	CE	payment	$*$	
PHI	CE	healthCare	$*$	



Some HIPAA privacy rules refer to particular classes of objects objects (e.g., de-identified health information); these define how data may be used after specific transformations have occurred.

Example 9. HIPAA §164.502(d): *(1)A covered entity may use protected health information to create information that is not individually identifiable health information or disclose protected health information only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity. (2) Health information that meets the standard and implementation specifications for deidentification under §164.514(a) and (b) is considered not to be individually identifiable health information, i.e., de-identified. The requirements of this subpart do not apply to information that has been de-identified in accordance with the applicable requirements of §164.514, provided that: (i) [...] and (ii) If de-identified information is re-identified, a covered entity may use or disclose such re-identified information only as permitted or required by this subpart.*

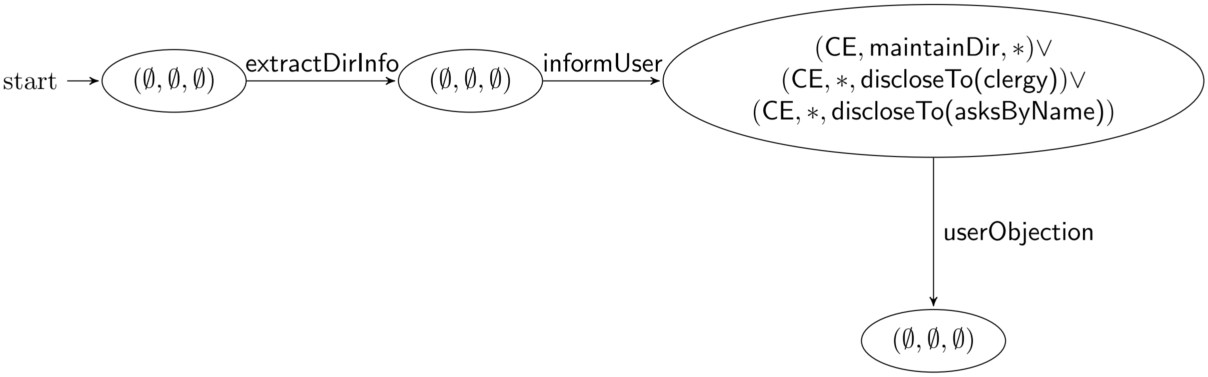
Object	Invoker	Purpose	Action	Condition
PHI	CE	$*$	deidentify	
PHI	CE	toDeidentify	discloseTo(BA)	
de-identified HI	$*$	$*$	$*$	



Other HIPAA rules specify conditions under which that rule applies. These conditions would be encoded in an avenance policy using contextual events. In the following example, specific information has additional permissions, but only as long as the user (i.e., the subject of the data) is aware of the possible use and does not object. To encode this data use rule, we employ two contextual events—informUser and userObjection—to specify how the authorization changes after the data subject has been informed of the possible use and after the data subject registers an objection to those uses.

Example 10. HIPAA §164.510(a)(1): *Except when an objection is expressed in accordance with paragraph (a)(2) of this section, a covered health care provider may: (i) Use the following protected health information to maintain a directory of individuals in its facility: (A) The individual's name; (B) The individual's location in the covered health care provider's facility; (C) The individual's condition described in general terms that does not communicate specific medical information about the individual; and (D) The individual's religious affiliation; and (ii) Disclose for directory purposes such information: (A) To members of the clergy; or (B) to other persons who ask for the individual by name. (2) Opportunity to object. A covered health care provider must inform an individual of the protected health information that it may include in a directory and the persons to whom it may disclose such information (including disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by paragraph (a)(1) of this section.*

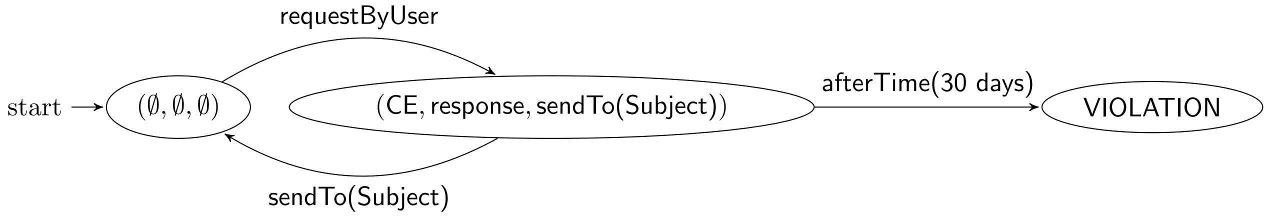
Object	Invoker	Purpose	Action	Condition
directory info	CE	maintainDir	$*$	after informUser unless userObjection
directory info	CE	$*$	discloseTo(clergy)	after informUser unless userObjection
directory info	CE	$*$	discloseTo(asksByName)	after informUser unless userObjection



Finally, some HIPAA privacy rules impose obligations rather than expressing permissions. These rules are expressed in the avenance language by using temporal transitions. Actions that fulfill obligations are contextual events, which trigger a state transition.

Example 11. HIPAA §164.524(b): *(1) The covered entity must permit an individual to request access to inspect or to obtain a copy of the protected health information about the individual that is maintained in a designated record set. (2)(i) The covered entity must act on a request for access no later than 30 days after receipt of the request as follows.*

Object	Invoker	Purpose	Action	Condition
PHI	CE	response	SendTo(Subject)	



Because we were able to express all 95 identified data use rules as avenance policy rules, our experience with HIPAA confirms that types of data-use restrictions defined by the HIPAA Privacy Rule can be expressed as rules in the avenance policy language.

Five HIPAA data-use rules, however, illustrate what might be termed *second-order use restrictions*. For example, §164.508, which deals with user authorizations (and exceptions to the authorization requirement), includes the statement that covered entities may use protected health information for any use explicitly authorized by the user.

Example 12. HIPAA §164.508(a)(1): *Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization.*

This privacy rule can be expressed in the avenance language using an uninterpreted label authorizedUses. However, we do not consider such a formulation to be useful for policy enforcement. Instead, we would expect to handle second-order rules simply by adding additional policy rules (corresponding to the authorized uses) to the avenance policy at the time an authorization is received.

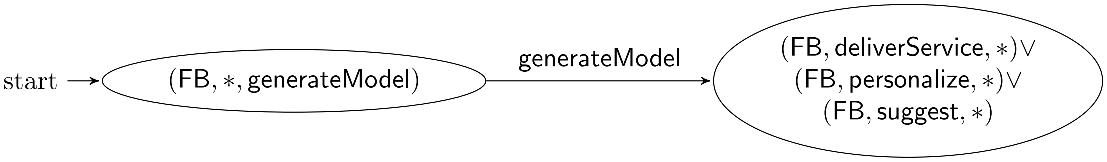
5.2 Facebook Privacy Policy

For our second case study, we selected of Facebook's Data Use Policy [18], which states how Facebook uses information it collects. Facebook is a widely used service provider; the terms of its data use policy are typical for the industry. The ability to express Facebook's data use policy is therefore a positive indicator for the avenance approach.

We performed a detailed analysis of Facebook's data use policy. Adopting the standard legal interpretation, we view any stated use as a permission. We employ the same methodology as we used to analyze HIPAA: first code each sentence of the data use policy using our five-fold attribute classification (this results in a set of 38 data use tuples) then formulate each of these tuples as an avenance policy rule. An example data use rule from Facebook's data use policy is given in Example 13; the full data use policy is described in Appendix C.

Example 13. *We are able to deliver our Services, personalize content, and make suggestions for you by using this information to understand how you use and interact with our Services and the people or things you're connected to and interested in on and off our Services.*

Object	Invoker	Purpose	Action	Condition
PI	FB	$*$	generateModel	
user model	FB	deliverService	$*$	
user model	FB	personalize	$*$	
user model	FB	suggest	$*$	



Facebook's data use policy describes permitted behaviors both in terms of particular functions (e.g., generating a user model) and general purposes that might motivate a variety of different functions (e.g., delivering services). Many rules depend on state transitions triggered by both synthesis (e.g., user model generation, anonymization, aggregation) and contextual events (e.g., changes in user settings). Facebook promises to delete posts after an account is deleted, defining an obligation. Note, however, that Facebook's data use policy does not contain any second-order rules. The published policy does modify the set of valid authorizations when a user updates preference settings; however this set of settings is a finite, pre-defined set that can be expressed by our first-order semantics.

6 Related Work

Use-based Privacy. Use-based privacy was first introduced by Cate [10] as a solution to the problems presented by the current regime of "notice and consent" and the underlying guidelines—the Fair Information Practice Principles [12]—that defined acceptable standards for handling sensitive data. Observing that users rarely make use of either opt-ins or opt-outs and typically don't make informed decisions about access to their data, Cate proposed a new approach. His work explored the legal and philosophical implications of use-based privacy; the feasibility of a technical regime for expressing or enforcing use-based privacy was not addressed.

Use-based Regimes. Usage Control (UCON) [35, 36] is an extension of traditional access control models (e.g., discretionary access control, mandatory access control, role-based access control) that enables continuity of access decisions. Here access control decisions are re-evaluated after the context (e.g., subject roles, time, number of previous accesses) changes. UCON was a reaction to increased networking and data sharing within a diverse ecosystem of devices; although not focused on privacy, it can be viewed as the first technical approach to use-based authorizations. Despite the name, however, UCON retains the tradition focus on authorizing accesses rather than uses. UCON can be instantiated with a variety of policy languages, but it does not support reactive policies (although it does allow actions to update subject, object, or environment properties). Initial UCON systems enforced policies on a single system, but later versions introduced distributed usage control [39, 21].

An alternative approach to use-based privacy was outlined by Petković et al. [37], who consider a restricted form of use-based authorization, which they call *purpose control.* Their work creates an audit log of service provider actions and then detects policy violations by checking whether the audit trail is a valid execution of the organizational process—modeled as a formula in the Calculus of Orchestration of Web Services (COWS)—for a permitted purpose. This work does not consider the invoker or the program type, and there is no notion of policy synthesis for derived values.

Instantiations of Use-based Privacy. Many languages have been proposed for expressing privacy requirements, and some of these languages could be employed to express use-based privacy policies.

PRML [40] is an XML-based language for expressing privacy declarations—authorizations that depend on the role of the invoker, the type of operation, the purpose, and (optionally) some conditions. It was intended for expressing enterprise privacy policies, e.g., site privacy policies. But privacy declarations in PRML are not sticky, and there is no support for reactive policies.

The PrimeLife policy language [8, 1] is an extension of XACML that introduces a new obligation handling mechanism; this mechanism implements a down-stream usage authorization system that specifies whether data can be shared with a third party. Access control decisions might depend on the purpose of the access or on the type of operation (e.g., read, write, delete) and can also include triggered obligations; authorized data is associated with a sticky policy that defines downstream access control permissions. The PrimeLife policy language, however, does not support reactive policies.

Contextual Integrity [32] is a philosophical approach to privacy that has been formalized as a logic for reasoning about privacy [3]. Contextual integrity can be interpreted as a special case of use-based privacy; uses are authorized when they occur in an appropriate context. The logical formalization focuses exclusively on data transmission, but the approach can be applied more broadly. This approach inherently supports a limited form of reactive policies based on contextual events (i.e., changes in context). However, this approach does not support policy synthesis for derived values, and it does not include sticky policies or obligations.

SecPAL4P [4] is a declarative language for expressing user privacy preferences and service provider data handling policies. Authorizations are declared as SecPAL 3.1 assertions, which can depend on the purpose of the use. SecPAL4P does not support obligations.Also, SecPAL assertions are not sticky and do not support reactive policies.

Legalease [43] is a privacy policy language that implicitly supports use-based policies encoded as domain-specific attributes. For example, a legalese policy might say, "DENY DataType IP Address, UseForPurpose Advertising EXCEPT ALLOW DataType IPAddress:Truncated"; this policy states that the full IP address may not be used for advertising. Many use-based policies can be encoded in legalese by defining appropriate attributes. However, legalese does not support policies that are dependent on temporal or system events or policies that include obligations. It also does not support discretionary (user-defined) policies, local policies, or compound policies defined by multiple authorities. It does not support obligations or sticky policies, and it provides only limited support for reactive policies. Legalese is deployed in Grok, a policy compliance system for Bing that automatically maps code-level elements to attributes and enforces policies using compile-time information flow analysis.

The Thoth policy language [17] specifies data use policies comprising confidentiality, integrity, and declassification policies, each of which defines which principals are authorized and under what conditions. Although policies are designed to be expressed at a lower level than under our approach, Thoth's conditions are sufficiently flexible to capture policies that depend on who, what, or why as well as temporal, discretionary, autocratic, and jurisdictional policies. The language does not, however, support reactive policies. Thoth is implemented as a kernel-level compliance layer for enforcing data use policies in data retrieval systems.

Automata Policies. Avenance policies use privacy automata as policy rules to instantiate the reactive approach to use-based privacy proposed in this paper. Automata have long been used to model reference monitors [42, 19]. Under these frameworks, an automaton monitors the execution of a single program. The automaton can be interpreted as a policy for the monitored program; acceptance by the automaton means that the program is correct (or policy-compliant).

Lonet [24] is a system for expressing and enforcing security policies for shared data using isolated containers. Lonet policies—which are associated with data files and defined as metadata—are expressed as automata; states specify the set of authorized users and declare event-driven obligatory meta-code, and state transitions specify how to derive policies for derived values depending on the type of program that produces the derived value. Whether a use is authorized by a Lonet policy depends only on the type of use; Lonet policies do not consider the invoker or the purpose of the use, and the current state does not depend on any contextual events. Lonet policies were a precursor to avenance policies with coarser granularity and more limited expressiveness.

Pardo et al. [34] propose an automata-based approach to specifying dynamic privacy policies for online social networks. This work expresses evolving policies, in which the current privacy policy is activated or deactivated by contextual events. For example, "Co-workers cannot see my posts while I am not at work". These policies are parameterized over a static privacy policy language. The proposed approach does not admit synthesis events as state transitions and provides no means to derive policies for derived values.

7 Conclusion

An effective privacy regime needs to be compatible with modern practices for data collection, data sharing, and data use; use-based privacy offers a promising approach. We have taken a first step towards evaluating its feasibility. We identify requirements for a successful use-based privacy regime, and we vet these requirements with a user study. We also introduce avenance policies, an instantiation of use-based privacy that meets all four identified requirements. We evaluate this instantiation of use-based privacy by expressing the full set of data use policies defined in HIPAA and in Facebook's site privacy policy as avenance policies. We view the success of this experiment as evidence of the feasibility of this approach to use-based privacy. Widespread adoption will likely require an effective enforcement mechanism for ensuring policy compliance. But we view the avenance approach as a promising step towards developing a privacy-enhancing, use-based privacy ecosystem for the modern world.

Acknowledgements

We are grateful to Fred Cate and Peter Swire for fruitful discussions about early versions of these ideas, and to Deirdre Mulligan, Arvind Narayanan, Seda Gurses, and Molly Feldman for helpful feedback and comments on this paper.

References

[1] Claudio A. Ardagna, Laurent Bussard, Sabrina De Capitani di Vimercati, Gregory Neven, Stefano Paraboschi, Eros Pedrini, Franz-Stefan Preiss, Dave Raggett, Pierangela Samarati, Slim Trabelsi, and Mario Verdicchio. PrimeLife policy language. In *W3C Workshop on Access Control Application Scenarios*. W3C, 2009.

[2] Paul Ashley, Satoshi Hada, Günter Karjoth, and Matthias Schunter. E-P3P privacy policies and privacy authorization. In *Proceedings of the 2002 ACM Workshop on Privacy in the Electronic Society*, pages 103–109. ACM, 2002.

[3] Adam Barth, Anupam Datta, John C. Mitchell, and Helen Nissenbaum. Privacy and contextual integrity: Framework and applications. In *IEEE Symposium on Security and Privacy*, pages 184–198, 2006.

[4] Moritz Y. Becker, Alexander Malkis, and Laurent Bussard. A framework for privacy preferences and data-handling policies. *Microsoft Research Cambridge Technical Report, MSR-TR-2009-128*, 2009.

[5] Elizabeth A. Bell, Lucila Ohno-Machado, and M. Adela Grando. Sharing my health data: A survey of data sharing preferences of healthy individuals. In *AMIA Annual Symposium Proceedings*, volume 2014, page 1699. American Medical Informatics Association, 2014.

[6] Eleanor Birrell, Anders Gjerdrum, Robbert van Rennesse, Håvard Johansen, Dag Johansen, and Fred B. Schneider. SGX enforcement of use-based authorizations. In preparation.

[7] Travis D. Breaux, Matthew W. Vail, and Annie I. Anton. Towards regulatory compliance: Extracting rights and obligations to align requirements with regulations. In *Requirements Engineering, 14th IEEE International Conference*, pages 49–58. IEEE, 2006.

[8] Jan Camenisch, Abhi Shelat, Dieter Sommer, Simone Fischer-Hübner, Marit Hansen, Henry Krasemann, Gérard Lacoste, Ronald Leenes, and Jimmy Tseng. Privacy and identity management for everyone. In *Proceedings of the 2005 Workshop on Digital Identity Management*, DIM '05, pages 20–27, 2005.

[9] K. Cameron. The laws of identity. `http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf`, 2005.

[10] Fred Cate. Principles for protecting privacy. *Cato Journal*, 22:33–57, 2002.

[11] Fred Cate, Peter Cullen, and Viktor Mayer-Schönberger. Data protection principles for the 21st century. Oxford Internet Institute, 2013.

[12] Federal Trade Commission et al. Fair information practice principles. *last modified June*, 25, 2007.

[13] Sunny Consolvo, Ian E. Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge. Location disclosure to social relations: Why, when, & what people want to share. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 81–90. ACM, 2005.

[14] Lorrie Cranor, Marc Langheinrich, Massimo Marchiori, Martin Presler-Marshall, and Joseph Reagle. The platform for privacy preferences 1.0 (P3P 1. 0) specification. *W3C recommendation*, 16, 2002.

[15] Lorrie Faith Cranor and Paul Resnick. Protocols for automated negotiations with buyer anonymity and seller reputations. *Netnomics*, 2(1):1–23, 2000.

[16] Cynthia Dwork. Differential privacy. In *33rd International Colloquium on Automata, Languages and Programming, part II (ICALP)*, volume 4052, pages 1–12, Venice, Italy, July 2006. Springer Verlag.

[17] Eslam Elnikety, Aastha Mehta, Anjo Vahldiek-Oberwagner, Deepak Garg, and Peter Druschel. Thoth: Comprehensive policy compliance in data retrieval systems. In *USENIX Security Symposium*, pages 637–654, 2016.

[18] Facebook. Data policy. `https://www.facebook.com/full_data_use_policy`, September 2016.

[19] Richard Gay, Heiko Mantel, and Barbara Sprick. Service automata. In *Formal Aspects in Security and Trust.*, volume 7140 of *Lecture Notes in Computer Science*, pages 148–163. Springer, 2011.

[20] David Grande, Nandita Mitra, Anand Shah, Fei Wan, and David A. Asch. Public preferences about secondary uses of electronic health information. *JAMA Internal Medicine*, 173(19):1798–1806, 2013.

[21] M. Hilty, A. Pretschner, D. Basin, C. Schaefer, and T. Walter. A policy language for distributed usage control. In Joachim Biskup and Javier López, editors, *12th European Symposium On Research In Computer Security (ESORICS)*, volume 4734 of *Lecture Notes in Computer Science*, pages 531–546, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[22] Health insurance portability and accountability act (HIPAA), 1996.

[23] Johnson Iyilade and Julita Vassileva. P2U: A privacy policy specification language for secondary data sharing and usage. In *Security and Privacy Workshops (SPW), 2014 IEEE*, pages 18–22. IEEE, 2014.

[24] Håvard D Johansen, Eleanor Birrell, Robbert Van Renesse, Fred B. Schneider, Magnus Stenhaug, and Dag Johansen. Enforcing privacy policies with meta-code. In *Proceedings of the 6th Asia-Pacific Workshop on Systems*, 2015.

[25] Elisavet Kozyri and Fred B. Schneider. RIF: Reactive information flow labels. Technical report, Cornell University, Computing and Information Science. In preparation.

[26] Marc Langheinrich, Lorrie Cranor, and Massimo Marchiori. Appel: A P3P preference exchange language. *W3C Working Draft*, 2002.

[27] Scott Lederer, Jennifer Mankoff, and Anind K. Dey. Who wants to know what when? Privacy preference determinants in ubiquitous computing. In *CHI'03 Extended Abstracts on Human Factors in Computing Systems*, pages 724–725. ACM, 2003.

[28] Lawrence Lessig. The architecture of privacy. *Vanderbilt Journal of Entertainment Law & Practice*, 1:56–65, 1999.

[29] Jialiu Lin, Michael Benisch, Norman Sadeh, Jianwei Niu, Jason Hong, Banghui Lu, and Shaohui Guo. A comparative study of location-sharing privacy preferences in the United States and China. *Personal and Ubiquitous Computing*, 17(4):697–711, 2013.

[30] Aleecia M. McDonald and Lorrie Faith Cranor. The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society*, 4:543–568, 2008.

[31] Craig Mundie. Privacy pragmatism: Focus on data use, not data collection. *Foreign Aff.*, 93:28, 2014.

[32] Helen Nissenbaum. *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford University Press, 2009.

[33] Helen Nissenbaum. A contextual approach to privacy online. *Daedalus*, 140(4):32–48, 2011.

[34] Raúl Pardo, Christian Colombo, Gordon J. Pace, and Gerardo Schneider. An automata-based approach to evolving privacy policies for social networks. In *Proceedings of the 16th International Conference on Runtime Verification (RV 2016)*, volume 10012 of *Lecture Notes in Computer Science*, pages 285–301. Springer International Publishing, 2016.

[35] Jaehong Park and Ravi Sandhu. Towards usage control models: Beyond traditional access control. In *Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies*, SACMAT '02, pages 57–64, 2002.

[36] Jaehong Park and Ravi Sandhu. The UCONABC usage control model. *ACM Trans. Inf. Syst. Secur.*, 7(1):128–174, February 2004.

[37] Milan Petkovic, Davide Prandi, and Nicola Zannone. Purpose control: Did you process the data for the intended purpose? *Secure Data Management*, 6933:145–168, 2011.

[38] Aarathi Prasad, Jacob Sorber, Timothy Stablein, Denise Anthony, and David Kotz. Understanding sharing preferences and behavior for mHealth devices. In *Proceedings of the 2012 ACM Workshop on Privacy in the Electronic Society*, pages 117–128. ACM, 2012.

[39] Alexander Pretschner, Manuel Hilty, and David Basin. Distributed usage control. *Communications of the ACM*, 49(9):39–44, 2006.

[40] The Privacy Rights Markup Language. *Zero Knowledge Confidential*, 2001.

[41] Ramprasad Ravichandran, Michael Benisch, Patrick Gage Kelley, and Norman M. Sadeh. Capturing social networking privacy preferences. In *International Symposium on Privacy Enhancing Technologies Symposium*, pages 1–18. Springer, 2009.

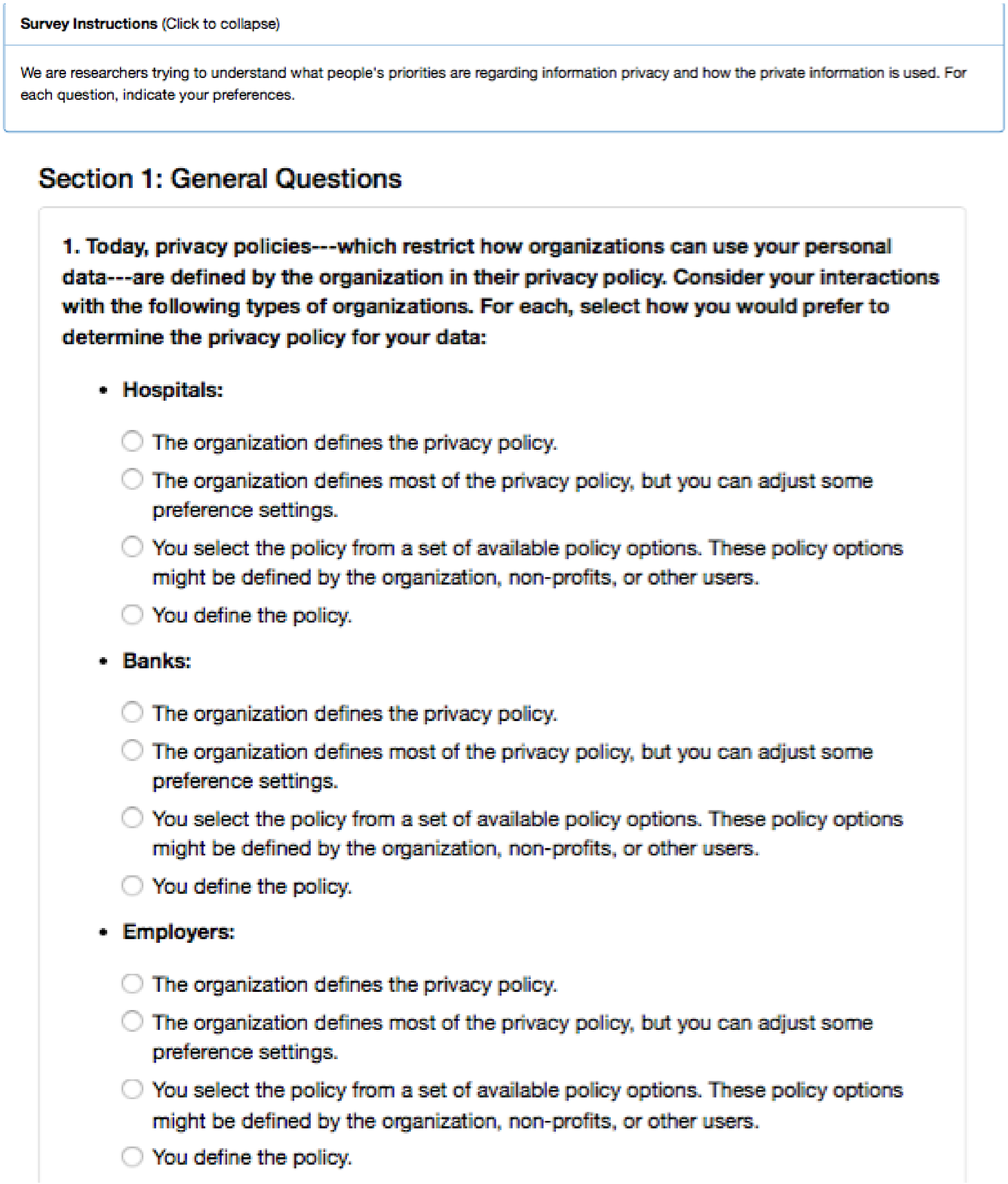
[42] Fred B. Schneider. Enforceable security policies. *ACM Transactions on Information and System Security (TISSEC)*, 3(1):30–50, 2000.

[43] Shayak Sen, Saikat Guha, Anupam Datta, Sriram K. Rajamani, Janice Tsai, and Jeannette M. Wing. Bootstrapping privacy compliance in big data systems. In *Proceedings of the 35th IEEE Symposium on Security and Privacy (Oakland)*, 2014.

[44] Daniel J. Solove. Privacy self-management and the consent paradox. *Harvard Law Review*, 126(7):1880–1903, 2013.

[45] Samuel D. Warren and Louis D. Brandeis. The right to privacy. *Harvard Law Review*, 4(5):193–220, December 1890.

A User Study



Survey Instructions (Click to collapse)

We are researchers trying to understand what people's priorities are regarding information privacy and how the private information is used. For each question, indicate your preferences.

Section 1: General Questions

1. Today, privacy policies---which restrict how organizations can use your personal data---are defined by the organization in their privacy policy. Consider your interactions with the following types of organizations. For each, select how you would prefer to determine the privacy policy for your data:

- **Hospitals:**

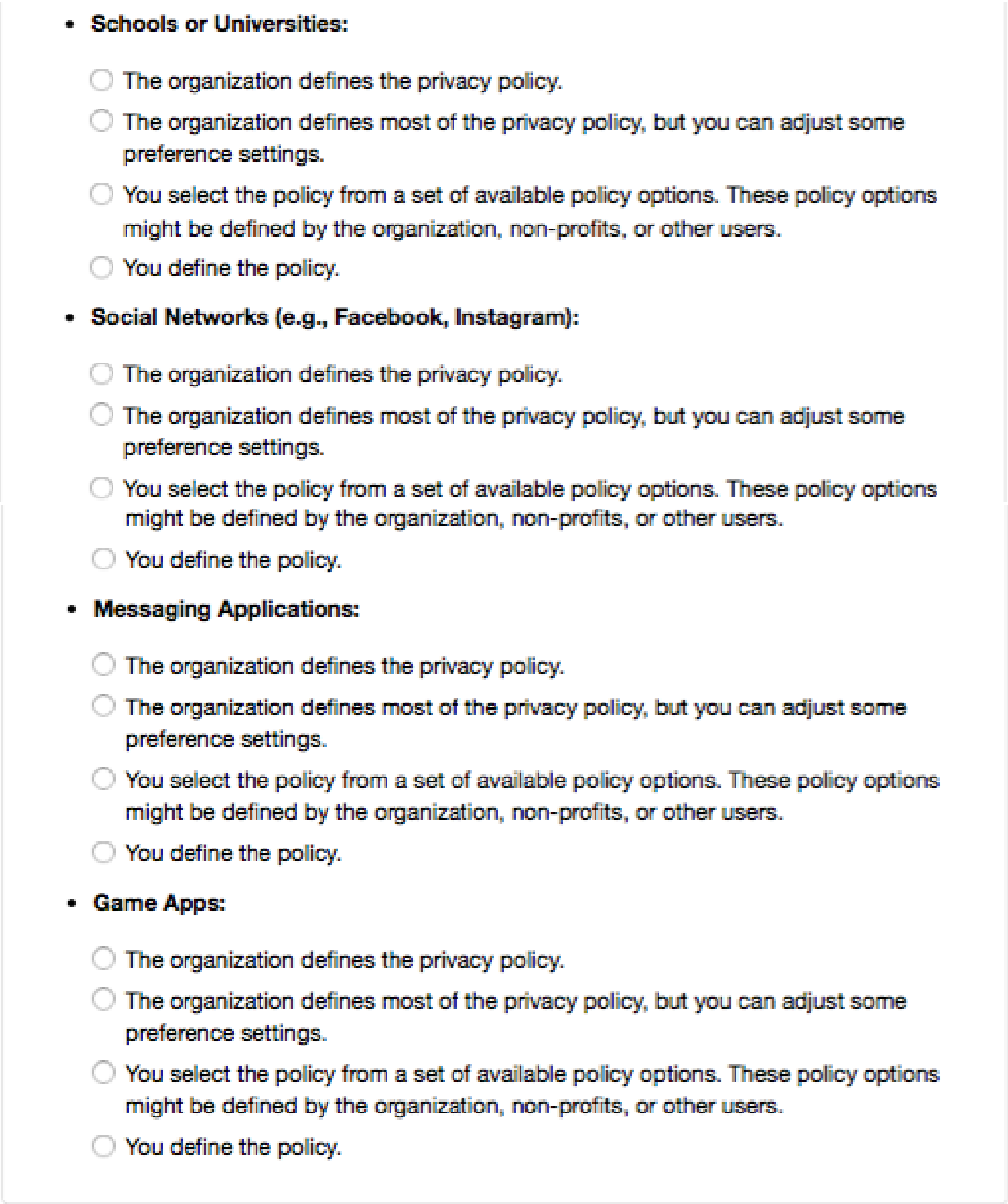
  ○ The organization defines the privacy policy.
  ○ The organization defines most of the privacy policy, but you can adjust some preference settings.
  ○ You select the policy from a set of available policy options. These policy options might be defined by the organization, non-profits, or other users.
  ○ You define the policy.

- **Banks:**

  ○ The organization defines the privacy policy.
  ○ The organization defines most of the privacy policy, but you can adjust some preference settings.
  ○ You select the policy from a set of available policy options. These policy options might be defined by the organization, non-profits, or other users.
  ○ You define the policy.

- **Employers:**

  ○ The organization defines the privacy policy.
  ○ The organization defines most of the privacy policy, but you can adjust some preference settings.
  ○ You select the policy from a set of available policy options. These policy options might be defined by the organization, non-profits, or other users.
  ○ You define the policy.



- **Schools or Universities:**

  ○ The organization defines the privacy policy.
  ○ The organization defines most of the privacy policy, but you can adjust some preference settings.
  ○ You select the policy from a set of available policy options. These policy options might be defined by the organization, non-profits, or other users.
  ○ You define the policy.

- **Social Networks (e.g., Facebook, Instagram):**

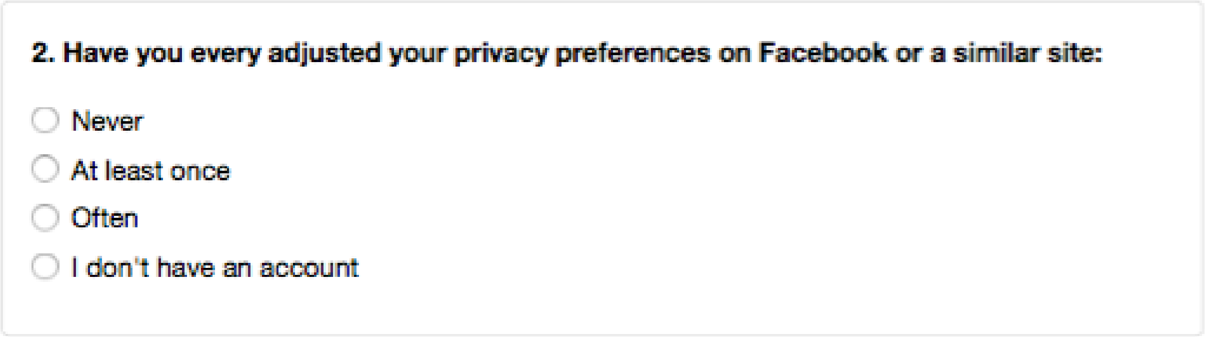
  ○ The organization defines the privacy policy.
  ○ The organization defines most of the privacy policy, but you can adjust some preference settings.
  ○ You select the policy from a set of available policy options. These policy options might be defined by the organization, non-profits, or other users.
  ○ You define the policy.

- **Messaging Applications:**

  ○ The organization defines the privacy policy.
  ○ The organization defines most of the privacy policy, but you can adjust some preference settings.
  ○ You select the policy from a set of available policy options. These policy options might be defined by the organization, non-profits, or other users.
  ○ You define the policy.

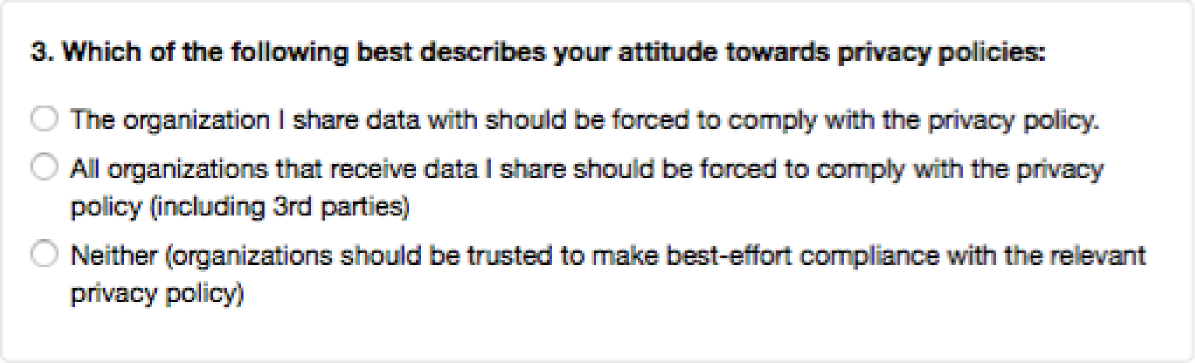
- **Game Apps:**

  ○ The organization defines the privacy policy.
  ○ The organization defines most of the privacy policy, but you can adjust some preference settings.
  ○ You select the policy from a set of available policy options. These policy options might be defined by the organization, non-profits, or other users.
  ○ You define the policy.



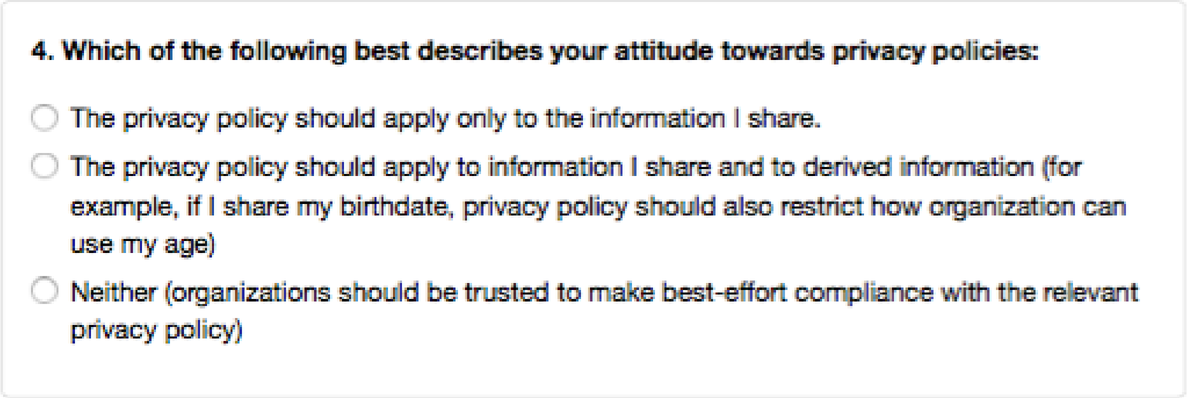
2. Have you every adjusted your privacy preferences on Facebook or a similar site:

○ Never
○ At least once
○ Often
○ I don't have an account



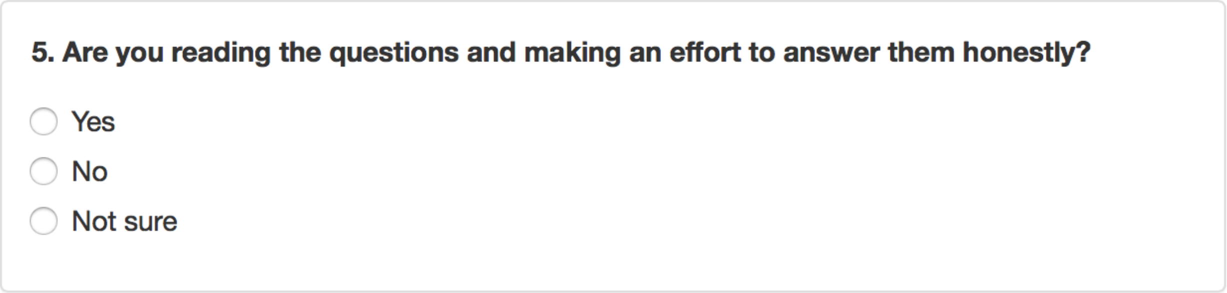
3. Which of the following best describes your attitude towards privacy policies:

○ The organization I share data with should be forced to comply with the privacy policy.
○ All organizations that receive data I share should be forced to comply with the privacy policy (including 3rd parties)
○ Neither (organizations should be trusted to make best-effort compliance with the relevant privacy policy)



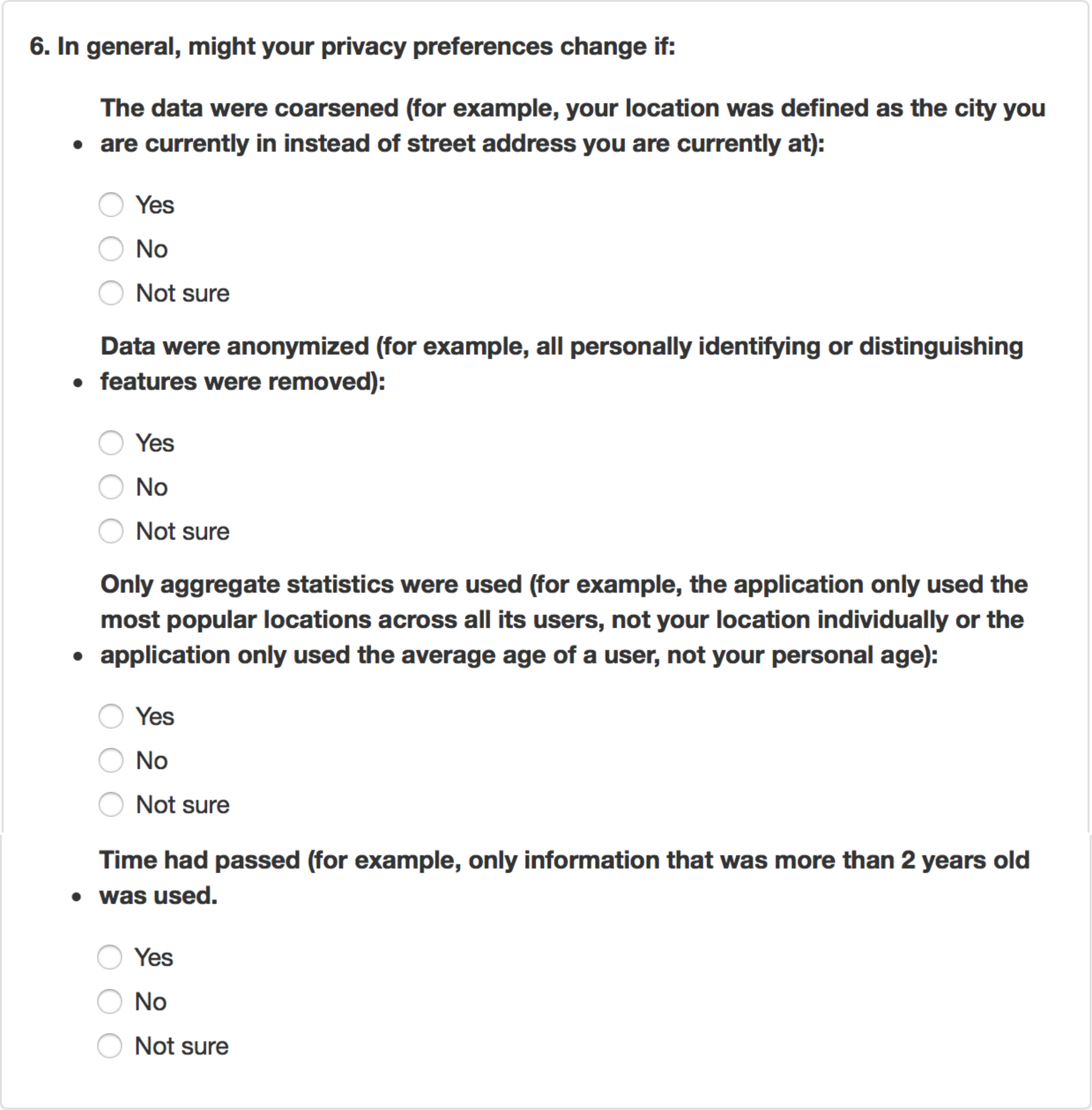
4. Which of the following best describes your attitude towards privacy policies:

○ The privacy policy should apply only to the information I share.
○ The privacy policy should apply to information I share and to derived information (for example, if I share my birthdate, privacy policy should also restrict how organization can use my age)
○ Neither (organizations should be trusted to make best-effort compliance with the relevant privacy policy)



5. Are you reading the questions and making an effort to answer them honestly?

○ Yes
○ No
○ Not sure



6. In general, might your privacy preferences change if:

- The data were coarsened (for example, your location was defined as the city you are currently in instead of street address you are currently at):

  ○ Yes
  ○ No
  ○ Not sure

- Data were anonymized (for example, all personally identifying or distinguishing features were removed):

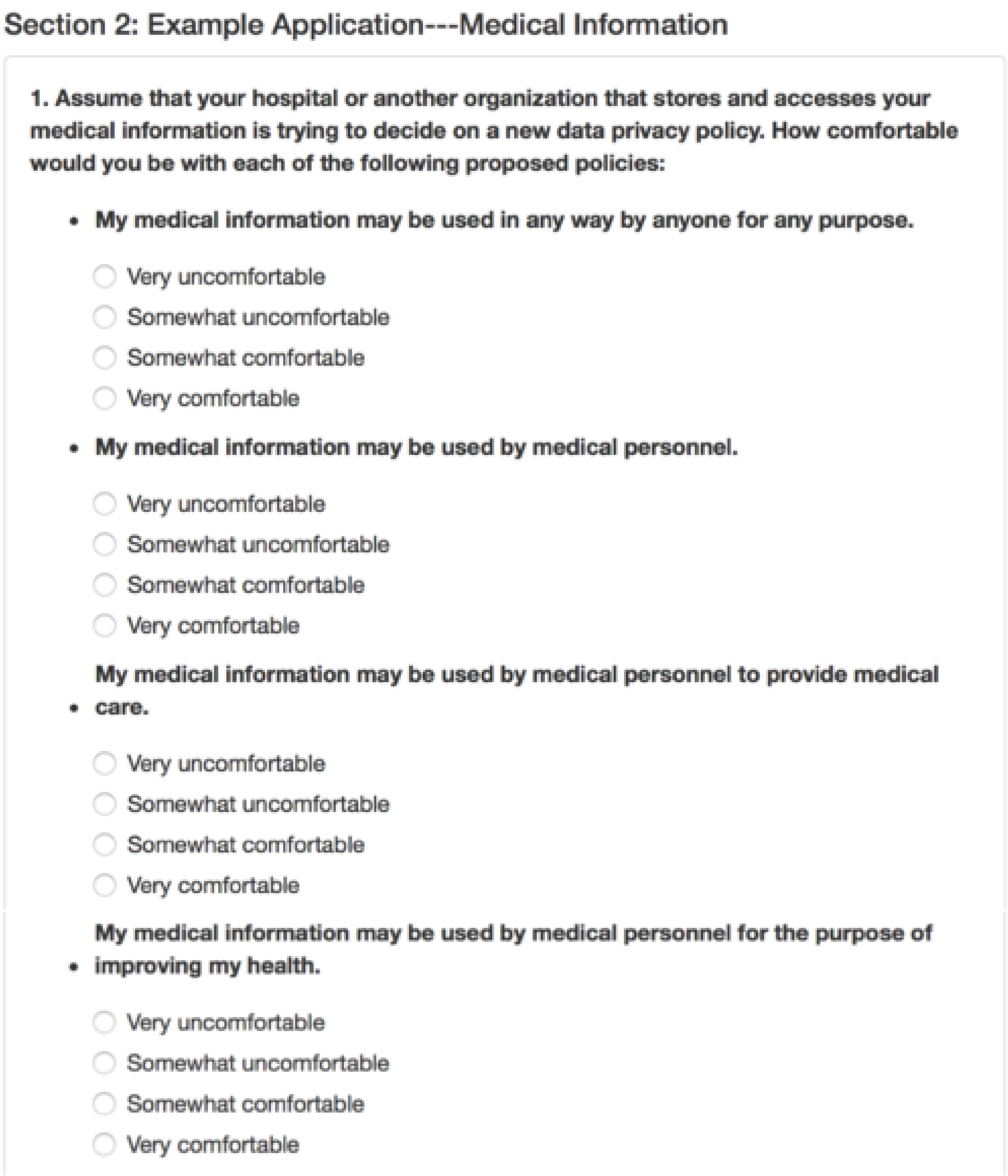
  ○ Yes
  ○ No
  ○ Not sure

- Only aggregate statistics were used (for example, the application only used the most popular locations across all its users, not your location individually or the application only used the average age of a user, not your personal age):

  ○ Yes
  ○ No
  ○ Not sure

- Time had passed (for example, only information that was more than 2 years old was used.

  ○ Yes
  ○ No
  ○ Not sure



Section 2: Example Application---Medical Information

1. Assume that your hospital or another organization that stores and accesses your medical information is trying to decide on a new data privacy policy. How comfortable would you be with each of the following proposed policies:

- **My medical information may be used in any way by anyone for any purpose.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

- **My medical information may be used by medical personnel.**

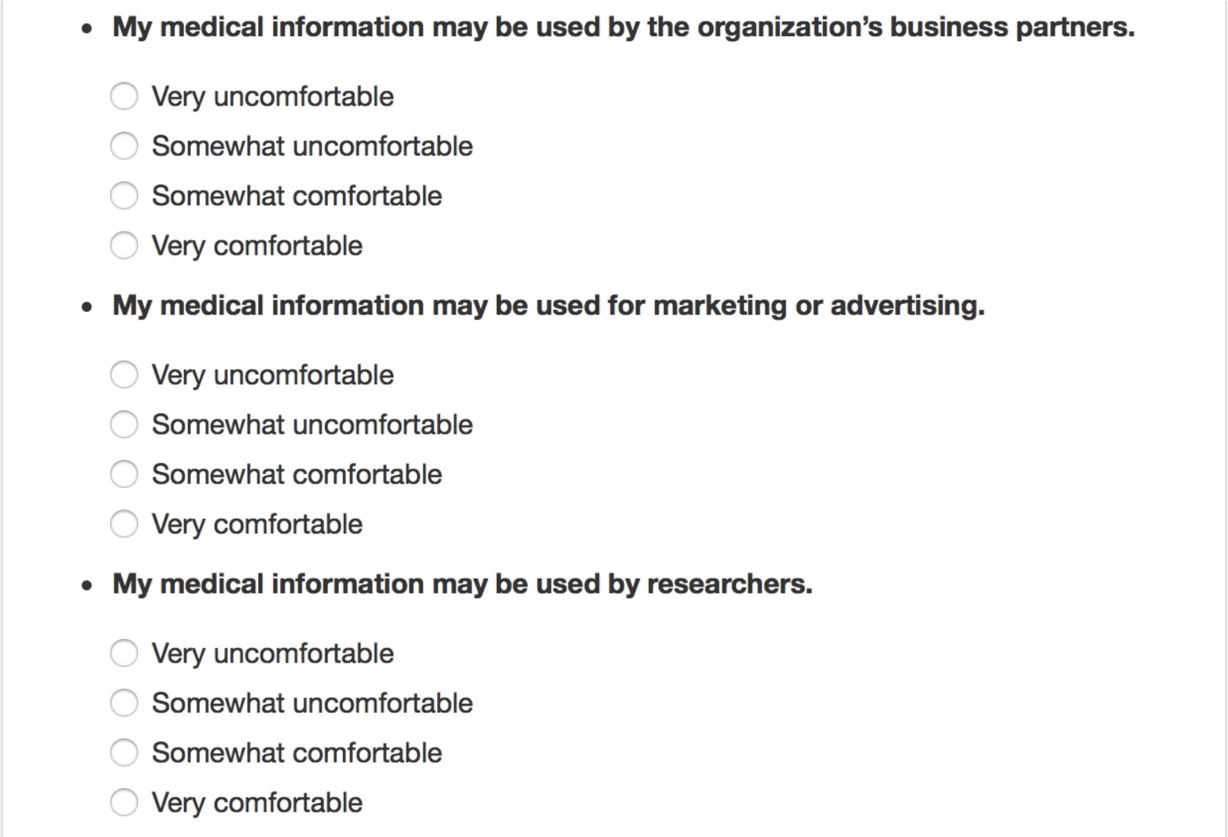
  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

- **My medical information may be used by medical personnel to provide medical care.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

- **My medical information may be used by medical personnel for the purpose of improving my health.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable



- **My medical information may be used by the organization's business partners.**

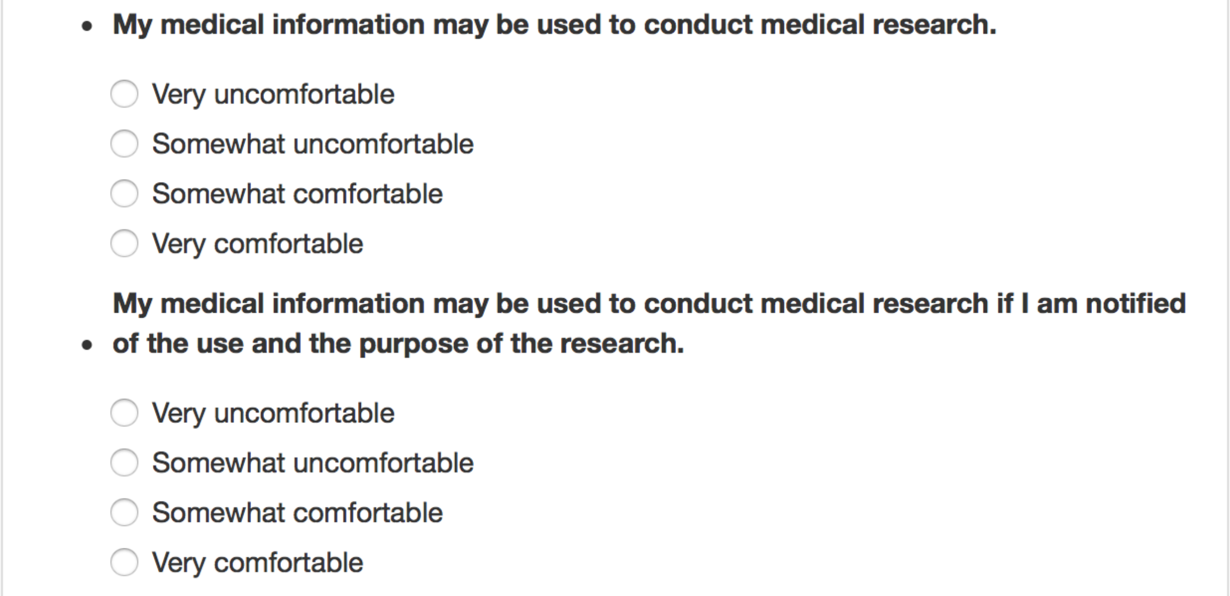
  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

- **My medical information may be used for marketing or advertising.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

- **My medical information may be used by researchers.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

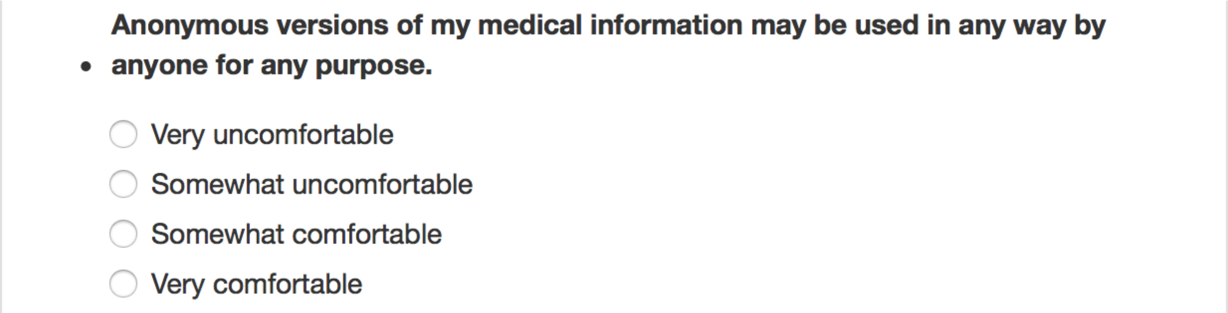


- **My medical information may be used to conduct medical research.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

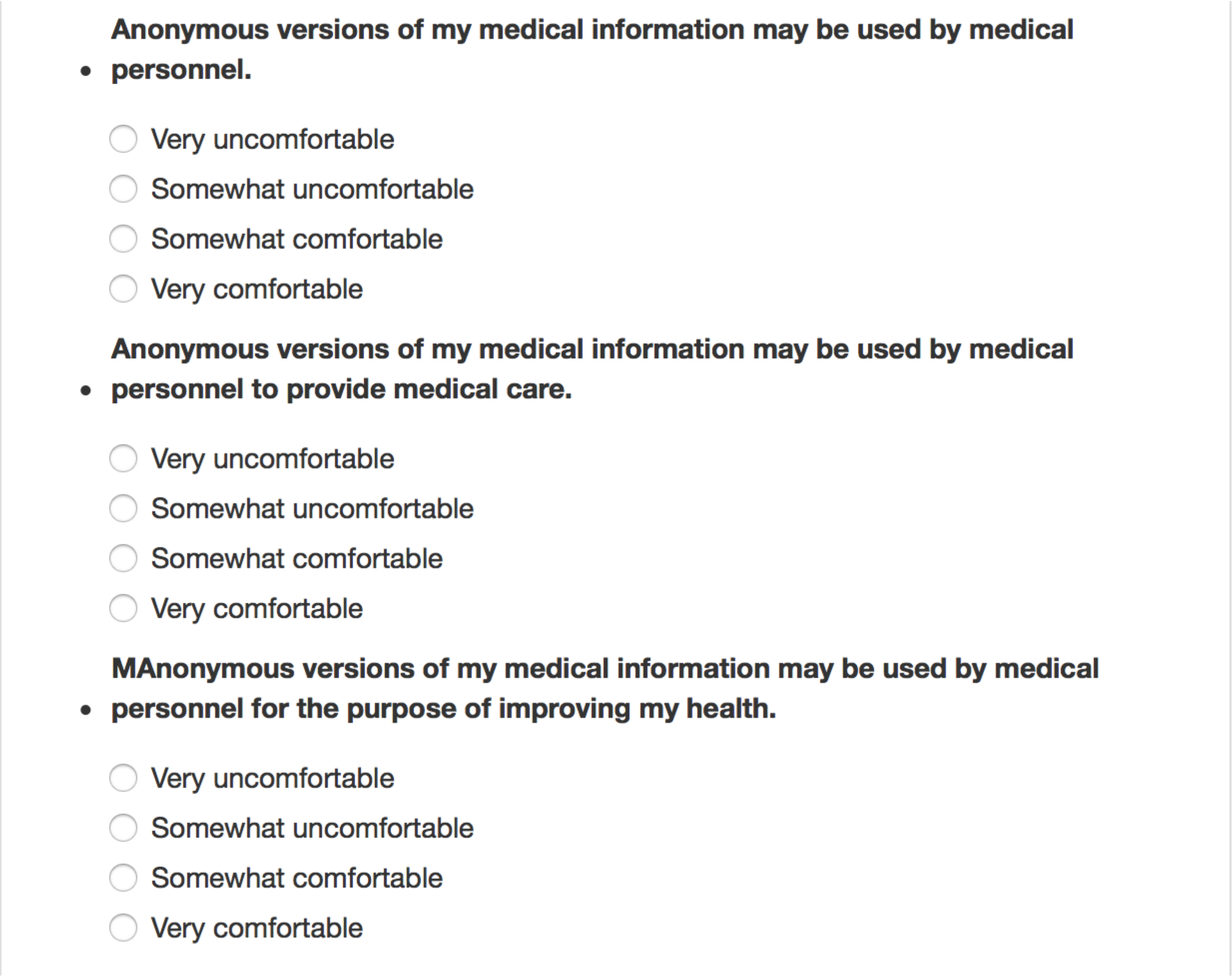
- **My medical information may be used to conduct medical research if I am notified of the use and the purpose of the research.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable



- **Anonymous versions of my medical information may be used in any way by anyone for any purpose.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable



- **Anonymous versions of my medical information may be used by medical personnel.**

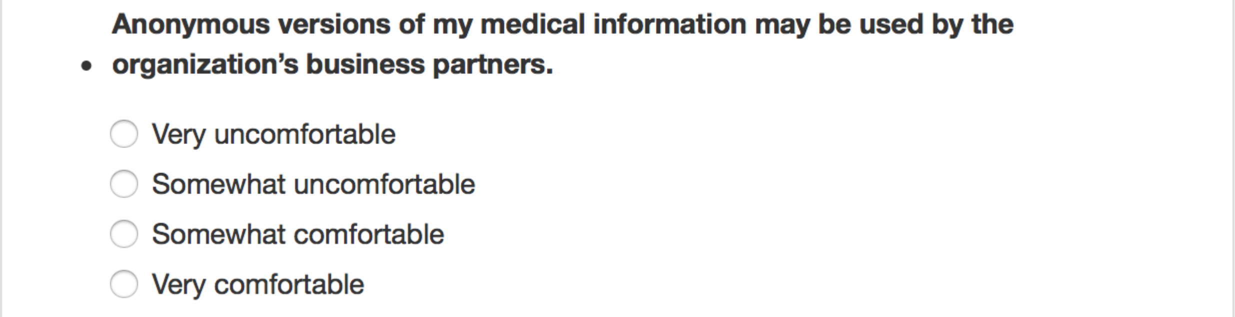
  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

- **Anonymous versions of my medical information may be used by medical personnel to provide medical care.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

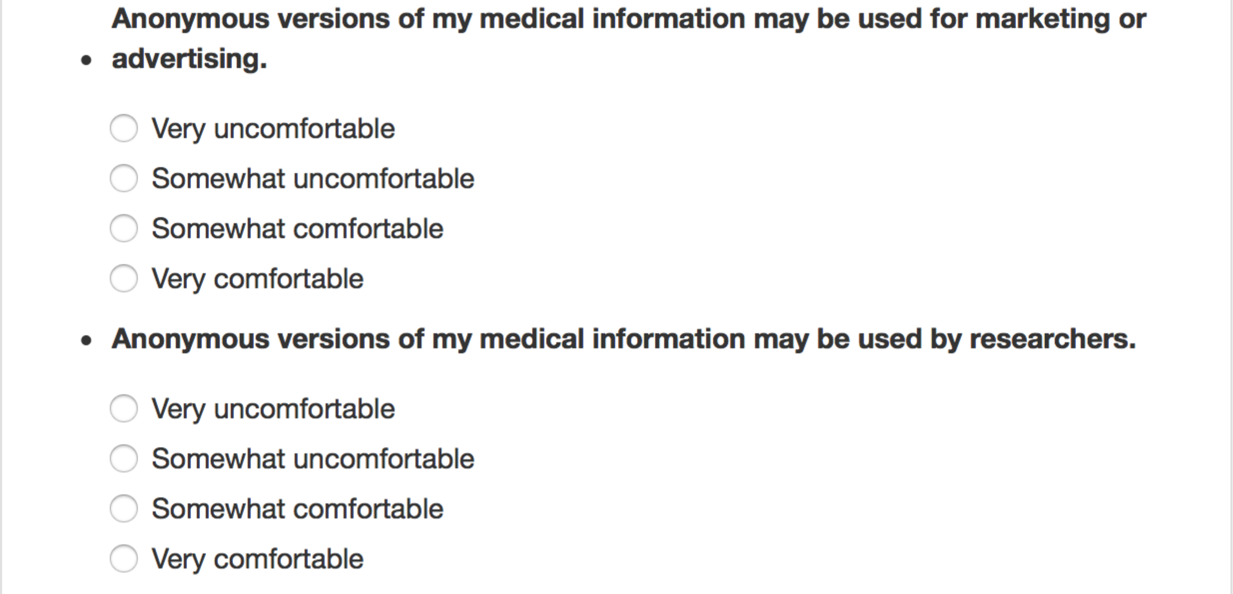
- **MAnonymous versions of my medical information may be used by medical personnel for the purpose of improving my health.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable



- **Anonymous versions of my medical information may be used by the organization’s business partners.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

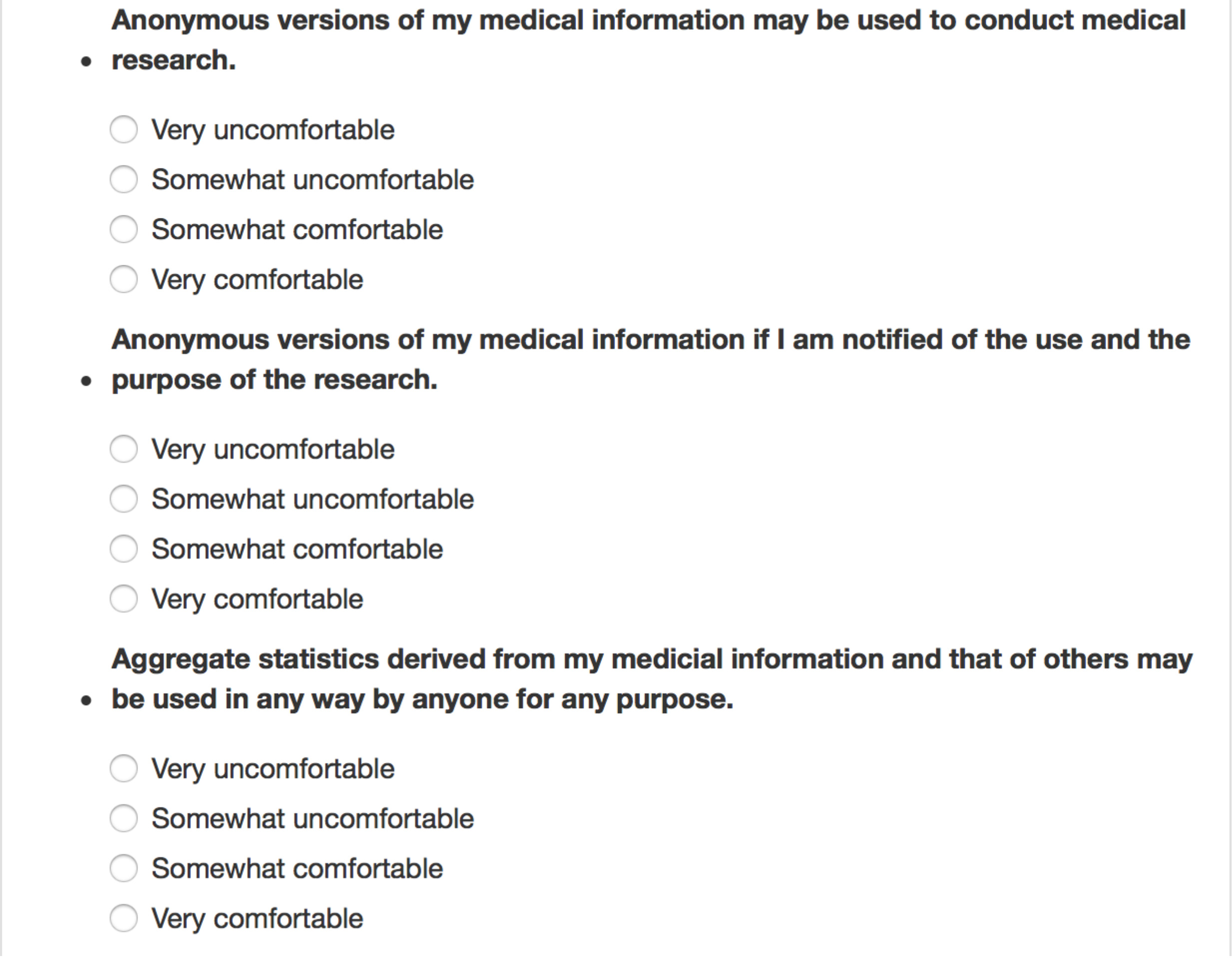


- **Anonymous versions of my medical information may be used for marketing or advertising.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

- **Anonymous versions of my medical information may be used by researchers.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable



- **Anonymous versions of my medical information may be used to conduct medical research.**

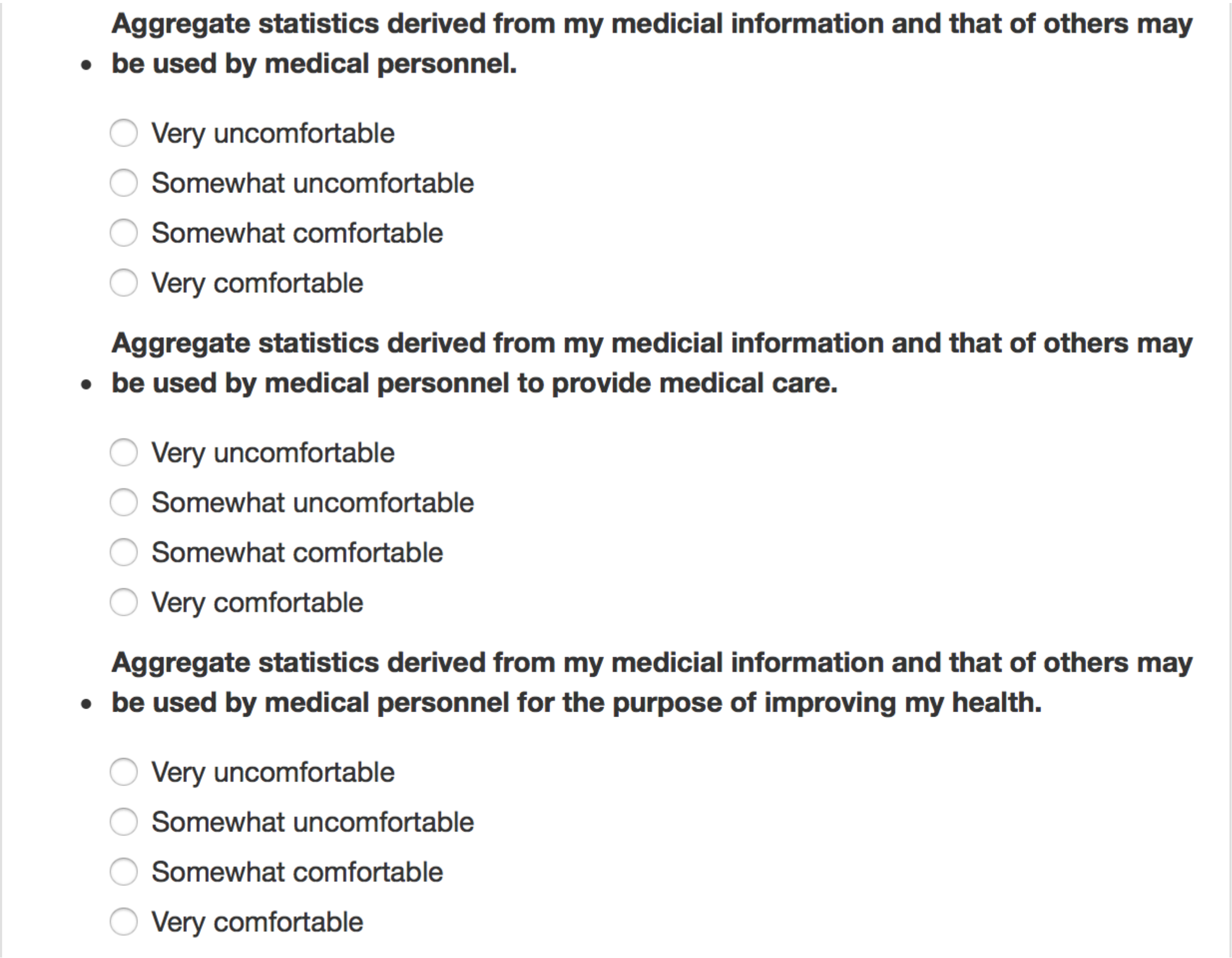
  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

- **Anonymous versions of my medical information if I am notified of the use and the purpose of the research.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

- **Aggregate statistics derived from my medicial information and that of others may be used in any way by anyone for any purpose.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable



- **Aggregate statistics derived from my medicial information and that of others may be used by medical personnel.**

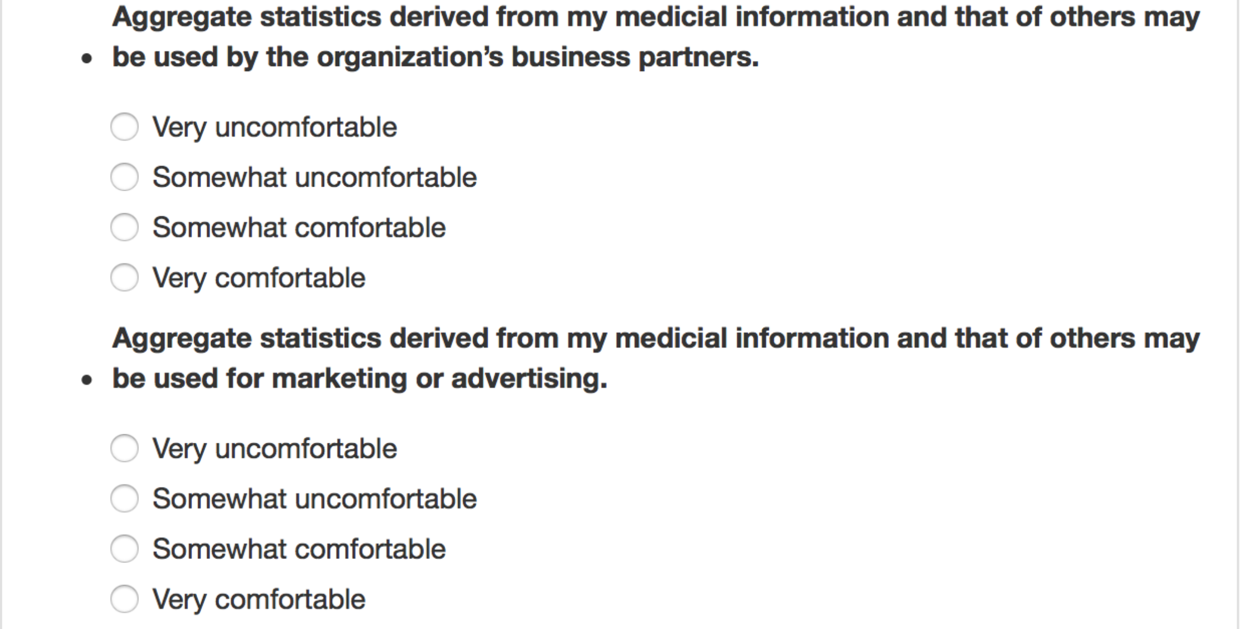
  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

- **Aggregate statistics derived from my medicial information and that of others may be used by medical personnel to provide medical care.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

- **Aggregate statistics derived from my medicial information and that of others may be used by medical personnel for the purpose of improving my health.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

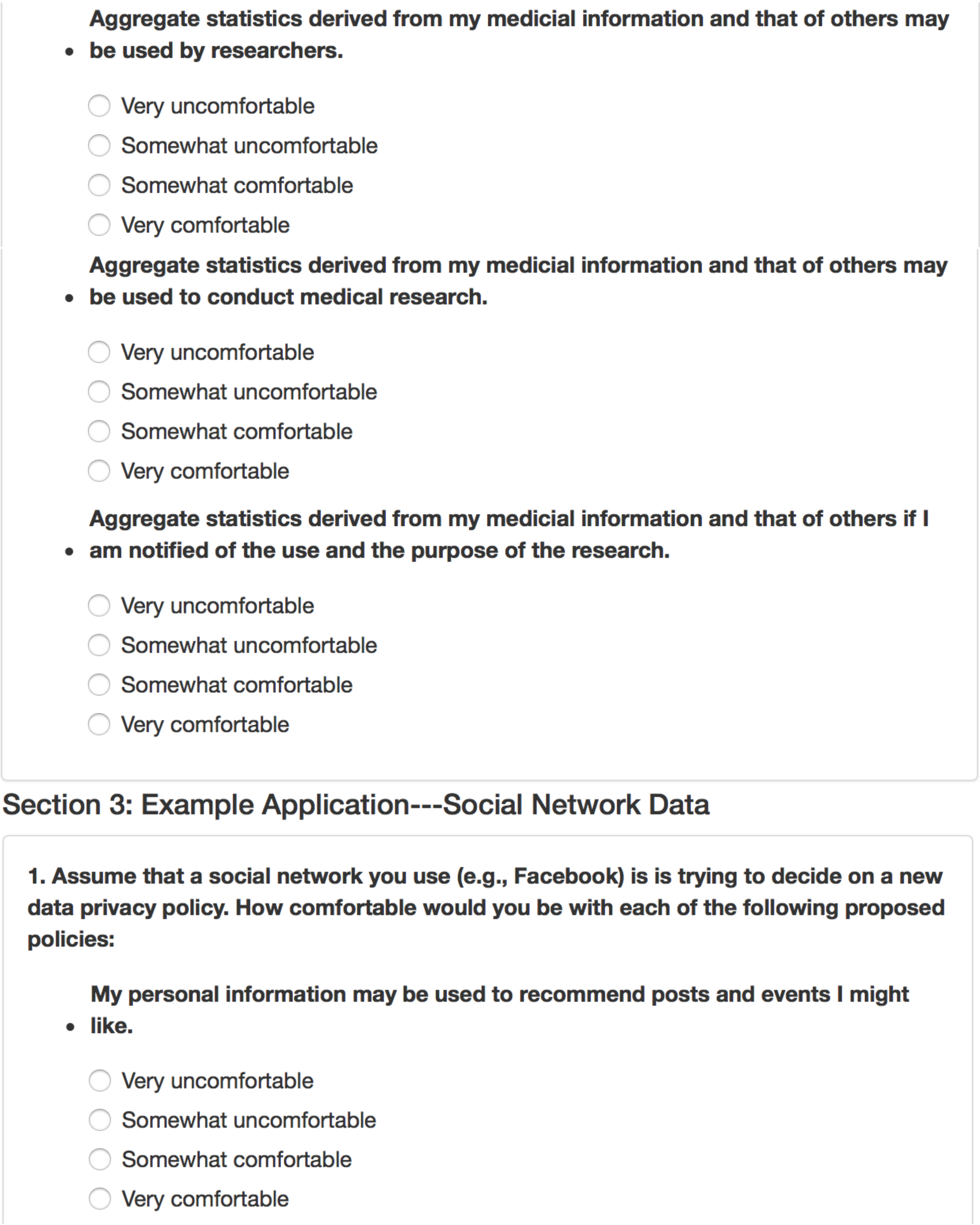


- **Aggregate statistics derived from my medicial information and that of others may be used by the organization’s business partners.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

- **Aggregate statistics derived from my medicial information and that of others may be used for marketing or advertising.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable



- **Aggregate statistics derived from my medicial information and that of others may be used by researchers.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

- **Aggregate statistics derived from my medicial information and that of others may be used to conduct medical research.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

- **Aggregate statistics derived from my medicial information and that of others if I am notified of the use and the purpose of the research.**

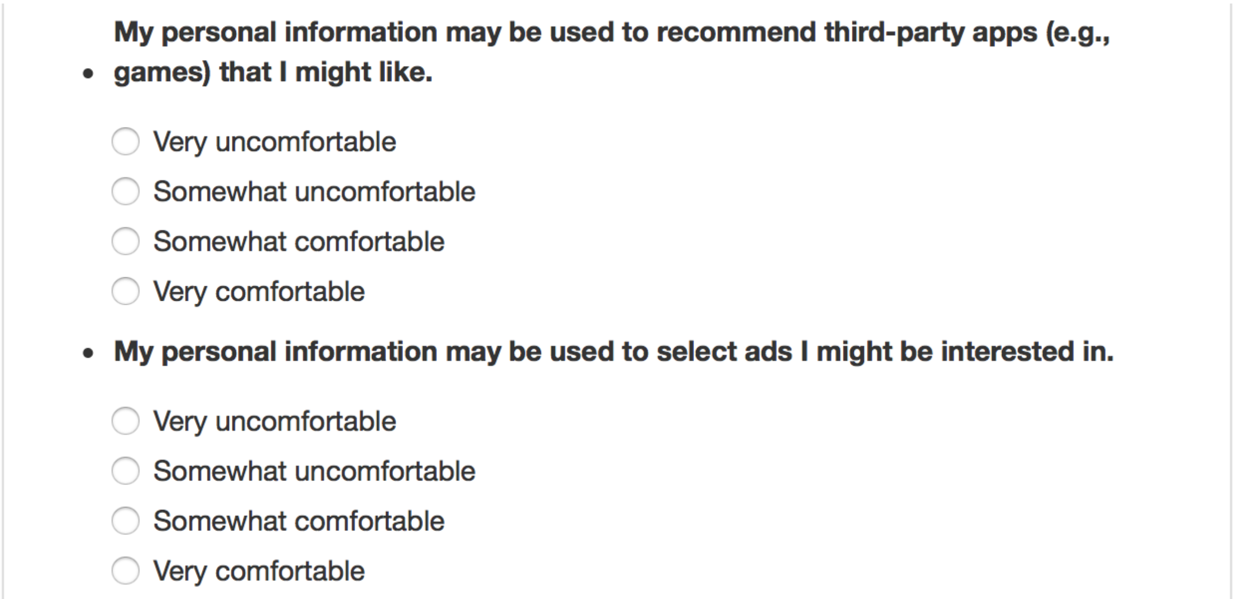
  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

Section 3: Example Application---Social Network Data

1. Assume that a social network you use (e.g., Facebook) is is trying to decide on a new data privacy policy. How comfortable would you be with each of the following proposed policies:

- **My personal information may be used to recommend posts and events I might like.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

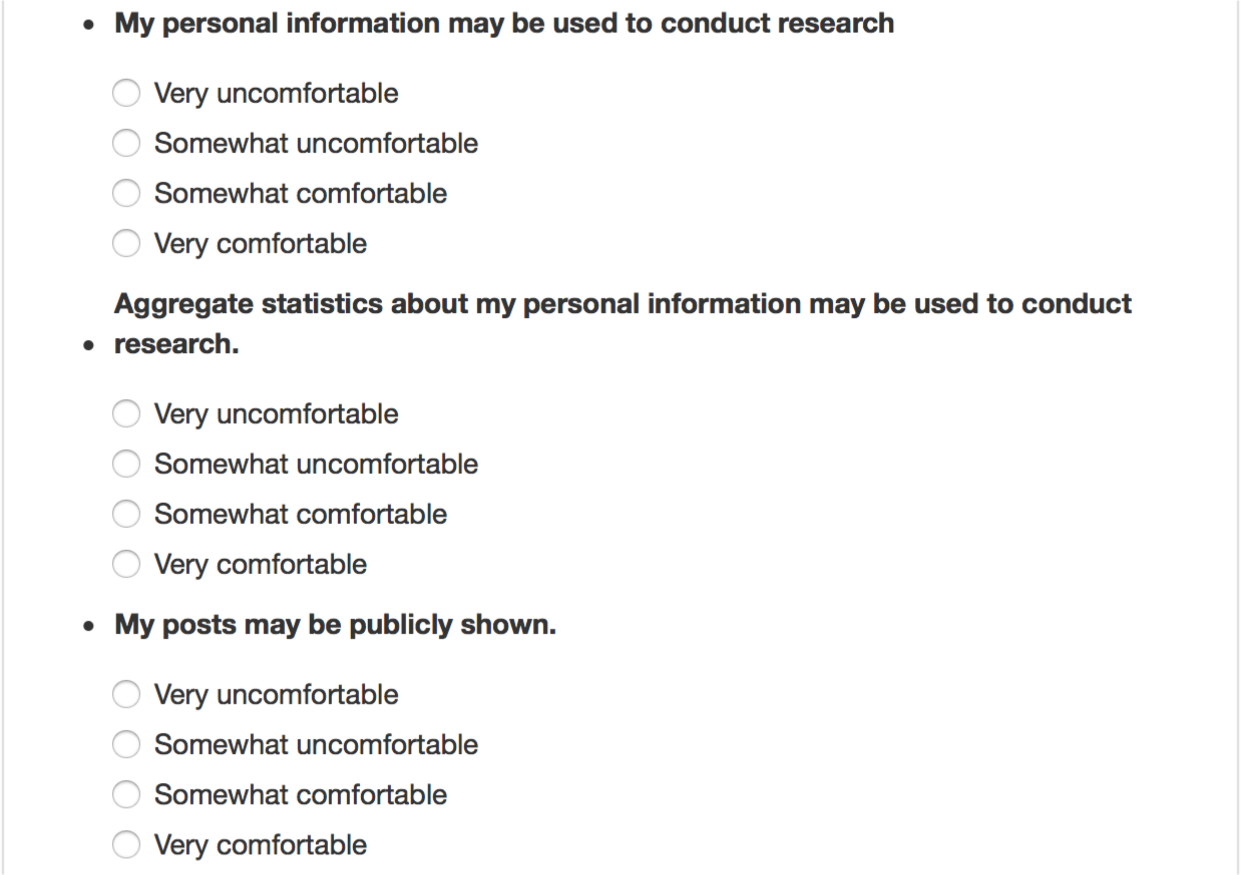


- **My personal information may be used to recommend third-party apps (e.g., games) that I might like.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

- **My personal information may be used to select ads I might be interested in.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable



- **My personal information may be used to conduct research**

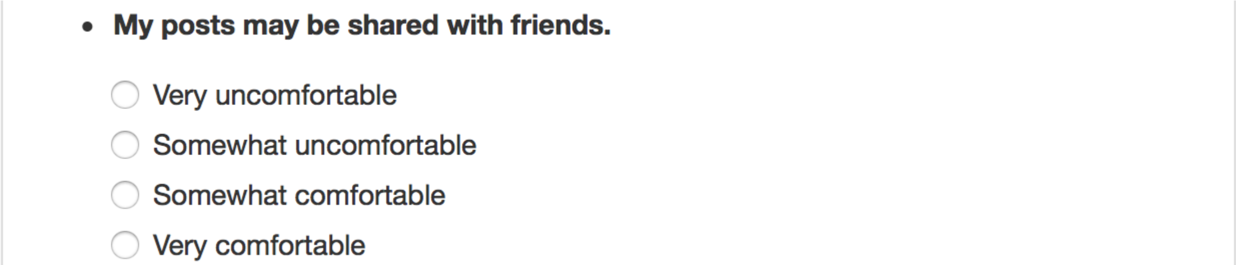
  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

- **Aggregate statistics about my personal information may be used to conduct research.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

- **My posts may be publicly shown.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable



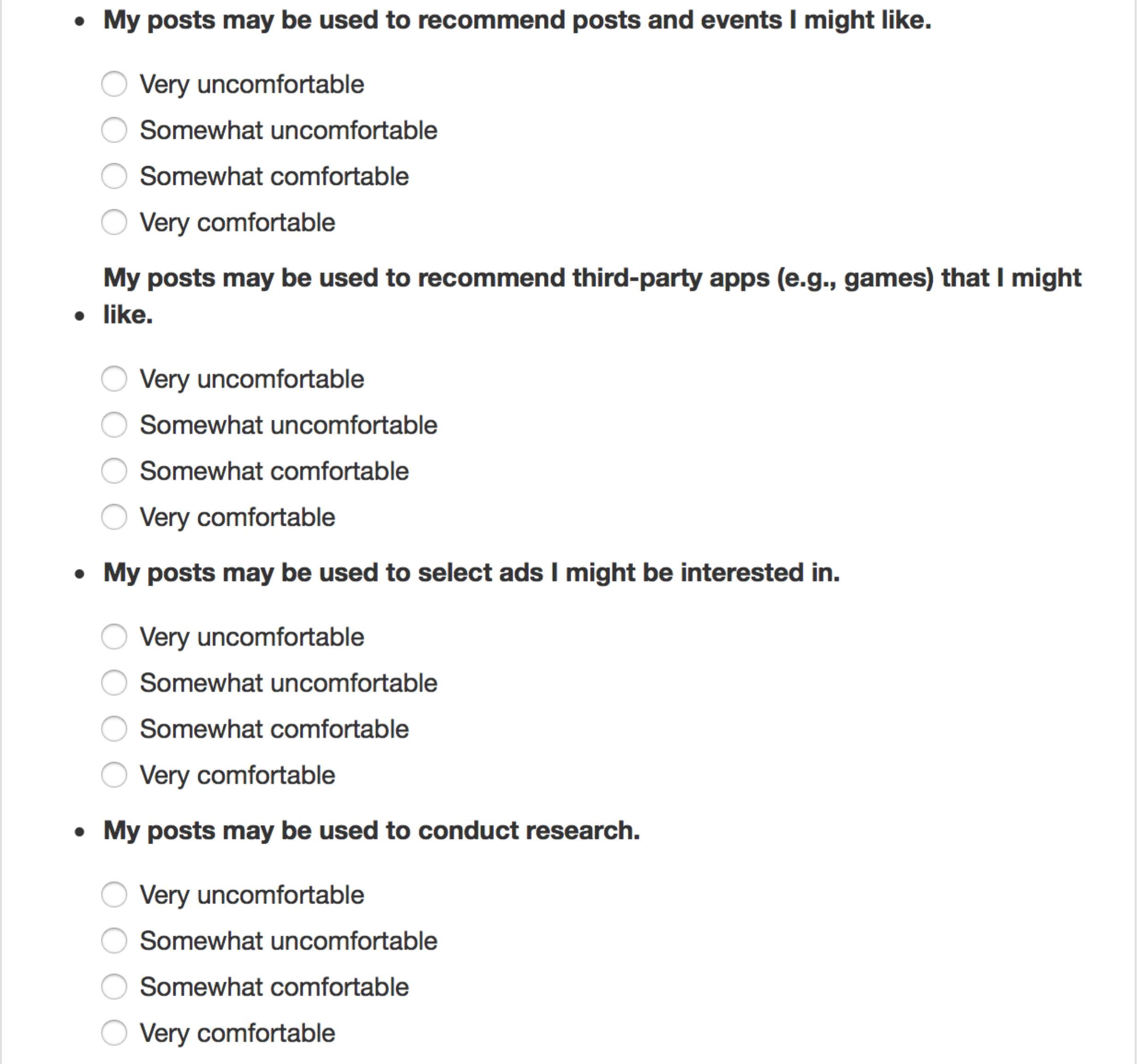
- **My posts may be shared with friends.**

  ○ Very uncomfortable

  ○ Somewhat uncomfortable

  ○ Somewhat comfortable

  ○ Very comfortable



- **My posts may be used to recommend posts and events I might like.**

  ○ Very uncomfortable

  ○ Somewhat uncomfortable

  ○ Somewhat comfortable

  ○ Very comfortable

- **My posts may be used to recommend third-party apps (e.g., games) that I might like.**

  ○ Very uncomfortable

  ○ Somewhat uncomfortable

  ○ Somewhat comfortable

  ○ Very comfortable

- **My posts may be used to select ads I might be interested in.**

  ○ Very uncomfortable

  ○ Somewhat uncomfortable

  ○ Somewhat comfortable

  ○ Very comfortable

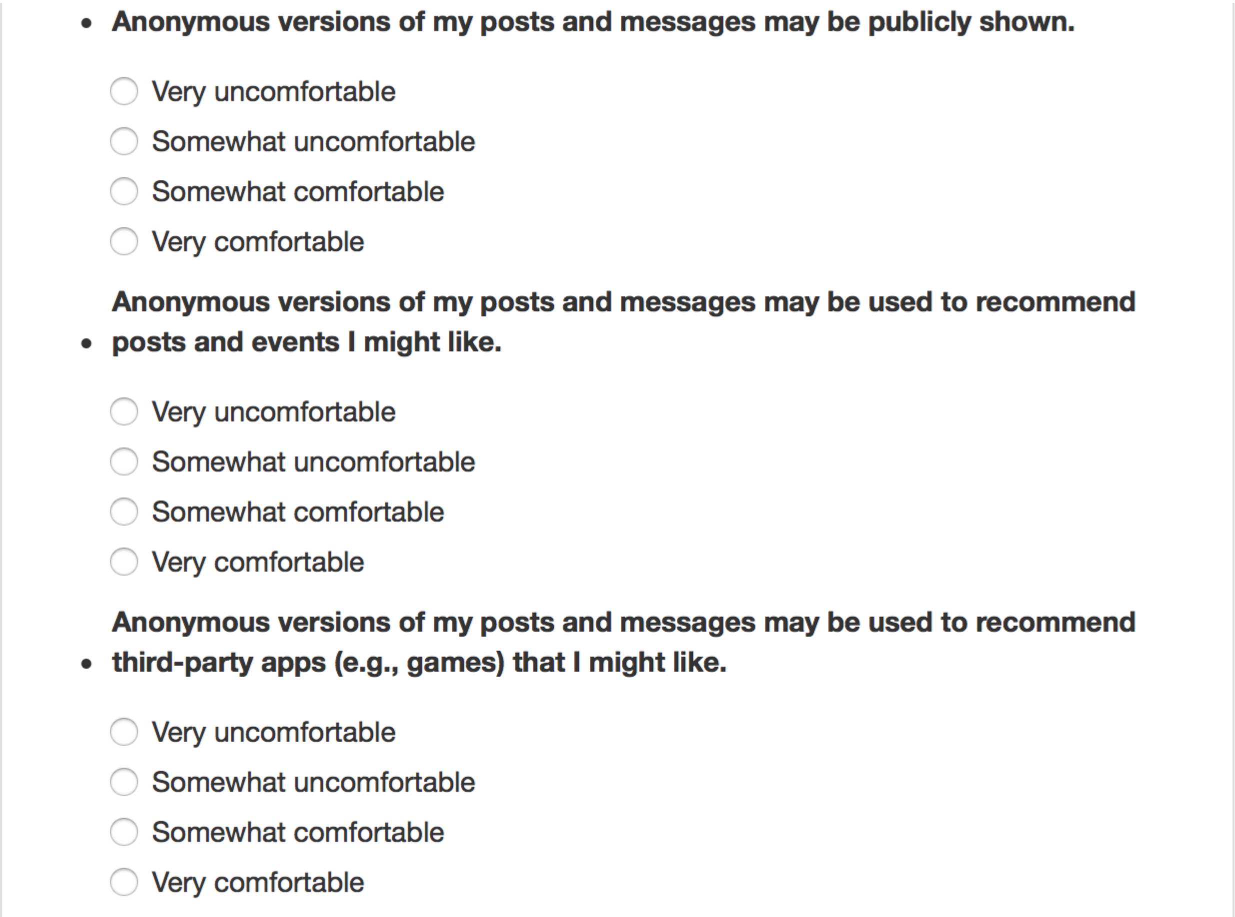
- **My posts may be used to conduct research.**

  ○ Very uncomfortable

  ○ Somewhat uncomfortable

  ○ Somewhat comfortable

  ○ Very comfortable



- **Anonymous versions of my posts and messages may be publicly shown.**

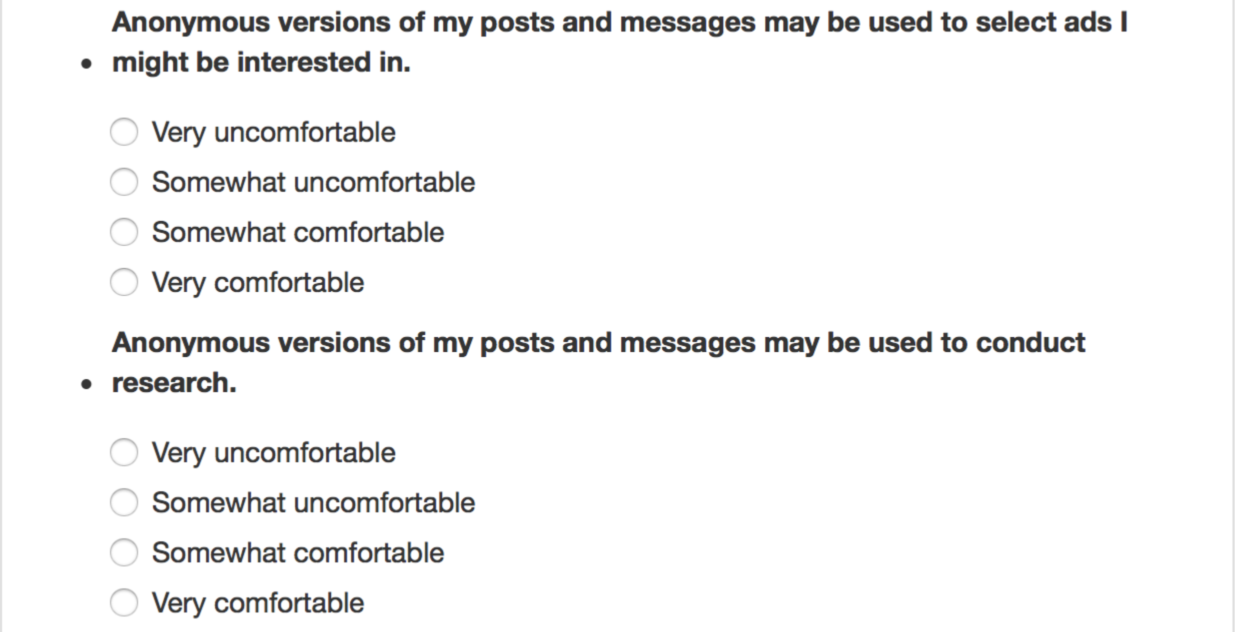
  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

- **Anonymous versions of my posts and messages may be used to recommend posts and events I might like.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

- **Anonymous versions of my posts and messages may be used to recommend third-party apps (e.g., games) that I might like.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

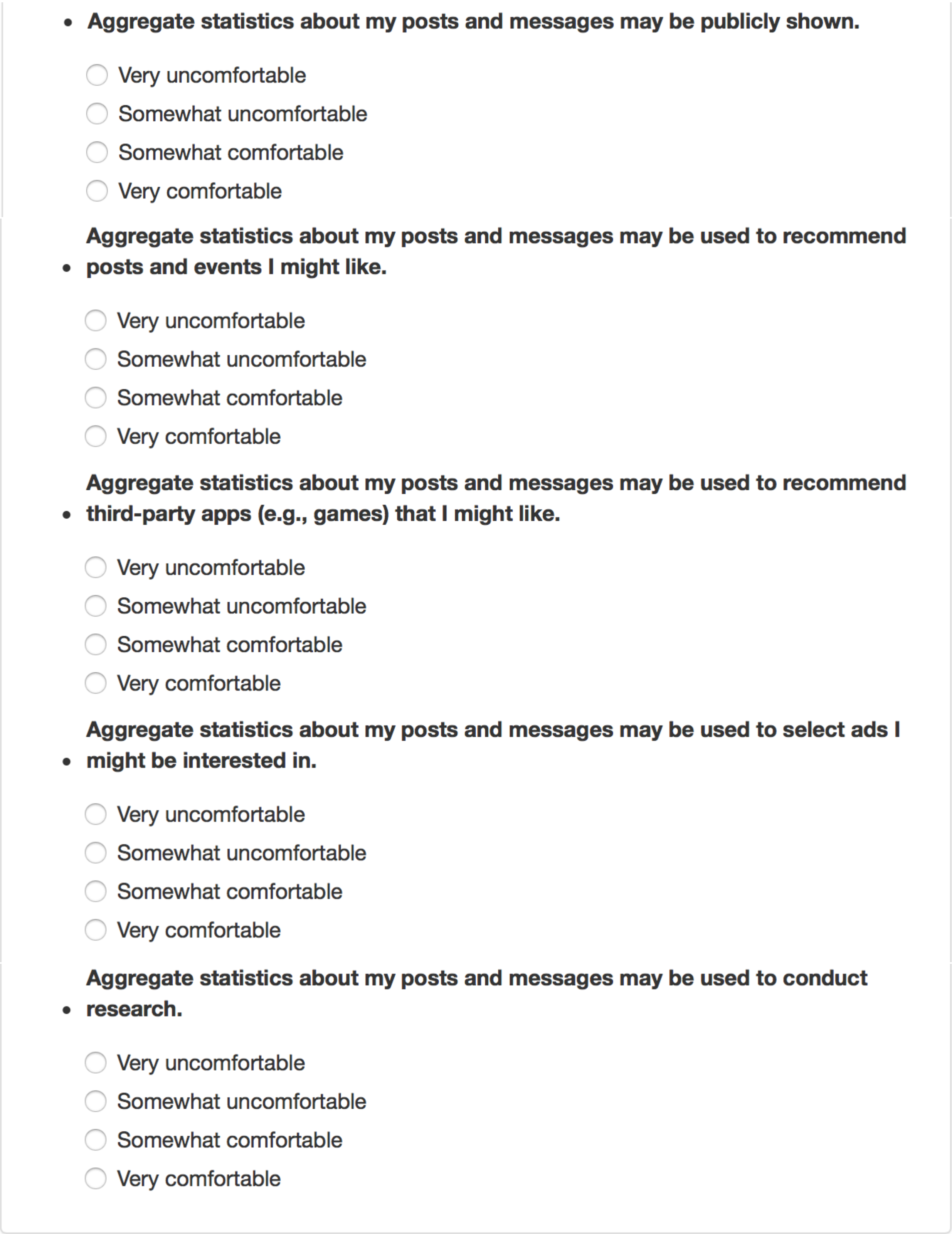


- **Anonymous versions of my posts and messages may be used to select ads I might be interested in.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

- **Anonymous versions of my posts and messages may be used to conduct research.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable



- **Aggregate statistics about my posts and messages may be publicly shown.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

- **Aggregate statistics about my posts and messages may be used to recommend posts and events I might like.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

- **Aggregate statistics about my posts and messages may be used to recommend third-party apps (e.g., games) that I might like.**

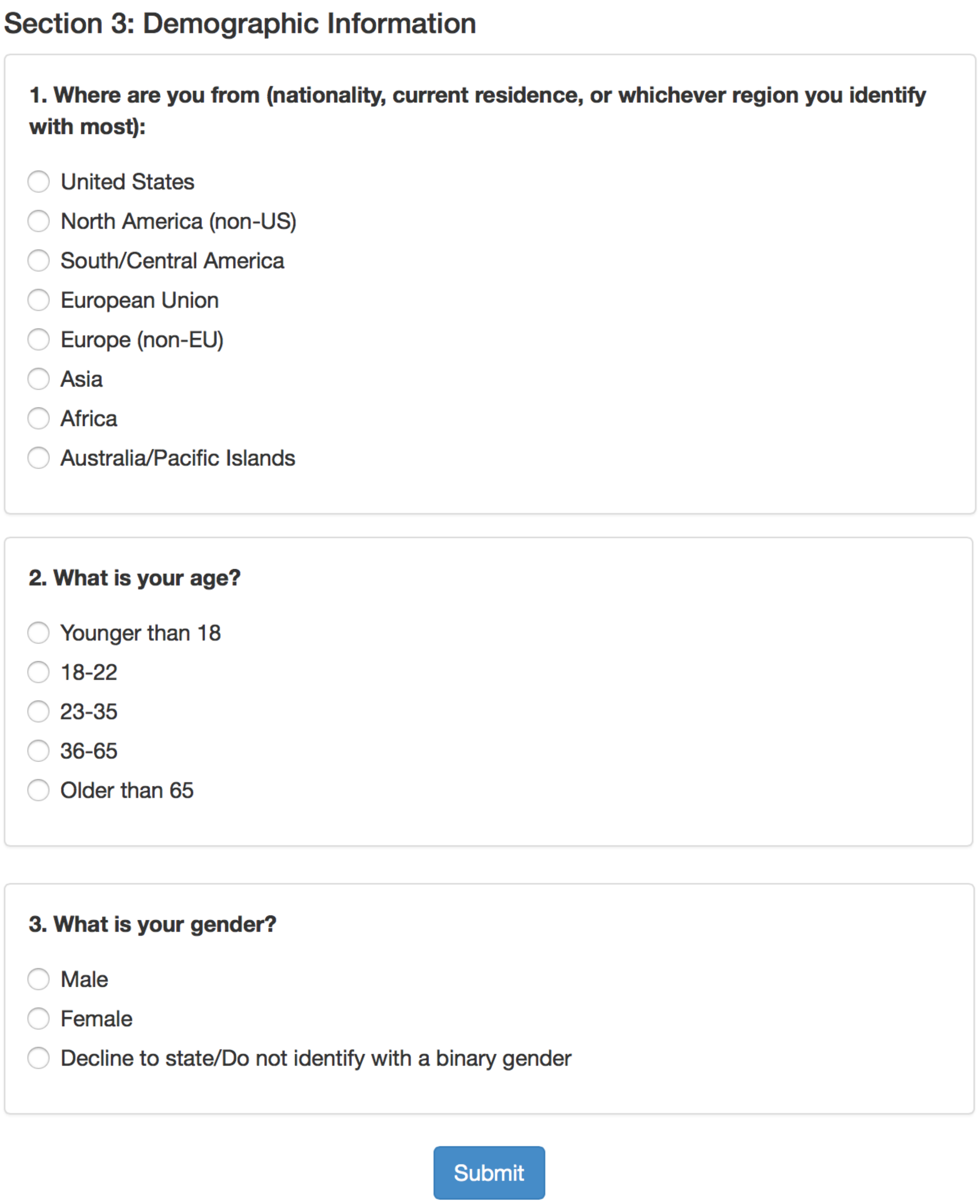
  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

- **Aggregate statistics about my posts and messages may be used to select ads I might be interested in.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable

- **Aggregate statistics about my posts and messages may be used to conduct research.**

  ○ Very uncomfortable
  ○ Somewhat uncomfortable
  ○ Somewhat comfortable
  ○ Very comfortable



Section 3: Demographic Information

1. Where are you from (nationality, current residence, or whichever region you identify with most):

○ United States
○ North America (non-US)
○ South/Central America
○ European Union
○ Europe (non-EU)
○ Asia
○ Africa
○ Australia/Pacific Islands

2. What is your age?

○ Younger than 18
○ 18-22
○ 23-35
○ 36-65
○ Older than 65

3. What is your gender?

○ Male
○ Female
○ Decline to state/Do not identify with a binary gender

B Encoding HIPAA as Data-use Tuples

Provision	Object	Invoker	Action	Purpose	Condition
§164.502(a)(1)(i)	protected health information	covered entity	disclose to individual		
(2)(ii)	protected health information	covered entity	disclose		when required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entitys compliance with this subpart.
(d)(1)	protected health information	covered entity	use	to create information that is not individually identifiable health information	
	protected health information	covered entity	disclose to a business associate	to create information that is not individually identifiable health information	
(2)	de-identified information				until reidentified
(e)(1)(i)	protected health information	covered entity	discloseto a business associate		if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information.

Provision	Object	Invoker	Action	Purpose	Condition
(3)(ii)(A)	record of disclosure of protected health information about an unemancipated minor	covered entity	disclose or provide access to a parent, guardian, or other person acting in loco parentis		if, and to the extent, permitted or required by an applicable provision of State or other law, including applicable case law
§164.506(c)(1)	protected health information (except psychotherapy notes)	covered entity	use or disclose	for its own treatment, payment, or health care operations.	
(2)	protected health information (except psychotherapy notes)	covered entity	disclose	for treatment activities of a health care provider	
(3)	protected health information (except psychotherapy notes)	covered entity	disclose to another covered entity or a health care provider	for the payment activities of the entity that receives the information.	
(4)(i)	protected health information (except psychotherapy notes)	covered entity that has or had a relationship with the individual who is the subject	disclose to another covered entity that has or had a relationship with the individual who is the subject	for a purpose listed in paragraph (1) or (2) of the definition of health care operations (other than marketing)	
(ii)	protected health information (except psychotherapy notes)	covered entity that has or had a relationship with the individual who is the subject	disclose to another covered entity that has or had a relationship with the individual who is the subject	for the purpose of health care fraud and abuse detection or compliance.	

Provision	Object	Invoker	Action	Purpose	Condition
(5)	protected health information (except psychotherapy notes)	A covered entity that participates in an organized health care arrangement	disclose to another covered entity that participates in the organized health care arrangement	for any health care operations activities of the organized health care arrangement. (other than marketing)	
§164.508(a)(1)	protected health information	covered entity	use or disclose consistent with authorization		with an authorization that is valid under this section.
(2)(i)(A)	psychotherapy notes	originator of notes	use	for treatment	
(i)(B)	psychotherapy notes	covered entity	use or disclosure	for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling	
(i)(C)	psychotherapy notes	covered entity	use or disclosure	to defend itself in a legal action or other proceeding brought by the individual	
(3)(i)(A)	protected health information	covered entity	use or disclosure in a face-to-face communication to the individual	for marketing	

Provision	Object	Invoker	Action	Purpose	Condition
(i)(B)	protected health information	covered entity	use or disclose in a communication constituting a promotional gift of nominal value		
§164.510(a)(1)(i)	The individuals name; The individuals location in the covered health care providers facility; The individuals condition described in general terms that does not communicate specific medical information about the individual; and The individuals religious affiliation;	covered entity	use	to maintain a directory of individuals in its facility,	provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure. Except when an objection is expressed in accordance with paragraphs (a)(2) or (3) of this section
ii	The object from §164.510(a)(1)(i)	covered entity	disclose to persons who ask for the individual by name		provided that the same conditions as in §164.510(a)(1)(i) apply
	The object from §164.510(a)(1)(i)	covered entity	disclose to members of the clergy		provided that the same conditions as in §164.510(a)(1)(i) apply

Provision	Object	Invoker	Action	Purpose	Condition
(b)(1)(i)	the protected health information directly relevant to such persons involvement with the individuals care or payment related to the individuals health care	covered entity	disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual"		with the individual's agreement etc.
	the protected health information directly relevant to such persons involvement with the individuals care or payment related to the individuals health care	covered entity	disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual		if the individual is unavailable or incapacitated and covered entity believes disclosure is in individual's best interest
(ii)	protected health information	covered entity	use or disclose	to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individuals location, general condition, or death.	with the individual's agreement etc.

Provision	Object	Invoker	Action	Purpose	Condition
	protected health information	covered entity	use or disclose	to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individuals location, general condition, or death.	if the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the protected health information for which disclosure is sought is not intended to be used against the
	protected health information	covered entity	use or disclose to a public or private entity authorized by law or by its charter to assist in disaster relief efforts	for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section, to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individuals location, general condition, or death.	The requirements in paragraphs (b)(2) and (3) of this section apply to such uses and disclosure to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

Provision	Object	Invoker	Action	Purpose	Condition
	protected health information	covered entity	use or disclose to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section."	"to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individuals location, general condition, or death."	". The requirements in paragraphs (b)(2) and (3) of this section apply to such uses and disclosure to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances."
§164.512(a)(1)	protected health information	covered entity	use or disclose to the extent required by law		
(b)(1)(i)	protected health information	covered entity	disclose to a public health authority that is authorized by law to collect or receive such information	"for the purpose of preventing or controlling disease,injury, or disability"	
	protected health information	covered entity	disclose to an official of a foreign government agency that is acting in collaboration with a public health authority"		at the direction of a public health authority

Provision	Object	Invoker	Action	Purpose	Condition
(ii)	reports of child abuse or neglect	covered entity	disclose to a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;		
(iii)	protected health information	covered entity	disclose to a person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility	”for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity”	
§164.512(a)(1)	protected health information	covered entity	use or disclose to the extent required by law		
iv	protected health information	covered entity	disclose to person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition		if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation

Provision	Object	Invoker	Action	Purpose	Condition
(v)(A)	protected health information about an individual who is a member of the workforce of the employer	covered entity is a covered health care provider who is a member of the workforce of such employer	disclose to an employer		
(v)(A)	protected health information about an individual who is a member of the workforce of the employer	covered entity who provides health care to the individual at the request of the employer:	disclose to an employer		
(v)(B)	protected health information that consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance	covered entity	disclose to an employer		
(v)(C)	protected health information	covered entity	disclose to an employer		”The employer needs such findings in order to comply with its obligations, under 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance;”

Provision	**Object**	**Invoker**	**Action**	**Purpose**	**Condition**
(v)(D)	protected health information	Covered health care provider	disclose to an employer		The covered health care provider provides written notice to the individual that protected health information relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer
(2)	protected health information	public health authority	use	”for the purpose of preventing or controlling disease, injury, or disability”	
(c)(1)(i)	”protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence (except reports of child abuse or neglect)”	covered entity	disclose to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence		if required by law

Provision	Object	Invoker	Action	Purpose	Condition
(ii)	”protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence (except reports of child abuse or neglect)”	covered entity	disclose to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence”		If the individual agrees to the disclosure
(iii)(B)	”protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence (except reports of child abuse or neglect)”	covered entity	disclose to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence”		”The covered entity, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; ”
	protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence (except reports of child abuse or neglect)	covered entity	disclose to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence”		If the individual is unable to agree because of incapacity,a law enforcement or other public official authorized to receive the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure

Provision	Object	Invoker	Action	Purpose	Condition
(d)	protected health information	covered entity	disclose to a health oversight agency	”for oversight activities authorized by law,including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative,or criminal proceedings or actions; or other activities necessary for appropriate oversight”	
(e)(i)	protected health information	covered entity	disclose		”In response to an order of a court or administrative tribunal
ii	protected health information	covered entity	disclose		”In response to a subpoena, discovery request, or other lawful process, if the covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iii) of this section, from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request”

Provision	Object	Invoker	Action	Purpose	Condition
	protected health information	covered entity	disclose	In response to a subpoena, discovery request, or other lawful process	if The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iv) of this section, from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of paragraph (e)(1)(v) of this section. ”
(f)(1)(i)	protected health information	covered entity	disclose to a law enforcement official	for a law enforcement	”As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for laws subject to paragraph (b)(1)(ii) or (c)(1)(i) of this section”

Provision	Object	Invoker	Action	Purpose	Condition
(ii)(A)	protected health information	covered entity	disclose to a law enforcement official	for a law enforcement ,"In compliance with and as limited by the relevant requirements of: (A) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer; (B) A grand jury subpoena; or (C) An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law,	provided that: (1) The information sought is relevant and material to a legitimate law enforcement inquiry; (2) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and (3) Deidentified information could not reasonably be used.
ii-B	protected health information	covered entity	disclose to a law enforcement official	for a law enforcement	In compliance with and as limited by the relevant requirements of a grand jury subpoena

Provision	Object	Invoker	Action	Purpose	Condition
ii-C	protected health information	covered entity	disclose to a law enforcement official	for a law enforcement	”In compliance with and as limited by the relevant requirements of an administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that: (1) The information sought is relevant and material to a legitimate law enforcement inquiry; (2) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and (3) Deidentified information could not reasonably be used.”

Provision	Object	Invoker	Action	Purpose	Condition
2	"Name and address; Date and place of birth; Social security number; ABO blood type and rh factor;) Type of injury; Date and time of treatment; Date and time of death, if applicable; and A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or mustache), scars, and tattoos. "	covered entity	disclose to a law enforcement official	"for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person	in response to a law enforcement officials request
3i	protected health information about an an individual who is or is suspected to be a victim of a crime	covered entity	disclose to a law enforcement official	for a law enforcement	"in response to a law enforcement officials request, if the indvidual agrees"

Provision	Object	Invoker	Action	Purpose	Condition
ii	protected health information about an an individual who is or is suspected to be a victim of a crime	covered entity	disclose to a law enforcement official	for a law enforcement	”in response to a law enforcement officials request and if he covered entity is unable to obtain the individuals agreement because of incapacity or other emergency circumstance, provided that: (A) The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim; (B) The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and (C) The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.”

Provision	Object	Invoker	Action	Purpose	Condition
(4)	protected health information about an individual who has died	covered entity	disclose to a law enforcement official	for the purpose of alerting law enforcement of the death of the individual	if the covered entity has a suspicion that such death may have resulted from criminal conduct.
(5)	protected health information that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity.	covered entity	disclose to a law enforcement official	for a law enforcement	
(6)(i)(A)	protected health information	covered entity	disclose to a law enforcement official	for a law enforcement	
(i)(B)	protected health information	covered entity	disclose to a law enforcement official	for a law enforcement	
(i)(C)	protected health information	covered entity	disclose to a law enforcement official	for a law enforcement	
(g)(1)	protected health information	covered entity	disclose to a coroner or medical examiner	”for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law.”	

Provision	Object	Invoker	Action	Purpose	Condition
	protected health information	A covered entity that also performs the duties of a coroner or medical examiner	use	”for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law.”	
(2)	protected health information	covered entity	disclose to funeral directors		”consistent with applicable law, as necessary to carry out their duties with respect to the decedent. ”
	protected health information	covered entity	disclose to funeral directors		”If necessary for funeral directors to carry out their duties AND and in reasonable anticipation of,the individuals death”
(h)	protected health information	covered entity	disclose to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue”	”for the purpose of facilitating organ, eye or tissue donation and transplantation.”	

Provision	Object	Invoker	Action	Purpose	Condition
(i)(1)(i)	protected health information	covered entity	use or disclose	for research	”provided that: The covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by 164.508 for use or disclosure of protected health information has been approved by either: (A) An Institutional Review Board (IRB), or (B) A privacy board”
(ii)	protected health information	covered entity	use or disclose	for research	provided that The covered entity obtains from the researcher representations that: (A) Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research; (B) No protected health information is to be removed from the covered entity by the researcher in the course of the review; and (C) The protected health information for which use or access is sought is necessary for the research purposes

Provision	Object	Invoker	Action	Purpose	Condition
iii	protected health information about a decedent	covered entity	use or disclose	for research	”provided that The covered entity obtains from the researcher: (A) Representation that the use or disclosure sought is solely for research on the protected health information of decedents; (B) Documentation, at the request of the covered entity, of the death of such individuals; and (C) Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.”
j1i	protected health information	covered entity	use or disclose to a person or persons the covered entity believes, in good faith, to be reasonably able to prevent or lessen the threat, including the target of the threat”		”if the covered entity, in good faith, believes the use or disclosure) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public”

Provision	Object	Invoker	Action	Purpose	Condition
ii	”protected health information (only statement and (f)(2)(i) information) not learned in course of treatment to affect propensity to commit the criminal conduct or counseling or therapy or through a requet by the individual to initiate /to be referred for treatment, counseling,or therapy”	covered entity	use or disclose		”if the covered entity, in good faith, believes the use or disclosure Is necessary for law enforcement authorities to identify or apprehend an individual: (A) Because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim; or (B) Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody, as those terms are defined in 164.501”

Provision	Object	Invoker	Action	Purpose	Condition
k1i	protected health information of individuals who are Armed Forces personnel	covered entity	use or disclose	for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission	if the appropriate military authority has published by notice in the FEDERAL REGISTER the following information: (A) Appropriate military command authorities; and (B) The purposes for which the protected health information may be used or disclosed."
ii	the protected health information of an individual who is a member of the Armed Forces	. A covered entity that is a component of the Departments of Defense or Transportation	disclose to the Department of Veterans Affairs (DVA)	for the purpose of a determination by DVA of the individuals eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.	upon the separation or discharge of the individual from military service
iii	protected health information	A covered entity that is a component of the Department of Veterans Affairs	use or disclose to components of the Department that determine eligibility for or entitlement to, or that provide, benefits under the laws administered by the Secretary of Veterans Affairs."		

Provision	Object	Invoker	Action	Purpose	Condition
(iv)	protected health information of individuals who are foreign military personnel	covered entity	use or disclose to their appropriate foreign military authority	for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission	
(2)	protected health information	covered entity	disclose to authorized federal officials	”for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, et seq.) and implementing authority (e.g., Executive Order 12333). ”	
(3)	protected health information	covered entity	disclose to authorized federal officials	”for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or to for the conduct of investigations authorized by 18 U.S.C. 871 and 879. ”	
4	protected health information	A covered entity that is a component of the Department of State	use	to make medical suitability determinations	

Provision	Object	Invoker	Action	Purpose	Condition
i	whether or not the individual was determined to be medically suitable	A covered entity that is a component of the Department of State	disclose to the officials in the Department of State who need access to such information for the purpose of a required security clearance conducted pursuant to Executive Orders 10450 and 12698		
ii	whether or not the individual was determined to be medically suitable	A covered entity that is a component of the Department of State	disclose to the officials in the Department of State who need access to such information as necessary to determine worldwide availability or availability for mandatory service abroad under sections 101(a)(4) and 504 of the Foreign Service Act		
4	protected health information	A covered entity that is a component of the Department of State	use	to make medical suitability determinations	
iii	whether or not the individual was determined to be medically suitable	A covered entity that is a component of the Department of State	disclose to the officials in the Department of State who need access to such information for a family to accompany a Foreign Service member abroad, consistent with section 101(b)(5) and 904 of the Foreign Service Act.”		

Provision	Object	Invoker	Action	Purpose	Condition
4	protected health information	A covered entity that is a component of the Department of State	use	to make medical suitability determinations	
4	protected health information	A covered entity that is a component of the Department of State	use	to make medical suitability determinations	
5	protected health information about an inmate	covered entity	disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual	for any purpose for which such protected health information may be disclosed.	if the correctional institution or such law enforcement official represents that such protected health information is necessary for: (A) The provision of health care to such individuals; (B) The health and safety of such individual or other inmates;(C) The health and safety of the officers or employees of or others at the correctional institution; (D) The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another; (E) Law enforcement on the premises of the correctional institution; and (F) The administration and maintenance of the safety, security, and good order of the correctional institution. ”

Provision	Object	Invoker	Action	Purpose	Condition
4	protected health information	A covered entity that is a component of the Department of State	use	to make medical suitability determinations	
6i	protected health information relating to eligibility for or enrollment in the health plan	A health plan that is a government program providing public benefits	disclose to another agency administering a government program providing public benefits		if the sharing of eligibility or enrollment information among such government agencies or the maintenance of such information in a single or combined data system accessible to all such government agencies is required or expressly authorized by statute or regulation.
ii	protected health information relating to the program	A covered entity that is a government agency administering a government program providing public benefits	disclose to another covered entity that is a government agency administering a government program providing public benefits		if the programs serve the same or similar populations and the disclosure of protected health information is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions of such programs.

Provision	Object	Invoker	Action	Purpose	Condition
(l)	protected health information	covered entity	disclose		”as authorized by and to the extent necessary to comply with laws relating to workers compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault. ”
Sec 164.514(e)(1)	a limited data set that meets the requirements of paragraphs (e)(2) of this section	covered entity	use or disclose	for the purposes of research, public health, or health care operations.	if the covered entity enters into a data use agreement with the limited data set recipient, in accordance with paragraph (e)(4) of this section.”
(f)(1)(i)	Demographic information relating to an individual;individual.	covered entity	use or disclose to a business associate or to an institutionally related foundation	”for the purpose of raising funds for its own benefit	a statement required by 164.520(b)(1)(iii)(B) is included in the covered entitys notice; (ii) The covered entity must include in any fundraising materials it sends to an individual under this paragraph a description of how the individual may opt out of receiving any further fundraising communications. (iii) The covered entity must make reasonable efforts to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications.

Provision	Object	Invoker	Action	Purpose	Condition
(ii)	Dates of health care provided to an	covered entity	use or disclose to a business associate or to an institutionally related foundation	”for the purpose of raising funds for its own benefit	a statement required by 164.520(b)(1)(iii)(B) is included in the covered entitys notice; (ii) The covered entity must include in any fundraising materials it sends to an individual under this paragraph a description of how the individual may opt out of receiving any further fundraising communications. (iii) The covered entity must make reasonable efforts to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications.
(g)	protected heath information	covered entity	use or disclose	for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits	only as required by law
§164.522(a)(1)(iii)	protected health information	A covered entity	use or disclose		that agrees to a restriction under paragraph (a)(1)(i)

Provision	Object	Invoker	Action	Purpose	Condition
(iii)	protected health information	A covered entity that agrees to a restriction under paragraph (a)(1)(i)	use		if the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment”
	protected health information	A covered entity that agrees to a restriction under paragraph (a)(1)(i)	disclose to a health care provider	to provide such treatment to the individual.	if the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment and the covered entity must request that such health care provider not further use or disclose the information
§164.524(a)(1)	”protected health information (except psychotherapy notes, info compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding)”	covered entity	disclose to the individual		”no later than 30 days after receipt of the request, exceptions 524(2)(ii)-(v),(3)”
§164.526(a)(1)	protected health information	covered entity	amend		”on request by the individual, no later than 60 days after receipt of such a request, exceptions”
§164.528(a)(1)	accounting of disclosures	covered entity	discloseto the individual		no later than 60 days after receipt of such a request

C Encoding Facebook's Privacy Policy as Data-use Tuples

Provision	Object	Invoker	Action	Purpose	Condition
We are able to deliver our Services, personalize content, and make suggestions for you by using this information to understand how you use and interact with our Services and the people or things youre connected to and interested in on and off our Services.	Things you do and information you provide, things others do and information they provide, your networks and connections, information about payments, device information, information from websites and apps that use our Services, information from third-party partners, and information from Facebook companies	Facebook	create model of how you use and interact with our Services and the people or things youre connected to and interested in on and off our Services		
	model of how you use and interact with our Services and the people or things youre connected to and interested in on and off our Services	Facebook		deliver our Services	
	model of how you use and interact with our Services and the people or things youre connected to and interested in on and off our Services	Facebook		personalize content	
	model of how you use and interact with our Services and the people or things youre connected to and interested in on and off our Services	Facebook		make suggestions for you	

Provision	Object	Invoker	Action	Purpose	Condition
We also use information we have to provide shortcuts and suggestions to you. For example, we are able to suggest that your friend tag you in a picture by comparing your friend's pictures to information we've put together from your profile pictures and the other photos in which you've been tagged.	information we have	Facebook		provide shortcuts and suggestions to you	
When we have location information, we use it to tailor our Services for you and others, like helping you to check-in and find local events or offers in your area or tell your friends that you are nearby.	location information	Facebook		tailor our Services for you and others	
We conduct surveys and research, test features in development, and analyze the information we have to evaluate and improve products and services, develop new products or features, and conduct audits and troubleshooting activities.	the information we have	Facebook	analyze	to evaluate and improve products and services, develop new products or features, and conduct audits and troubleshooting activities.	

Provision	Object	Invoker	Action	Purpose	Condition
We use your information to send you marketing communications, communicate with you about our Services and let you know about our policies and terms.	your information	Facebook	communicate with you	marketing	
	your information	Facebook	communicate with you	to communicate about our Services	
	your information	Facebook	communicate with you	to let you know about our policies and terms.	
We also use your information to respond to you when you contact us.	your information	Facebook		to respond to you	when you contact us
We use the information we have to improve our advertising and measurement systems so we can show you relevant ads on and off our Services and measure the effectiveness and reach of ads and services.	the information we have	Facebook	use to improve our advertising and measurement systems	so we can show you relevant ads on and off our Services	
	the information we have	Facebook	use to measure the effectiveness and reach of ads and services.		
We use the information we have to help verify accounts and activity, and to promote safety and security on and off of our Services, such as by investigating suspicious activity or violations of our terms or policies.	the information we have	Facebook		to help verify accounts and activity	
	the information we have	Facebook		to promote safety and security on and off of our Services	
We use cookies and similar technologies to provide and support our Services and each of the uses outlined and described in this section of our policy.	cookies and similar technologies	Facebook		to provide and support our Services and each of the uses outlined and described in this section of our policy.	

Provision	Object	Invoker	Action	Purpose	Condition
When you share and communicate using our Services, you choose the audience who can see what you share. For example, when you post on Facebook, you select the audience for the post, such as a customized group of individuals, all of your Friends, or members of a Group.	information you share	Facebook	share with people permitted by preferences		until preference settings change
When you use third-party apps, websites or other services that use, or are integrated with, our Services, they may receive information about what you post or share.	what you post or share	Facebook	share with those third-party apps, websites or other services that use, or are integrated with, our Services		When you use third-party apps, websites or other services that use, or are integrated with, our Services
In addition, when you download or use such third-party services, they can access your Public Profile, which includes your username or user ID, your age range and country/language, your list of friends.	Public Profile	Facebook	share with third-party services		after you download or use such third-party services
	any information that you share with them	Facebook	share withthird-party services		after you download or use such third-party services
Information collected by these apps, websites or integrated services is subject to their own terms and policies.	information collected by third-party apps	third-party services	uses permitted by their terms and policies		

Provision	Object	Invoker	Action	Purpose	Condition
We share information we have about you within the family of companies that are part of Facebook.	information we have ab0ut you	Facebook	sharewithin the family of companies that are part of Facebook.		
If the ownership or control of all or part of our Services or their assets changes, we may transfer your information to the new owner.	your information	Facebook	transferto the new owner		If the ownership or control of all or part of our Services or their assets changes
We use all of the information we have about you to show you relevant ads.	all the information we have about you	Facebook		to show you relevant ads	
We do not share information that personally identifies you with advertising, measurement or analytics partners unless you give us permission.	information that personally identifies you	Facebook	share with advertising, measurement or analytics partners		if you give permission
We may provide these partners with information about the reach and effectiveness of their advertising without providing information that personally identifies you, or if we have aggregated the information so that it does not personally identify you.	non-personally identifying information about reach and effectiveness of their advertising.	Facebook	share with advertising, measurement or analytics partners		
	aggregate information	Facebook	share with advertising, measurement or analytics partners		

Provision	Object	Invoker	Action	Purpose	Condition
We transfer information to vendors, service providers, and other partners who globally support our business. These partners must adhere to strict confidentiality obligations in a way that is consistent with this Data Policy and the agreements we enter into with them.	information	Facebook	transfer to vendors, service providers, and other partners who globally support our business		These partners must adhere to strict confidentiality obligations in a way that is consistent with this Data Policy and the agreements we enter into with them.
Information associated with your account will be kept until your account is deleted, unless we no longer need the data to provide products and services.	information associated with your account	Facebook	delete		after you delete your account
	information associated with your account	Facebook	delete		when no longer needed to provide products and services
When you delete your account, we delete things you have posted, such as your photos and status updates.	things you have posted	Facebook	delete		after you delete your account
We may access, preserve and share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so.	your information	Facebook	access, preserve and share	to response to a legal request	if we have a good faith belief that the law requires us to do so.

Provision	Object	Invoker	Action	Purpose	Condition
We may also access, preserve and share information when we have a good faith belief it is necessary to: detect, prevent and address fraud and other illegal activity; to protect ourselves, you and others, including as part of investigations; or to prevent death or imminent bodily harm.	your information	Facebook	access, preserve and share		when we have a good faith belief it is necessary to detect, prevent and address fraud and other illegal activity
	your information	Facebook	access, preserve and share		when we have a good faith belief it is necessary to protect ourselves, you and others, including as part of investigations
	your information	Facebook	access, preserve and share		when we have a good faith belief it is necessary to prevent death or imminent bodily harm.