“No tengo nada que ocultar” y otros malentendidos de la privacidad

DANIEL J. SOLOVE*

INDICE

I. INTRODUCCIÓN

Desde los ataques del 11 de Septiembre, el gobierno se ha dedicado a la vigilancia extensa y la minería de datos (*Nota del Traductor: en inglés data mining, técnicas de extracción de información oculta y predecible de grandes bases de datos*). Con respecto a la vigilancia, en Diciembre de 2005, el New York Times reveló que luego del 11 de Septiembre, la Administración de Bush autorizó secretamente a la Administración de Seguridad Nacional (NSA, por sus siglas en inglés) para practicar, sin necesidad de orden judicial, escuchas telefónicas de las llamadas de los ciudadanos estadounidenses.[1]

En cuanto a la minería de datos que implica el análisis de datos personales en busca de patrones de comportamiento sospechoso, el gobierno ha comenzado numerosos programas. En 2002, los medios revelaron que el Departamento de Defensa estaba construyendo un proyecto de minería de datos, llamado “Conciencia Total de la Información” (TIA, por sus siglas en inglés), bajo el liderazgo del Almirante John Pointdexter.[2] Se esperaba que TIA reuniera variedad de información sobre la gente, incluyendo financiera, educacional, de salud y otros datos. La información se analizaría luego en busca de patrones de comportamiento sospechoso. Según Poindexter: “La única forma de detectar… terroristas es buscar patrones de actividad basados en observaciones de pasados ataques terroristas, así como estimaciones sobre cómo los terroristas van a adaptarse a nuestras medidas para evitar ser detectados.”[3] Cuando el programa salió a la luz, estalló una protesta pública, y el Senado de Estados Unidos votó posteriormente para negarle financiación al programa, llevándolo finalmente a su desaparición.[4] No obstante, muchos componentes de la TIA continúan en varias agencias del gobierno, aunque de forma

menos sistemática y más clandestina.[5]

En mayo de 2006, USA Today reveló que la NSA había obtenido los registros de clientes de varias compañías telefónicas y los estaba analizando para identificar potenciales terroristas.[6] La base de datos de llamadas telefónicas se reportó como la "base de datos más grande jamás recopilada en el mundo."[7] En junio de 2006, el New York Times afirmó que el gobierno de Estados Unidos había estado accediendo a los registros bancarios de la Sociedad para las Transacciones Financieras Interbancarias Mundiales (SWIFT, por sus siglas en inglés), que controla las transacciones financieras de miles de bancos alrededor del mundo.[8] Muchas personas respondieron con indignación ante estos anuncios, pero muchas otras no encontraron mayor problema en el asunto. La razón para su falta de preocupación, explicaron, era: "no tengo nada que ocultar."[9]

El argumento de que no existe un problema de privacidad si la persona no tiene nada que ocultar es frecuentemente dado en relación a asuntos de privacidad. Cuando el gobierno se dedica a la vigilancia, muchas personas creen que no existe una amenaza a la privacidad a menos que descubra una actividad ilícita, en cuyo caso una persona no tiene una justificación legítima para reclamar que ésta permanezca en privado. De este modo, si un individuo se dedica solamente a actividades legales, no tiene nada de qué preocuparse. Cuando se trata del gobierno recolectando y analizando información personal, muchas personas sostienen que el daño a la privacidad existe sólo si se revelan los muertos en el armario. Por ejemplo, supongamoss que el gobierno examina los registros telefónicos de alguien y descubre que la persona hizo llamadas a sus padres, a un amigo en Canadá, a una tienda de vídeo y a un local de entrega de pizzas. "¿Y qué?", puede decir esa persona, "No estoy avergonzado ni humillado por esta información. Si alguien me pregunta, con mucho gusto voy a decirle dónde compro. No tengo nada que ocultar."

El argumento de "nada que ocultar" y sus variantes son bastante frecuentes en discusiones sobre la privacidad. El experto en seguridad de datos Bruce Schneier lo llama la "contestación más común contra los defensores de la privacidad."[10] El perito en Derecho Geoffrey Stone se refiere a él como "dicho del que se abusan."[11] El argumento de nada que ocultar es uno de los principales argumentos hechos a la hora de balancear privacidad contra seguridad. En su forma más convincente, argumenta que el interés en la privacidad va generalmente de mínimo a trivial, haciendo entonces del balance frente a preocupaciones sobre la seguridad una victoria predestinada para la seguridad. A veces el argumento de nada que ocultar es planteado como una pregunta: "Si no tienes nada que ocultar, ¿entonces a qué le tienes miedo?" Otros preguntan: "Si no estás haciendo nada malo, ¿entonces qué tienes que ocultar?"

En este escrito, voy a explorar el argumento de nada que ocultar y sus variantes en mayor profundidad. Luchar contra el argumento de nada que ocultar es importante, porque éste refleja los sentimientos de un gran porcentaje de la población. En el discurso popular, los formulaciones superficiales del argumento de nada que ocultar pueden ser fácilmente refutados. Pero cuando el argumento es hecho en su forma más fuerte, es mucho más convincente. Para responder al argumento de nada que ocultar, es necesario que tengamos una teoría sobre lo que es la privacidad y por qué es valiosa. En esencia, el argumento de nada que ocultar surge de una noción sobre la privacidad y su valor. ¿Qué es exactamente "privacidad"? ¿Qué tan valiosa es y cómo calculamos su valor? ¿Cómo sopesamos la

privacidad frente a valores compensatorios? Estas preguntas han asolado durante mucho tiempo a aquellos que buscan desarrollar una teoría sobre la privacidad y una justificación para su protección legal.

Este ensayo comienza en la Parte II, discutiendo acerca del argumento de nada que ocultar. Primero, introduzco el argumento como a menudo se presenta en el discurso popular y examino formas frecuentes de responder a él. Segundo, presento al argumento en la que creo es su forma más fuerte. En la Parte III, hablo brevemente de mi trabajo hasta ahora en la conceptualización de la privacidad. Explico por qué las teorías existentes sobre la privacidad han sido insatisfactorias, han llevado a la confusión, y han impedido el desarrollo de respuestas legales y políticas efectivas a problemas de privacidad. En la Parte IV, expongo que el argumento de nada que ocultar (aún en su forma más fuerte) deriva de ciertas suposiciones erróneas sobre la privacidad y su valor. El problema, en definitiva, no es encontrar una respuesta a la pregunta: “Si no tienes nada que ocultar, ¿entonces a qué le tienes miedo?” El problema está en la pregunta misma.

II. EL ARGUMENTO DE "NADA QUE OCULTAR"

Cuando se discute si la vigilancia del gobierno y la minería de datos representan una amenaza a la privacidad, muchas personas responden que no tienen nada que ocultar. Este argumento impregna el discurso popular sobre la privacidad y los problemas de seguridad. En Gran Bretaña, por ejemplo, el gobierno ha instalado millones de cámaras de vigilancia públicas en ciudades y pueblos, que son monitoreados por los funcionarios a través de circuitos cerrados de televisión.[12] En un eslogan de campaña para el programa, el gobierno declara: "Si no tienes nada que ocultar, no tienes nada que temer."[13] En los Estados Unidos, un integrante anónimo del Departamento de Justicia comentó: "Si [los funcionarios del gobierno] necesitan leer mis e-mails. . . que así sea. No tengo nada que ocultar. ¿Y usted? "[14] Un blogger, en referencia a obtener perfiles personales por razones de seguridad, declara: "Adelante, investíguenme, no tengo nada que ocultar."[15] Otro blogger proclama: "a mí no me importa que averiguen cosas sobre mí, yo no tengo nada que ocultar! De esta manera apoyo los esfuerzos del presidente Bush para detectar terroristas mediante el monitoreo de nuestras llamadas telefónicas!"[16]. Variaciones del argumento de nada que ocultar aparecen con frecuencia en blogs, cartas a editores, entrevistas televisivas, y otros foros. Incluyo algunos ejemplos:

** Yo no tengo nada que ocultar. No creo que tenga mucho que ocultarle al gobierno en primer lugar. No creo que les importe si hablo de mi insoportable vecino.[17]*
** ¿Si me importa que el FBI vigile mis llamadas telefónicas? Yo no tengo nada que ocultar. Tampoco el 99,99 por ciento de la población. Si las escuchas telefónicas hubieran evitado alguno de los incidentes del 11 de septiembre, miles de vida se hubiesen salvado.[18]*
** Como he dicho, no tengo nada que ocultar. La mayoría de los norteamericanos no tiene nada que ocultar. Y los que tienen algo para ocultar deben ser descubiertos, y averiguar que obtienen con ello.[19]*

El argumento no es de cosecha reciente. Por ejemplo, uno de los personajes de una novela de 1888 escrita por Henry James, "El reverberador", reflexiona: "[Si] esta gente ha

hecho cosas malas deberían avergonzarse de ellos mismos y no se debe tenerles lástima, y si no lo han hecho, no hay necesidad de protestar porque otras personas lo sepan"[20].

Me encontré con el argumento de nada que ocultar tan a menudo en las noticias, entrevistas, debates y similares, que decidí hacer un blog sobre la cuestión. Les pedí a los lectores de mi blog, "Compartiendo Opiniones", si tenían alguna respuesta adecuada al argumento de nada que ocultar.[21] Como consecuencia, recibí una catarata de comentarios:

** Mi respuesta es "¿Así que usted tiene cortinas?" o "¿Puedo ver sus gastos con tarjetas de crédito del año pasado?"*[22]

** Así que mi respuesta al argumento "Si no tienes nada que ocultar..." es simple: "Yo no necesito justificar mi posición. Usted necesita justificar la suya. Vuelva con una orden judicial"*[23].

** Yo no tengo nada que ocultar. Pero no veo por qué debo mostrar algo.*[24]

** Si no tiene nada que ocultar, entonces usted no tiene una vida.*[25]

** Muéstrame lo tuyo y yo te mostraré lo mío.*[26]

** No se trata de tener algo que ocultar, se trata de cosas que son privadas.*[27]

** Joe Stalin lo resumió en forma excelente. ¿Por qué alguien tiene que decir algo?* [28]

La mayoría de las réplicas al argumento de nada que ocultar son respuestas rápidas e ingeniosas. En efecto, a primera vista, parece fácil refutarlo. Todo el mundo probablemente tenga algo que ocultar. Como Aleksandr Solzhenitsyn dijo: "Todo el mundo es culpable de algo o tiene algo que ocultar. Todo lo que hay que hacer es buscar lo suficiente para encontrarlo."[29] Del mismo modo, en la novela de Friedrich Dürrenmatt *Trampas*, un hombre aparentemente inocente es llevado a juicio por un grupo de abogados jubilados como parte de un juego . En el simulacro de juicio, el hombre inquiere cuál será su delito. "Un asunto totalmente secundario", responde el fiscal. . . . "Un crimen siempre se puede encontrar."[30] Por lo general se puede pensar en algo tan convincente que incluso la persona más abierta querría esconderlo. Como uno de los comentarios a mi blog señaló: "Si no tienes nada que ocultar, entonces, literalmente, significa que estás dispuesto a dejarte fotografiar desnudo. Y que me das plenos derechos a que pueda mostrar estas fotografías a tus vecinos."[31] El experto en privacidad canadiense David Flaherty expresa una idea similar cuando dice: “No hay ser humano consciente en el mundo occidental, que no tenga algo de respeto de su intimidad; aquellos que lo niegan no pueden soportar ni siquiera un cuestionario de escasos minutos sobre aspectos íntimos de su vida sin capitular ante algún tipo de intrusión.”[32]

Esas respuestas sólo refutan el argumento de nada que ocultar cuanto se expresa en forma extrema, lo que no es particularmente fuerte. Con sólo una línea que declare alguna preferencia de una persona en particular, el argumento de nada que ocultar no es muy convincente. Sin embargo, si se expresa de una forma más sofisticada, el argumento es más

desafiante. En primer lugar, debe ampliarse más allá de lo que haga una persona en particular. Cuando se formula como una preferencia personal, el argumento de nada que ocultar es difícil de refutar porque es difícil pelear con las preferencias de una persona en particular. Como un comentarista acertadamente señala: al decir "no tengo nada que ocultar", usted está diciendo que está bien que el gobierno infringa los derechos de potencialmente millones de sus compañeros estadounidenses, pudiendo arruinar sus vidas en el proceso. Para mí, el argumento de "yo no tengo nada que ocultar" equivale básicamente a “no me importa lo que suceda, siempre y cuando no me suceda a mí"[33].

En sus variantes más convincentes, el argumento de nada que ocultar puede ser expresado de una manera más general. En lugar de sostener que "no tengo nada que ocultar", el argumento se puede reformular postulando que ningún ciudadano respetuoso debería tener nada que ocultar. Sólo si la gente desea encubrir actividades ilícitas debería estar preocupada, pero de acuerdo al argumento de nada que ocultar, las personas que participan en una conducta ilegal no tienen derecho legítimo a mantener la privacidad de las mismas.

En una línea argumental semejante, el juez Richard Posner sostiene que: "Cuando la gente de hoy lamenta la falta de privacidad, lo que quieren, creo yo, es principalmente algo muy distinto a la reclusión: quieren más poder para ocultar información sobre sí mismos para que otros no puedan utilizarla en su contra"[34]. La privacidad de una persona involucra “el derecho a ocultar hechos deshonrosos acerca de sí mismo."[35] En otras palabras, la privacidad se invoca cuando hay algo que ocultar y que consiste en información negativa acerca de una persona. Posner afirma que la ley no debe proteger a las personas cuando ocultan información deshonrosa. "El economista", argumenta, "advertirá un paralelo con los esfuerzos de los vendedores para ocultar defectos en sus productos."[36]

Por supuesto, se podría objetar que hay información que no es deshonrosa acerca de las personas que, sin embargo, quieren ocultar porque les da vergüenza o simplemente no quieren que los demás conozcan. En su mínima expresión el argumento de nada que ocultar no se refiere a todos los datos personales, solamente se refiere al subconjunto de información personal que está involucrada en la vigilancia del gobierno. Cuando la gente responde que no tiene nada que ocultar a la NSA y a la minería de datos, la más sofisticada manera de entender su argumento es aplicarlo exclusivamente a las piezas particulares de información que recogen los programas de la NSA. La información acerca de los números telefónicos con los cuales se establecen llamadas, incluso lo que se dice en muchas conversaciones, es probable que a menudo no sea vergonzoso o deshonroso para un ciudadano respetuoso de la ley. La refutación al argumento de nada que ocultar basada en la exposición como si estuviésemos desnudos o en la revelación de los secretos más íntimos a sus amigos sólo es relevante si existe la posibilidad de que tales programas realmente produzcan estos tipos de revelaciones. Sin embargo, este tipo de información no es probable que sea capturado en la vigilancia del gobierno. Incluso si lo fuera, muchas personas racionalmente podrían asumir que la información va a ser expuesta solamente a unos pocos funcionarios, y tal vez ni siquiera vista por ojos humanos. Las computadoras podrían almacenar los datos y analizarlos para obtener los patrones, sin que ninguna persona tuviera contacto con los datos. Como Posner argumenta: “Se dice que la recolección, principalmente a través de medios electrónicos, de grandes cantidades de datos personales invade la privacidad. Pero las máquinas de recolección y procesamiento de datos no pueden,

como tal, invadir la privacidad. Debido a su volumen, los datos son primero tamizados por las computadoras, en la búsqueda de nombres, direcciones, números de teléfono, etc, que pueden tener valor de inteligencia. Este tamiz inicial, lejos de invadir la privacidad (un ordenador no es un ser sensible), mantiene los datos más privados para que no puedan ser leídos por cualquier oficial de inteligencia."[37]

Hay un componente final de las versiones más atractivas del argumento de nada que ocultar -una comparación del valor relativo del interés en la privacidad que está siendo amenazada con el interés del gobierno en promover la seguridad. Como un comentarista de mi blog astutamente señala: "No se puede hablar de cómo la gente se siente acerca de la posible pérdida de privacidad de una manera significativa, sin reconocer que a la mayoría de las personas a las que no les importa los programas de la NSA ven como un potencial beneficio ceder una pequeña cantidad de su intimidad para una ganancia potencial de la seguridad nacional."[38] En otras palabras, el argumento de nada que ocultar se puede justificar mediante la comparación entre los valores relativos de la privacidad y la seguridad. El valor que el argumento asigna a la privacidad es bajo, debido a que la información no suele ser especialmente sensible. Los que tienen que preocuparse más son los que mantienen una conducta ilegal, y el valor de la protección de su privacidad es menor o inexistente. Por el lado de la balanza de los intereses del gobierno, la seguridad tiene un valor muy alto. Tener un ordenador que analice los números de teléfono que alguien marca no puede exponer profundos secretos oscuros o información embarazosa para el mundo. La máquina trabajará simplemente, ajena a cualquier patrón que no se conside sospechoso. En otras palabras, si no se está haciendo nada malo, no tienes nada que ocultar ni nada que temer.

Por lo tanto, en una forma más convincente que se expresa a menudo en el discurso popular, el argumento de nada que ocultar procede de la siguiente manera:

"La vigilancia de la NSA, la minería de datos, o la información gubernamental que reúnen los programas se traducirá en la divulgación de determinados elementos de información a unos cuantos funcionarios públicos, o tal vez sólo para los equipos informáticos del gobierno. Esta descripción muy limitada de la información particular en cuestión no es probable que amenace a la privacidad de los ciudadanos respetuosos de la ley. Sólo aquellos que están involucrados en actividades ilegales tienen una razón para ocultar información. Aunque puede haber algunos casos en los que la información puede ser sensible o embarazosa para los ciudadanos respetuosos de la ley, la divulgación limitada disminuye la amenaza a la privacidad. Además, el interés de la seguridad en la detección, investigación y prevención de los ataques terroristas es muy alto y pesa más que los mínimos o moderados intereses de los ciudadanos respetuosos de la ley en mantener la privacidad de estas piezas particulares de información." Planteado de esta manera, el argumento de nada que ocultar es categórico. Se equilibra el grado en que se ve comprometida la privacidad de un individuo por la divulgación de cierta información limitada contra los potentes intereses nacionales de seguridad. Bajo tal esquema de equilibrio, es muy difícil que la privacidad prevalezca.

III. EL CONCEPTO DE LA PRIVACIDAD

Por cierta cantidad de tiempo, los estudiosos han proclamado que la privacidad es un

concepto tan esquivo que es de poca utilidad. De acuerdo a Arthur Miller, la privacidad es "extremadamente vaga y evanescente"[39]. Hyman Gross declara que "el concepto de privacidad esta infectado con perniciosas ambigüedades"[40]. De manera similar Collin Bennet anuncia "los intentos de definir el concepto de 'privacidad' no han encontrado ningún exito"[41]. Robert Post declara que "la privacidad es un valor tan complejo, enredada con tantos aspectos tan enfrentados y contradictorios, tan llena de diversos significados diferentes que a veces me desespera pensar si podrá definirse completamente"[42]. "Quizás lo más claro acerca de la privacidad," observa Judith Jarvis Thompson, "es que nadie parece tener una clara idea de lo que es"[43].

A menudo, el discurso filosófico acerca del concepto de la privacidad es ignorado en debates legales y politicos. Muchos jueces, políticos y estudiosos simplemente analizan el tema sin articular un concepto del significado de la privacidad. Sin embargo, darle un concepto es esencial para el análisis del tema. Todos los que trabajan en leyes y política tienen un concepto implícito de privacidad. En muchos casos, el tema de la privacidad nunca se opone a intereses conflictivos porque las cortes, los legisladores y demás fracasan incluso al reconocer que la privacidad está en juego. Por lo tanto es de vital importancia que continuemos trabajando para desarrollar el concepto de la privacidad ¿Pero cómo? ¿Por qué los anteriores intentos fueron tan insatisfactorios?

A – Un concepto plural de la privacidad

Muchos intentos de conceptualizar a la privacidad lo hacen por la vía de localizar su esencia, sus características principales o el común denominador que aglutina las varias cosas que colocamos bajo ese nombre. Me refiero a esto como el método tradicional de conceptualización. Este método plural busca entender la privacidad "per genus et differentiam", buscando los elementos necesarios y suficientes que demarquen qué es la privacidad.

En mi artículo "Conceptualizando la privacidad", discutí un amplio rango de intentos de localizar su común denominador[44]. Examine distintos candidatos para el común denominador en la literatura y en las leyes existentes. Algunos intentos eran demasiado estrechos, excluyendo cosas que comúnmente entendemos como privadas. Por ejemplo, varios teóricos han debatido que debe ser interpretada en términos de intimidad. De acuerdo al filósofo Julie Innes: "La esencia de la privacidad no puede ser capturada si nos enfocamos exclusivamente en información, acceso, o decisiones íntimas porque la privacidad involucra esas tres areas completamente… Sugiero que esas áreas aparentemente separadas sean englobadas bajo el común denominador de privacidad. La privacidad cubre información, acceso y decisiones íntimas"[45]. El problema de entender la privacidad como intimidad yace en que no toda la informacion o las decisiones que tomamos son íntimas. Por ejemplo nuestro número de Seguridad Social, afiliación política, creencia religiosa y más pueden no ser íntimas, pero sí las consideramos privadas. Por supuesto, podríamos ampliar la definición de intimidad, pero eso la convertiría en un sinónimo de privacidad más que en una elaboración de lo que la privacidad significa. El propósito de definir la privacidad como intimidad es desarrollar un concepto coherente y cohesivo, pero tiene la desventaja de ser demasiado estrecho.

En el extremo opuesto, algunos intentos son demasiado amplios; por ejemplo Samuel Warren y Louis Brandei entienden el concepto como “el derecho a que te dejen en paz”[46] ¿Qué significa exactamente ser dejado en paz? Hay muchas formas en que invadimos el espacio del otro que no son consideradas un ataque a la privacidad. Si me pegas un empujón en la calle no me estas dejando en paz. Quizás hasta llegues a lastimarme, pero no presenta un problema de privacidad.

En definitiva, cualquier intento de encontrar un núcleo en común para la multitud de cosas que componen lo que llamamos privacidad enfrenta un difícil dilema. Si uno decide que determinado denominador es suficientemente amplio para enmarcar casi todo, corre el riesgo de que ser sobreinclusivo o demasiado genérico. Si se decide por algo más preciso, el riesgo consiste en que sea demasiado restrictivo. En *Conceptualizando la privacidad*, examiné las distintas ideas propuestas y encontré que todas sufren de esos mismos problemas[47].

Mi argumento es que en lugar de conceptualizar la privacidad de la manera tradicional, deberíamos entenderla como un conjunto de semejanzas familiares. En su *Investigaciones filosóficas*, Ludwig Wittgenstein argumentó que algunos conceptos no tienen "una cosa en común" sino que están “relacionados entre sí de muchas maneras diferentes."[48] En lugar de estar relacionadas por un denominador común, algunas cosas comparten “una complicada red de similitudes superpuestas y entrecruzadas: a veces son totalmente similares, a veces sólo lo son en detalle."[49] En otras palabras, la privacidad no es reducible a una esencia singular, es una pluralidad de cosas diferentes que no comparten un elemento en común, pero que no obstante tienen una semejanza entre sí.

En mi trabajo sobre la conceptualización de la privacidad hasta el momento, he tratado de sentar las bases para una comprensión pluralista. En algunas obras, he tratado de analizar cuestiones específicas de privacidad, tratando de articular mejor la naturaleza de los problemas. Por ejemplo, en mi libro, *La Persona Digital,* sostuve que la recolección y el uso de información personal en las bases de datos presenta un conjunto diferente de problemas que el que presenta la vigilancia del gobierno.[50] Muchos comentaristas habían estado utilizando la metáfora de *1984* de George Orwell para describir los problemas creados por la recolección y el uso de datos personales.[51] Yo sostengo que la metáfora de Orwell, que se centra en los daños de la vigilancia (tales como la inhibición y el control social) puede ser apta para describir la aplicación de la ley de control de los ciudadanos. Pero gran parte de los datos recogidos en bases de datos no es particularmente confidencial, como la raza, fecha de nacimiento, sexo, dirección, o estado conyugal. Muchas personas no se preocupan por ocultar los hoteles en que se quedan, los coches de su propiedad o alquiler, o el tipo de bebidas que consumen. Las personas a menudo no toman muchas medidas para mantener en secreto dicha información. Con frecuencia, aunque no siempre, las actividades de las personas no se inhiben aunque los demás conozcan esta información.

Yo sugiero una metáfora diferente para captar los problemas: *El proceso* de Franz Kafka, que representa una burocracia con fines inescrutables que utiliza la información de las personas para tomar decisiones importantes acerca de ellos, pero le niega al pueblo la posibilidad de participar en la decisión de cómo se usa esta información.[52] El problema capturado por la metáfora de Kafka es de diferente orden que los problemas causados por la vigilancia. A menudo no producen inhibición ni escalofríos. En cambio, los problemas son

el procesamiento de información –almacenamiento, uso o análisis de datos- antes que la recolección. Afectan a las relaciones de poder entre las personas y las instituciones del Estado moderno. Ellos no sólo frustran a los individuos creando una sensación de indefensión e impotencia, también afectan la estructura social mediante la alteración del tipo de relaciones que las personas tienen con las instituciones que toman decisiones importantes sobre sus vidas.

He explorado las formas en que las soluciones jurídicas y políticas se centran demasiado en el nexo de problemas bajo la metáfora de Orwell -los problemas de vigilancia- y no se enfocan adecuadamente frente a los problemas de Kafka -los de procesamiento de información.[53]

La dificultad era que los comentaristas estaban tratando de concebir los problemas causados por las bases de datos en términos de vigilancia cuando, de hecho, estos problemas eran diferentes. La forma en que estos problemas se conciben tiene un tremendo impacto en los aspectos jurídicos y en las soluciones políticas utilizadas para resolverlos. Como observó John Dewey, "[Un] problema bien puesto está medio resuelto."[54] "La forma en que se concibe al problema" explica Dewey "decide qué sugerencias específicas son contempladas y cuales son descartadas, los datos que se seleccionan y los que se rechazan, este es el criterio para determinar la relevancia y la irrelevancia de las hipótesis y estructuras conceptuales."[55]

En un artículo posterior, *Una taxonomía de la privacidad*, he desarrollado una taxonomía de la vida privada -una forma de bosquejar los múltiples tipos de problemas y daños que constituyen violaciones a la privacidad.[56] La taxonomía es mi intento de formular un modelo de los problemas de estudio del cúmulo de leyes, casos, temas y materiales culturales e históricos. La taxonomía la he desarrollado como sigue:

Recolección de Información
- Vigilancia
- Interrogatorio

Procesamiento de la Información
- Colección
- Identificación
- Inseguridad
- Uso secundario
- Exclusión

Difusión de la Información
- Violación de la confidencialidad
- Revelación
- Exposición
- Mayor accesibilidad
- Chantaje
- Apropiación
- Distorsión

Invasión
- Intrusión

Interferencia Decisional

La taxonomía presenta cuatro categorías generales de problemas de privacidad con dieciséis subcategorías diferentes. La primera categoría general es la recolección de información, que incluye las formas en que se reúnen los datos sobre las personas. Las subcategorías, vigilancia e interrogatorio, representan las dos maneras más problemáticas de recopilar información. Un problema de privacidad ocurre cuando alguna actividad de una persona, negocio o entidad gubernamental crea daño al interrumpir las actividades de valor de los demás. Estos dañosno tienen por qué ser físicos o emocionales, ya que pueden ocurrir al desalentar comportamientos socialmente beneficiosos (por ejemplo, la libertad de expresión y de asociación) o dando lugar a desequilibrios de poder que inciden negativamente en la estructura social (por ejemplo, el poder ejecutivo excesivo).

La segunda categoría general es el procesamiento de la información. Esto implica el análisis del almacenamiento y la manipulación de datos. Hay un número de problemas que pueden causar el procesamiento de información, e incluyo cinco subcategorías en mi taxonomía. Por ejemplo, un problema que etiqueto como *inseguridad* resulta en un aumento de la vulnerabilidad de las personas a los posibles abusos de su información.[57] El problema que yo llamo exclusión involucra a la imposibildad de las personas de objetar la forma en que sus datos son usados.[58]

La difusión de información es la tercera categoría general. Implica las formas en que se transfiere -o se amenaza con transferir- a otros. Identifico siete formas diferentes. Finalmente, la última categoría incluye las invasiones. Las invasiones son interferencias directas con el individuo, como la intrusión en su vida o en la regulación del tipo de decisiones que puede hacer de su vida.

El propósito de mi taxonomía es definir más precisamente la privacidad con el fin de evitar distintos daños y problemas que provocan confusión o no son reconocidos. Alguien podría objetar, sin embargo, que varios de los problemas que discuto no son realmente problemas de "privacidad". Pero no existe un conjunto satisfactorio de condiciones necesarias o suficientes para definir que es la privacidad, no existe un criterio específico para decidir cuándo es un asunto privado y cuando no Las violaciones a la privacidad consisten en una red de problemas relacionados que no están conectados por un elemento común, pero tienen algunas semejanzas entre sí. Podemos clasificar un asunto como privado si se parece a otras cosas que clasifican como tales. En otras palabras, usamos una forma de razonamiento analógico en el que "la tarea clave", como señala Cass Sunstein, "es decidir cuándo hay similitudes relevantes y cuando no."[59] Por consiguiente, no existen límites claros para lo que debe o no referirse como "privacidad". Algunos podrían objetar la falta de límites claros, pero esto presupone su existencia. La búsqueda de una definición tradicional de privacidad conduce a un debate bastante estéril e irresuelto. Mientras tanto, hay verdaderos problemas que deben ser abordados, pero se confunden o ignoran porque no encajan en varias concepciones prefabricadas de la privacidad. La ley a menudo se niega a ver los problemas e ignora todas las cosas que no pertenecen a una determinada concepción de la vida privada. Así, las ideas preestablecidas acerca de la vida privada impiden examinar los problemas. Ellos aún existen independientemente de cómo los clasifiquemos. Se pierde mucho tiempo tratando de determinar el concepto de privacidad sin

tener en cuenta los problemas que estamos enfrentando. Mi objetivo es ir directamente a los problemas y estudiarlos en detalle. Tratar de ajustarlos a todos dentro de una definición estrecha de la vida privada es negar sus múltiples aspectos y la posibilidad de entenderlos completamente.

Los conceptos deberían ayudarnos a comprender e iluminar la experiencia, no deberían restarle valor ni aumentar la confusión.

El término privacidad se debe utiliza como un término que aglutina una red de ideas relacionadas entre ellas. Más allá de este tipo de uso, el término privacidad no tiene mayor utilidad. De hecho, puede confundir más que aclarar.

Algunas personas podrían objetar a la inclusión o la falta de ciertos problemas en la taxonomía. No avanzaría en la taxonomía si la quisiera perfecta. Se trata más bien de un trasfondo del proyecto en curso. A medida que surjan nuevos problemas, la taxonomía se revisará. Que un problema particular sea clasificado como un problema de privacidad no es tan importante, sí lo es que sea reconocido como un problema. Independientemente de si etiquetamos el problema como parte del grupo de privacidad, todavía es un problema, y es importante protegernos de él. Por ejemplo, yo clasifico como una violación de la privacidad a un problema que llamo distorsión, que consiste en difundir información falsa o engañosa sobre una persona. Algunos podrían argumentar que la distorsión realmente no es un daño a la privacidad, porque la intimidad sólo involucra a la información veraz. ¿Pero qué más da? Independientemente de si la distorsión es clasificada como un problema de la privacidad, sigue siendo un problema. Al clasificarlo como un problema de privacidad nos limitamos a decir que tiene cierto parecido a otros problemas privados y verlos todos juntos podría ser útil para su tratamiento.

B. El valor social de la privacidad

Muchas teorías de la privacidad la ven como un derecho individual. Por ejemplo, Thomas Emerson declara que la privacidad "se basa en premisas de individualismo, que la sociedad existe para promover el valor y la dignidad de la persona. . . . El derecho a la privacidad. . . es esencialmente el derecho a no participar en la vida colectiva, el derecho de excluir a la comunidad."[60] En las palabras de un tribunal: “La privacidad es inherentemente personal. El derecho a la intimidad reconoce la soberanía del individuo "[61].

Tradicionalmente, los derechos han sido entendidos a menudo como la protección del individuo frente a la incursión de la comunidad, basado en el respeto a la personalidad del individuo y a su autonomía. Muchas teorías de valor de la privacidad la entienden de esta manera. Por ejemplo, Charles Fried argumenta que la privacidad es una de los

> *derechos básicos de las personas, ante los cuales todos son iguales, en virtud de su condición de personas. . . . En este sentido, es una visión kantiana, que requiere el reconocimiento de las personas como fines, y prohíbe la anulación de sus intereses más fundamentales con el fin de maximizar la felicidad o el bienestar de todos.*[62]

Muchos de los intereses que entran en conflicto con la privacidad, sin embargo, también implican a la autonomía de las personas y su dignidad. La libertad de expresión,

por ejemplo, es también un derecho individual, que es esencial a la autonomía. Sin embargo, en varios casos, se enfrenta con la privacidad. La privacidad de una persona puede estar en conflicto directo con el deseo de otra de hablar acerca de la vida de esa persona. Además, la seguridad no es sólo un interés de la sociedad, sino que es esencial para la autonomía individual. La autonomía y la dignidad se encuentran a menudo en ambos lados de la balanza, por lo que se hace difícil saber qué lado es el que protege la "la soberanía del individuo"[63].

Los estudiosos de las comunidades han lanzado críticas formidables a las declaraciones tradicionales de los derechos individuales. Amitai Etzioni, por ejemplo, sostiene que la privacidad es "una licencia social que excluye una categoría de actos (incluyendo pensamientos y emociones) del escrutinio público, de la comunidad y del gobierno."[64] Para Etzioni, muchas teorías de la privacidad la tratan como algo sacrosanto, incluso cuando entra en conflicto con el bien común.[65] Según Etzioni, "La privacidad no es un valor absoluto y no debe superar a todos los demás derechos concernientes al bien común."[66] Él pretende demostrar cómo la privacidad interfiere con intereses sociales más importantes y, a menudo, aunque no siempre, sostiene que la privacidad debe salir perdiendo en el balance.[67]

Etzioni tiene razón al criticar a aquellos que argumentan que la privacidad es un derecho individual que debe prevalecer sobre los intereses sociales. El problema, sin embargo, es que el equilibrio entre los derechos individuales y el bien común rara vez favorece a los derechos individuales, -a menos que el interés del lado del bien común sea trivial. La sociedad en general sale ganando cuando sus intereses se equilibran con las del individuo.

El problema de fondo con la opinión de Etzioni es que en su crítica de la teorías liberales de los derechos individuales como absolutos, los ve en permanente tensión con la sociedad. La misma dicotomía entre individuo y sociedad que invade las teorías liberales de los derechos individuales también impregna el comunitarismo de Etzioni. Etzioni considera que la tarea de los comunitaristas es "balancear los derechos individuales con las responsabilidades sociales, y la individualidad con la comunidad."[68] El problema con la visión comunitaria de Etzioni es que la individualidad no tiene por qué estar en el lado opuesto de la comunidad. Este punto de vista asume que el individuo y los intereses sociales son distintos y contradictorios. Una opinión similar también sustentan muchos de las concepciones liberales de los derechos individuales.

En contraste, John Dewey propuso una teoría alternativa sobre la relación entre el individuo y la comunidad. Para Dewey, no existe tal dicotomía estricta entre individuo y sociedad. El individuo está formado para la sociedad, y el bien de la persona y la sociedad están a menudo relacionados entre sí y no son antagónicos: "No podemos pensar en nosotros mismos salvo como seres sociales. Por lo tanto, no podemos separar la idea de nosotros mismos y nuestro propio bien de nuestra idea del otro y de su bien"[69] Dewey sostiene que el valor de la protección de los derechos individuales surge a partir de su contribución a la sociedad. En otras palabras, los derechos individuales no son triunfos, pero son protecciones ante las intrusiones de la sociedad.

La sociedad les da espacios al individuo debido a los beneficios sociales que de ello obtiene. Por lo tanto, Dewey sostiene que los derechos deben valorarse en base a "la

contribución que hacen al bienestar de la comunidad"[70]. De lo contrario, en cualquier tipo de cálculo utilitario, los derechos individuales no serían lo suficientemente valiosos como para compensar los intereses de la mayoría social, y sería imposible justificar su existencia. En este sentido, argumentó Dewey, debemos insistir en una "justificación social y base social" para las libertades civiles.[71]

Yo sostengo, al igual que Dewey, que el valor de la protección de la persona es un valor social. La sociedad implica una gran cantidad de fricción, y las personas estamos constantemente chocando unas con otras. Parte de lo que hace que una sociedad sea un buen lugar para vivir es que permite hasta un cierto punto a la gente la libertad para entrometerse con otros. Una sociedad que no proteja a la privacidad puede ser asfixiante, y no será un lugar en el que la mayoría desee vivir. Al proteger los derechos individuales, nosotros como sociedad decidimos mantenerlos controlados para obtener los beneficios de crear zonas liberadas para que puedan prosperar.

Como Robert Post argumenta, la privacidad no es más que un conjunto de restricciones sobre las reglas de la sociedad y sus normas. En otras palabras, la privacidad constituye un intento de la sociedad para promover normas de conducta, el decoro y la urbanidad.[72] La sociedad protege la privacidad como un medio para cumplir una especie de orden en la comunidad. Como Spiros Simitis declara: "las consideraciones sobre la privacidad ya no surgen de determinados problemas individuales, sino que expresan los conflictos que afectan a todos."[73] Varios estudiosos han argumentado que la privacidad es "parte esencial" de la sociedad y debe ser valorada en función de los roles sociales que cumple.[74] La privacidad, entonces, no es el grito del individuo en contra de los intereses de la sociedad, es la protección de la persona sobre la base de las propias normas y valores sociales. La privacidad no es simplemente una manera en que los individuos eluden el control social, es más bien una forma de control que se desprende de las normas de una sociedad. No es una limitación externa sobre la sociedad, de hecho, es una dimensión interna de elle. Por lo tanto, la privacidad tiene un valor social. Incluso cuando protege a la persona, lo hace por el bien de la sociedad. No deben considerarse a los derechos individuales como contrarios al bien social. Los problemas de privacidad se entremezclan con los intereses sociales.

Debido a que la privacidad implica la protección contra una pluralidad de diferentes daños o problemas, su valor difiere según del cual nos protega. No todas los problemas de privacidad son iguales, algunos son más dañinos que otros. Por lo tanto, no se puede atribuir un valor abstracto a la privacidad. Su valor diferirá sustancialmente dependiendo del tipo de problema o daño del que nos esté protegiendo. Por lo tanto, para comprender la intimidad, debemos conceptualizarla y darle un valor más plural. La privacidad es un conjunto de protecciones contra un conjunto de problemas relacionados. Estos problemas no están relacionados en la misma manera, ero se asemejan entre sí. Existe un valor social en la protección ante cada problema, y este valor difiere dependiendo de su naturaleza.

IV. EL PROBLEMA CON EL ARGUMENTO DE "NADA QUE OCULTAR"

A. Entendiendo las múltiples dimensiones de la privacidad

Es hora de volver al argumento de nada que ocultar. El razonamiento de este argumento es que cuando se trata de la vigilancia gubernamental o el uso de datos personales, no hay violación de la privacidad si una persona no tiene nada sensible, vergonzoso o ilegal que ocultar. Solamente los delincuentes involucrados en actividades ilícitas tienen algo que temer, pero para la gran mayoría de las personas, sus actividades no son ilegales o vergonzosas.

Al entender la privacidad como he expuesto se revela el defecto del argumento de nada que ocultar desde sus raíces. Muchos comentaristas que responden al argumento intentan una refutación directa, tratando de señalar las cosas que la gente desea ocultar. Pero el problema con el argumento de nada que ocultar es el supuesto subyacente de que la privacidad se refiere a cómo ocultar cosas malas. Estar de acuerdo con esta hipótesis es concederle demasiada importancia y conduce a un debate improductivo acerca de que información es probable que la gente quisiera ocultar. Como acertadamente señala Bruce Schneier, el argumento de nada que ocultar parte de una suposición errónea: "[la] premisa de la privacidad es ocultar algo malo"[75].

El problema más profundo con el argumento de nada que ocultar es que su miopía le hace ver a la privacidad como una forma de ocultar secretos. Pero si entendemos a la privacidad como una pluralidad de problemas relacionados podemos ver que el ocultamiento de cosas malas es sólo uno de los muchos problemas causados por los programas de gobierno tales como la vigilancia de la NSA y la minería de datos. En las categorías de mi taxonomía, varios problemas están implicados.

Los programas de la NSA implican problemas de recolección de información, específicamente en la categoría de la vigilancia. Las escuchas telefónicas implican la vigilancia de las conversaciones de la gente. La minería de datos a menudo comienza con la recolección de información personal, por lo general de varios terceros que posean datos de las personas. Bajo la actual jurisprudencia de la Corte Suprema , cuando el gobierno reúne datos a partir de terceros, no hay protección de la Cuarta Enmienda porque las personas carecen de una "expectativa razonable de privacidad" en la información expuesta a otras.[76] En el caso *Estados Unidos vs Miller*, la Corte Suprema concluyó que no hay una expectativa razonable de privacidad en los registros bancarios porque "Todos los documentos obtenidos, incluidos los estados financieros y boletas de depósito, sólo contienen información transmitida voluntariamente a los bancos y se expone a sus empleados en el curso ordinario de los negocios."[77] En Smith v Maryland, la Corte Suprema sostuvo que las personas carecen de una razonable expectativa de privacidad en los números de teléfono que marcan porque "Saben que tienen que transmitir la información numérica en el teléfonoa la empresa", por lo que no se puede "albergar ninguna expectativa general de que la marcación de números telefónicos se mantendrá en secreto."[78] Como he argumentado extensamente en otros lugares, la falta de protección de la Cuarta Enmienda a los registros de terceros le da al gobierno la posibilidad de acceder a una gran cantidad de información personal sin control o mínimamente limitado.[79]

Muchos investigadores se han referido a la recolección de información como una forma de vigilancia. Roger Clarke acuñó un término en inglés, *Dataveillance, (N.de T: unión entre dos palabras, Data y surveillance, dato y vigilancia)* , para referirse al "uso sistemático de los sistemas de datos personales en la investigación o monitoreo de las

acciones o comunicaciones de una o más personas."[80] Christopher Slobogin se ha referido a la recolección de información personal en registros comerciales como "vigilancia de transacciones."[81] La vigilancia puede crear efectos desalentadores sobre la libertad de expresión, la libre asociación y otros derechos esenciales para la democracia cubiertos por la Primera Enmienda.[82] Incluso la vigilancia de las actividades legales pueden inhibir a las personas de participar en ellas. El valor de la protección contra los efectos desalentadores no se mide simplemente centrándose en individuos particulares que son disuadidos de ejercer sus derechos. Los efectos desalentadores perjudican a la sociedad ya que, entre otras cosas, reducen el abanico de pluralidad de opiniones y el grado de libertad con que las personas se dedican a la actividad política.

El argumento de nada que ocultar se centra principalmente en los problemas de recolección de información asociados a los programas de la NSA. A su juicio, la vigilancia limitada de las actividades lícitas provocará daños al comportamiento mínimos que no se pueden equiparar a los beneficios obtenidos en materia de seguridad. Uno puede oponerse a este argumento, pero una de las dificultades más desalentadoras es que es a menudo muy difícil de demostrar evidencias concretas de determinados comportamientos.[83] Una pregunta difícil de responder es si la vigilancia de la NSA y la recolección de registros telefónicos tiene personas disuadidas de comunicar estas ideas particulares.

Con demasiada frecuencia, las discusiones sobre la vigilancia de la NSA y la minería de datos definen el problema sólo en términos de vigilancia. Para volver a mi discusión metáforica, los problemas no son sólo orwellianos, sino kafkianos. Los programas de la NSA son problemáticos aunque no se decubra ninguna información que la gente quiera ocultar. En *El Proceso* de Kafka, el problema no es la inhibición de comportamientos a la cual induce, sino más bien una impotencia y una vulnerabilidad asfixiantes creadas mediante el uso por parte del sistema judicial de los datos personales, y de la exclusión del protagonista para que no tenga ningún conocimiento o participación en el proceso. Los daños son aquellos creados por las burocracias - indiferencia, errores, abusos, la frustración y la falta de transparencia y rendición de cuentas. Uno de esos daños, por ejemplo, el que yo llamo *agregación*, surge a partir de la combinación de pequeños trozos de datos aparentemente inocuos[84]. Cuando se combinan, la información se vuelve mucho más reveladora acerca de una persona. Para la persona que realmente no tiene nada que ocultar, la agregación no es demasiado problema. Pero en la forma más fuerte, menos absoluta, del argumento de nada que ocultar, la gente argumenta que determinados datos no son algo que ellos quisieran ocultar. La agregación, sin embargo, significa que mediante la combinación de piezas de información que a priori no creamos necesario ocultar, el gobierno puede recoger información sobre nosotros que realmente puede ser que deseemos ocultar. Parte del encanto de la minería de datos para el gobierno es su capacidad para revelar una gran cantidad de información acerca de nuestras personalidades y actividades por medio de sofisticados análisis de los datos. Por lo tanto, sin una mayor transparencia, es difícil sostener que programas como el de la minería de datos de la NSA no revelarán información que las personas deseemos ocultar, ya que no sabemos precisamente lo que se revelará. Por otra parte, la minería de datos pretende predecir comportamientos, tratando de pronosticar nuestras acciones futuras. Las personas que coinciden con ciertos perfiles se consideran propensos a involucrarse en un similar patrón de comportamiento. Es muy difícil de refutar

las acciones que uno no ha realizado aún. El no tener nada que ocultar no siempre evita que se hagan predicciones de nuestras actividades futuras.

Otro de los problemas en la taxonomía, que está implicado en el programa de la NSA, es el problema al cual me refiero como *exclusión*.[85] La exclusión es el problema que se produce cuando las personas no tienen conocimiento acerca de cómo su información personal está siendo utilizada, así como se le niega la posibilidad de acceder a dichos datos y corregir posibles errores. El programa de la NSA implica una enorme base de datos de informaciones a la cual las personas no pueden acceder. En efecto, la existencia misma del programa se mantuvo en secreto durante años.[86] Este tipo de procesamiento de la información, que se oculta a la gente e impide su participación, se asemeja en cierto modo a una especie de problema del debido proceso. Es un problema estructural que involucra la forma en que las personas son tratadas por parte de las instituciones gubernamentales. Además, crea un desequilibrio de poder entre los individuos y el gobierno. ¿Hasta qué punto deben el Poder Ejecutivo y una agencia como la NSA, que está relativamente aislada del proceso político y la rendición pública de cuentas, tener un poder significativo sobre los ciudadanos? Esta cuestión no es si la información obtenida es algo que la gente quiere ocultar, sino más bien sobre el poder y la estructura de gobierno.

Un problema relacionado es el "uso secundario". El uso secundario es el uso de los datos obtenidos originalmente para un propósito con otro fin diferente, no relacionado con el primero, sin el consentimiento de la persona, El gobierno ha dicho poco acerca del tiempo durante el cual los datos se almacenan, cómo se usan, y cómo podrían usarse en el futuro. Los potenciales usos futuros de cualquier pieza de información personal son muy amplios, y sin límites ni rendición de cuentas sobre cómo se usa esta información, es muy difícil para las personas evaluar los peligros de que los datos estén bajo control del gobierno. Por lo tanto, el problema con el argumento de nada que ocultar es que se se centra exclusivamente en uno o dos tipos particulares de problemas de privacidad -la divulgación de información personal y la vigilancia- y no otros. Asume un punto de vista particular sobre lo que implica la intimidad, y establece los términos para el debate de una manera que a menudo es improductiva.

Es importante distinguir aquí entre dos maneras de justificar un programa tal como el programa de vigilancia y minería de datos de la NSA. La primera consiste en no reconocer un problema. Así es como obra el argumento de nada que ocultar. La segunda manera de justificar tal programa es reconocer los problemas, pero sostener que los beneficios superan a los daños a la privacidad. La primera justificación influye en la segunda, debido a que el bajo valor dado a la intimidad se basa en una visión estrecha del problema. El malentendido fundamental es que el argumento de nada que ocultar percibe a la privacidad de un modo particular -como una forma de secreto, como el derecho a ocultar cosas. Pero hay muchos otros tipos de daños distintos que los involucrados por la exposición de nuestros secretos al gobierno. Los problemas de privacidad son muchas veces difíciles de reconocer y reparar porque crean una abanico de nuevos tipos de daños. Los tribunales, los legisladores, y demás se enfocan en determinados tipos de daños y excluyen los otros, y sus miradas están cegadas a estos últimos.

B. Comprendiendo los problemas estructurales

Una de las dificultades con el argumento de nada que ocultar es que se busca un tipo de injuria visceral en lugar de una estructural. Irónicamente, esta concepción subyacente de la injuria es compartida por ambas posiciones, tanto por aquellos que abogan por una mayor protección de la privacidad como por aquellos que argumentan a favor de los intereses en conflicto a la privacidad. Por ejemplo, el profesor de derecho Ann Bartow argumenta que no he podido describir los daños a la privacidad de una manera convincente en mi artículo, *Una taxonomía de la Privacidad*, donde ofrezco un marco para la comprensión de los múltiples problemas relacionados con la privacidad.[87]

El desacuerdo principal de Bartow es que mi taxonomía de la privacidad "encuadra muy drásticamente a la privacidad, no la logra identificar suficientemente y trata de persuadir que las violaciones de privacidad pueden afectar negativamente la vida que vivimos, la vida de los seres humanos más allá de provocar unos simples sentimientos de inquietud."[88] Bartow le reclama a la taxonomía que no tiene "suficientes cadáveres", y que "carece de sangre y muerte, o al menos de huesos rotos y dinero ilícito, la privacidad está alejada de las categorías legales de daños"[89]

La mayoría de los problemas de privacidad carece de cadáveres. Por supuesto, hay casos excepcionales, tales como los asesinatos de Rebecca Shaeffer y Amy Boyer. Rebecca Shaeffer era actriz asesinada por un acosador que obtuvo su domicilio de un registro del Departamento de Vehículos Motorizados.[90] Este incidente hizo que el Congreso aprobara la ley de privacidad de los conductores en 1994.[91] Amy Boyer fue asesinada por un acosador que obtuvo sus datos personales, incluyendo su dirección de trabajo y su número de Seguridad Social, a partir de una base de datos de una empresa.[92] Dejando de lado estos ejemplos, no hay mucha muerte y sangre derramada en la ley de privacidad. Si este es el estándar para reconocer un problema, entonces pocos problemas de privacidad serán reconocido. Los casos horribles no son típicos, y el propósito de mi taxonomía es explicar por qué la mayoría de los problemas de privacidad siguen siendo perjudiciales a pesar de este hecho.

La objeción de Bartow es en realidad muy similar al argumento de nada que ocultar. Aquellos que apoyan al argumento de nada que ocultar tienen en mente un tipo particular de daño visceral a la privacidad, en donde es violada sólo cuando se produce un descrédito o algo profundamente embarazoso.

La búsqueda por parte de Bartow de historias de horror representa un deseo similar de encontrar daños viscerales a la privacidad. El problema es que no todos los daños a la privacidad son de este tipo. Al final del día, la privacidad no es una película de terror, y en muchos casos será más difícil hallar daños más palpables. Sin embargo, todavía existirán daños para abordar, aunque no sean sensacionalistas.

En muchos casos, la privacidad no se ve amenazada por algún acto atroz en particular sino por una lenta serie de actos relativamente menores que poco a poco comienzan a tener sentido. De esta manera, los problemas de privacidad se asemejan a ciertos daños medioambientales que se producen con el tiempo a través de una serie de pequeños actos sucesivos. Bartow quiere apuntar a un derrame importante, pero la contaminación gradual por una multitud de diferentes agentes a menudo crea problemas peores.

La ley frecuentemente se enfrenta a ciertos tipos de daños y no considera la

vergüenza, la humillación, ni la integridad física o psicológica.[93] Por ejemplo, después del 11 de septiembre, varias aerolíneas entregaron sus registros de pasajeros a las agencias federales en directa violación de sus políticas de privacidad. Las agencias federales utilizaron los datos para estudiar la seguridad de las aerolíneas.[94] Un grupo de pasajeros demandó a Northwest Airlines por revelar su información personal. Afirmaban que había incumplimiento de contrato por parte de Northwest Airlines. En el caso Dyer vs Northwest Airlines Corp., el tribunal rechazó el reclamo porque "las amplias declaraciones de políticas de la empresa en general, no dan lugar a reclamaciones contractuales", los pasajeros nunca basaron sus reclamos en dichas políticas, ni siquiera las leyeronleerlo, y que "no se pueden alegar daños contractuales que se deriven de la supuesta violación"[95]. Otro tribunal llegó a una conclusión similar.[96]

Independientemente de las considerandos de las decisiones sobre el derecho contractual, los casos muestran una dificultad en el sistema legal para resolver los problemas de privacidad. La divulgación de los registros de pasajeros representó una "violación de confidencialidad."[97] Los problemas causados oor la violación de la confidencialidad no consisten sólo en la angustia emocional individual que provocan, sino que implican una violación de la confianza dentro de una relación. El asegurarse que las promesas se cumplan y que la confianza se mantenga en las relaciones entre las empresas y sus clientes es un valor social muy importante. También queda implicado el problema del uso secundario.[98] Los datos recogidos con un propósito han sido usados para un fin distinto sin el consentimiento de las personas. Las líneas aéreas dieron información de sus pasajeros al gobierno con un propósito totalmente diferente más allá de aquel para el que fue originalmente reunida. Los problemas de uso secundarios no causan con frecuencia daños financieros, ni tampoco psicológicos. En cambio, el daño es el abuso de poder. En el caso Dyer, los datos fueron difundidos en una forma que ignora los intereses de los pasajeros a pesar de las promesas hechas en la política de privacidad. Aunque los pasajeros no estaban al tanto de la política, es un valor social importante el garantizar que las empresas cumplan con los límites establecidos en la forma en que utilizan la información personal. De lo contrario, los límites establecidos pierden su sentido, y las empresas pueden disponer silenciosa e ilimitadamente de los datos. Tal estado de cosas mantiene a casi todos los consumidores en una posición de debilidad. Eldaño, entonces, no afecta tanto a los individuos en particular, es mas bien un daño estructural.

Un problema similar aparece en otro caso, Smith vs Chase Manhattan Bank.[99] Un grupo de querellantes demandó al Chase Manhattan Bank por la venta de información de clientes a terceros violando su política de privacidad, según la cual la información se mantendría confidencial. El tribunal sostuvo que incluso presumiendo estas acusaciones como ciertas, los demandantes no podrían demostrar ningún daño real:

[El] "daño" en el corazón de esta pretendida demanda colectiva, es que los miembros del grupo ofrecen, únicamente, productos y servicios que ellos eran libres de rechazar. Esto no se puede considerar como un daño real.

La demanda no alega ningún caso en que el demandante nombrado o cualquier miembro de la clase haya sufrido ningún daño real debido a la recepción de una solicitud telefónica no deseada o correspondencia basura.[100]

La opinión de la corte acerca del daño, sin embargo, no tuvo en cuenta el incumplimiento dela confidencialidad.

Cuando se contraponen la privacidad y la seguridad, los daños a la privacidad a menudo se caracterizan en términos de daños a individuos, y el interés en la seguridad se caracteriza a menudo en un marco social más amplio. El interés en la seguridad en los programas de la NSA a menudo ha sido definido incorrectamente. En una Audiencia en el Congreso, el fiscal general Alberto Gonzales declaró:

Nuestro enemigos están escuchando, y no puedo evitar preguntarme si no estarán moviendo sus cabezas incrédulamente, asombrados de pensar que alguien pondría en peligro este programa sensible al filtrar su existencia en primer lugar, y sonriendo ante la posibilidad de revelar algo más o tal vez incluso de que se nos quite de manera unilateral una herramienta clave en la guerra contra el terror.[101]

El equilibrio entre la privacidad y la seguridad a menudo se formula en términos de la prescripción o no de una actividad concreta de recolección de información por parte del gobierno.

La cuestión, sin embargo, no es si a menudo la NSA u otros organismos del gobierno deben ser autorizados para reunir cierto tipo particular de información, sino que es qué tipo de supervisión y rendición de cuentas debe cumplir el gobierno cuando se dedica a registros e incautaciones. El gobierno puede emplear casi cualquier tipo de actividad investigadora con una orden de apoyo de una causa probable. Este es un mecanismo de supervisión -que obliga a los funcionarios del gobierno a justificar sus sospechas ante un juez o magistrado neutral antes de emplear estas tácticas. Por ejemplo, la ley de vigilancia electrónica permite las escuchas telefónicas, pero limita la práctica con supervisión judicial, los procedimientos para reducir al mínimo la amplitud de las escuchas y los requisitos que los funcionarios encargados de hacer cumplir la ley reportan a la corte para evitar abusos.[102] Son estos procedimientos que la Administración de Bush ha ignorado al realizar la NSA tareas de vigilancia sin orden judicial. La pregunta no es si queremos que el gobierno monitoree las conversaciones de este tipo, pero sí que el Poder Ejecutivo debería adherirse a los procedimientos de control adecuados que el Congreso ha promulgado como ley, o de forma encubierta debería ignorar cualquier descuido.

Por lo tanto, el interés en la seguridad no debe estar totalmente en contra de los intereses de la privacidad. Más bien, lo que se debe sopesar es el grado de limitación marginal sobre la eficacia de la recolección de información gubernamental o del programa de minería de datos mediante la imposición de supervisión judicial y procedimientos de minimización. Sólo en los casos en que tales procedimientos pongan completamente en peligro al programa de gobierno, entonces el interés de la seguridad debe ser prioritario, más que en la diferencia marginal entre un programa no comprometido frente a uno limitado.

Con demasiada frecuencia, la ponderación de los intereses privados contra los intereses de la seguridad se lleva a cabo de una manera que defrauda seriamente a la privacidad al exagerar los intereses de seguridad. Tal es la lógica del argumento de nada que

ocultar. Cuando se analiza el argumento, y se examinan y cuestionan sus supuestos subyacentes, podemos ver cómo se traslada el debate a sus términos, en el que obtiene su injusta ventaja. Es el momento de correr el velo al argumento de nada que ocultar.

V. CONCLUSIÓN

Ya sea en forma explícita o no, las concepciones de la vida privada sustentan casi todos los argumentos acerca de la privacidad, incluso la ocurrencia común de "no tengo nada que ocultar". Como he tratado de demostrar en este ensayo, la comprensión de la privacidad como una concepción pluralista revela que estamos hablando muchas veces pasado entre sí cuando se habla de temas de privacidad. Al centrarse más específicamente sobre los problemas relacionados bajo el sello de "privacidad", podemos enfocarnos mejor en cada problema en lugar de ignorarlos o confundirlos. El argumento de nada que ocultar se refiere a ciertos problemas, pero ignora otros. Presenta una visión singular y estrecha de concebir la vida privada, y triunfa al excluir de su consideración a otros problemas que plantea a menudo la vigilancia del gobierno y los programas de minería de datos. Cuando se enuncia de manera directa, el argumento de nada que ocultar puede atraparnos, porque obliga a centrar el debate en su estrecha comprensión de la privacidad. Pero cuando se enfrenta con la pluralidad de problemas de privacidad implicados por la recolección de datos del gobierno y su uso más allá de la vigilancia y la divulgación, es el final del argumento de nada que ocultar, no tiene nada que decir.

* Daniel J. Solove 2007. Profesor Asociado, Escuela de Leyes, Universidad George Washington; J.D., Escuela de Leyes de Yale.

1. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts: Secret Order to Widen Domestic Monitoring*, N.Y. TIMES, Dec. 16, 2005, en A1.

2. John Markoff, *Pentagon Plans a Computer System That Would Peek at Personal Data of Americans, N.Y. TIMES*, Nov. 9, 2002, en A12.

3. John M. Poindexter, *Finding the Face of Terror in Data*, N.Y. TIMES, Sept. 10, 2003, en A25.

4. DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 169 (2004).

5. Shane Harris, *TIA Lives On*, NAT'L J., Feb. 25, 2006, en 66.

6. Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, en A1; Susan Page, *Lawmakers: NSA Database Incomplete*, USA TODAY, June 30, 2006, en A1.

7. Cauley, cita anterior6, en A1.

8. Eric Lichtblau & James Risen, *Bank Data Sifted in Secret by U.S. to Block Terror*, N.Y. TIMES, June 23, 2006, en A1.

9. Ver texto al pie que acompaña las notas 12–33.

10. Bruce Schneier, Comentario, *The Eternal Value of Privacy*, WIRED, May 18, 2006, http://www.wired.com/news/columns/1,70886-0.html.

11. Geoffrey R. Stone, *Commentary, Freedom and Public Responsibility*, CHI. TRIB., May 21, 2006, en 11.

12. JEFFREY ROSEN, THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE (2004).

13. Id. a 36.

14. Comentario de NonCryBaby en http://www.securityfocus.com/comments/articles/2296/18105/threaded (Feb. 12, 2003).

15. Comentario de Yoven en http://www.danielpipes.org/comments/47675 (June 14, 2006, 14:03EST).

16. Reach For The Stars!, http://greatcarrieoakey.blogspot.com/2006/05/look-all- you-want-ive-got-nothing-to.html (May 14, 2006, 09:04 PST).

17. Comentario de annegb en Concurring Opinions, http://www.concurringopinions.com/archives/2006/05/is_there_a_good.html#comments (May 23, 2006, 11:37 EST).

18. Joe Schneider, *Letter to the Editor, NSA Wiretaps Necessary*, ST. PAUL PIONEER PRESS, Aug. 24, 2006, EN 11B.

19. Polls Suggest Americans Approve NSA Monitoring (NPR radio broadcast, May 19, 2006), disponible en 2006 WLNR 22949347.

20. HENRY JAMES, THE REVERBERATOR (1888), reimpreso en NOVELS 1886–1880, en 555, 687 (1989).

21. Concurring Opinions, cita anterior17 (May 23, 2006, 00:06 EST).

22. Comentario de Adam en Concurring Opinions, cita anterior 17 (May 23, 2006, 16:27 EST).

23. Comentario de Dissent en Concurring Opinions, cita anterior 17 (May 24, 2006, 07:48 EST).

24. Comentario de Ian a Concurring Opinions, cita anterior 17 (May 24, 2006, 19:51 EST).

25. Comentario de Matthew Graybosch en Concurring Opinions, cita anterior 17 (Oct.16, 2006, 12:09 EST).

26. Comentario de Neureaux en Concurring Opinions, cita anterior 17 (Oct. 16, 2006, 14:39 EST).

27. Comentario de Catter en Concurring Opinions, cita anterior 17 (Oct. 16, 2006, 11:36 PM EST).

28. Comentario de Kevin en Concurring Opinions, cita anterior 17 (July 24, 2006, 12:36 EST).

29. ALEKSANDR SOLZHENITSYN, CANCER WARD 192 (Nicholas Bethell & David Burg trans., Noonday Press 1991) (1968).

30. FRIEDRICH DÜRRENMATT, TRAPS 23 (Richard & Clara Winston trans., 1960).

31. Comentario de Andrew en Concurring Opinions, cita anterior 17 (Oct. 16, 2006, 15:06 EST).

32. David H. Flaherty, *Visions of Privacy: Past, Present*, *and Future*, en VISIONS PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE 19, 31 (Colin J. Bennett & Rebecca Grant eds., 1999).

33. Comentario de BJ Horn en Concurring Opinions, cita anterior 17 (June 2, 2006, 18:58 EST).

34. RICHARD A. POSNER, THE ECONOMICS OF JUSTICE 271 (1983).

35. RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 46 (5th ed. 1998).

36. Id.

37. Richard A. Posner, *Our Domestic Intelligence Crisis,* WASH. POST, Dec. 21, 2005, en A31.

38. Comentario de MJ en Concurring Opinions, cita anterior 17 (May 23, 2006, 17:30 EST).

39. ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS AND DOSSIERS 25 (1971).

40. Hyman Gross, *The Concept of Privacy*, 42 N.Y.U. L. REV. 34, 35 (1967).

41. COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 25 (1992).

42. Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2087 (2001).

43. Judith Jarvis Thomson, *The Right to Privacy*, in PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 272, 272 (Ferdinand David Schoeman ed., 1984).

44. Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1095–99 (2002).

45. JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION 56 (1992).

46. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890)

47. Solove, cita anterior 44, en 1099–1124.

48. LUDWIG WITTGENSTEIN, PHILOSOPHICAL INVESTIGATIONS § 65 (G.E.M. Anscombe trans., 3d ed. 2001).

49. Id. § 66.

50. SOLOVE, nota anterior 4, en 6–9.

51. GEORGE ORWELL, 1984 (Signet Classic 1984) (1949); SOLOVE, cita anterior 4, en 7.

52. FRANZ KAFKA, THE TRIAL 50–58 (Willa & Edwin Muir trans., Random House 1956) (1937); SOLOVE, cita anterior 4, en 8–9.

53. SOLOVE, nota anterior 4, en 27–75.

54. JOHN DEWEY, LOGIC: THE THEORY OF INQUIRY 112 (Jo Ann Boydston ed. 1991) (1938).

55. Id.

56. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).

57. Id. en 516–20.

58. Id. en 522–25.

59. CASS R. SUNSTEIN, LEGAL REASONING AND POLITICAL CONFLICT 67 (1996).

60. THOMAS I. EMERSON, THE SYSTEM OF FREEDOM OF EXPRESSION 545, 549 (1970).

61. Smith vs. City of Artesia, 772 P.2d 373, 376 (N.M. Ct. App. 1989).

62. Charles Fried, Privacy, 77 YALE L.J. 475, 478 (1968); véase también INNESS, cita anterior 45, en 95 ("[La] privacidad es importante porque reconoce nuestro respeto a las personas como seres autónomos, con capacidad para amar, cuidar y demás -en otras palabras, personas con la posibilidad de establecer libremente relaciones."); BEATE RÖSSLER, THE VALUE OF PRIVACY 117 (R.D.V. Glasgow trans., Polity Press 2005) (2001) ("El respeto de la vida privada de una persona es el respeto por ella como un sujeto autónomo ."); Stanley I. Benn, *Privacy, Freedom, and Respect for Persons*, en NOMOS XIII: PRIVACY 1, 26 (J. Roland Pennock & John W. Chapman eds., 1971) ("[El] respeto por alguien como una persona, como un elector, implica respeto por él como una especie de emprendimiento auto-creativo, que podría ser interrumpido, distorsionado, o incluso frustrado cuando se ve limitado por alguna intrusión. ").

63. Smith, 772 P.2d en 376.

64. AMITAI ETZIONI, THE LIMITS OF PRIVACY 196 (1999).

65. Id. en 187–88.

66. Id. en 38.

67. Id. en 187–88.

68. Id. en 198.

69. JOHN DEWEY, ETHICS (1908), reimpreso en 5 THE MIDDLE WORKS: 1899–1924, en 268 (Jo Ann Boydston ed., S. Ill. Univ. Press 1978).

70. JOHN DEWEY, LIBERALISM AND CIVIL LIBERTIES (1936), reimpreso en 11 THE LATER WORKS, 1935–1937, en 373 (Jo Ann Boydston ed., S. Ill. Univ. Press 1987).

71. Id. en 375.

72. Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 968 (1989).

73. Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 709 (1987). En el análisis de los problemas de la formulación de políticas legislativas federales sobre privacidad, Priscilla Regan demuestra la necesidad de pensar la privacidad en términos de sus beneficios sociales. Véase PRISCILLA M. REGAN, LEGISLATING PRIVACY, en xiv (1995) ("[El] análisis de la formulación de políticas del Congreso revela que se prestó poca atención a la posibilidad de darle mayor importancia social a la vida privada.").

74. Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1427–28 (2000) ("La privacidad de la información, en definitiva, es un elemento constitutivo de la sociedad civil en el sentido más amplio del término."); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1613 (1999) ("[La] privacidad de la información se concibe mejor como un elemento constitutivo de la sociedad civil."); ver también Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 455 (1980) ("La privacidad es también esencial para el gobierno democrático, ya que fomenta y promueve la autonomía moral del ciudadano, un requisito fundamental de una democracia.").

75. Schneier, scita anterior 10.

76. United States vs. Katz, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).

77. 425 U.S. 435, 442 (1976).

78. 442 U.S. 735, 743 (1979).

79. SOLOVE, cita anterior 4, en 165–209; véase también Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1117–37 (2002).

80. Roger Clarke, *Information Technology and Dataveillance*, 31 COMM. OF THE ACM 498, 499

(1988); véase también Roger Clarke, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*, AUSTRALIAN NATIONAL UNIVERSITY, Aug. 7, 2006, http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html.

81. Christopher Slobogin, *Transaction Surveillance by the Government*, 75 MISS. L.J. 139, 140 (2005).

82. Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 154–59 (2007).

83. Id.

84. Solove, cita anterior 56, en 506–11.

85. Id. en 522–25

86. Risen & Lichtblau, cita anterior 1.

87. Ann Bartow, *A Feeling of Unease About Privacy Law*, 155 U. PA. L. REV. PENNumbra 52, 52 (2006), http://www.pennumbra.com/issues/articles/154-3/Bartow.pdf.

88. Id.

89. Id. en 52, 62.

90. SOLOVE, cita anterior 4, en 147.

91. Id.

92. Remsburg vs. Docusearch, Inc., 816 A.2d 1001, 1005–06 (N.H. 2003).

93. SOLOVE, cita anterior 4, en 93–97, 100–01, 195–208; Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1228 (2003).

94. SOLOVE, cita anterior 4, en 93.

95. 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004).

96. *In re* Nw. Airlines Privacy Litig., No. 04-126, 2004 WL 1278459 (D. Minn. June 6, 2004).

97. Solove, nota anterior 56, en 526–30.

98. id en 520–22.

99. 741 N.Y.S.2d 100 (N.Y. App. Div. 2002).

100. Id en 102.

101. *Wartime Executive Power and the National Security Agency's Surveillance Authority: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. 15 (2006) (declaración de, Att'y Gen. of the United States).

102. Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 775–76 (2005).