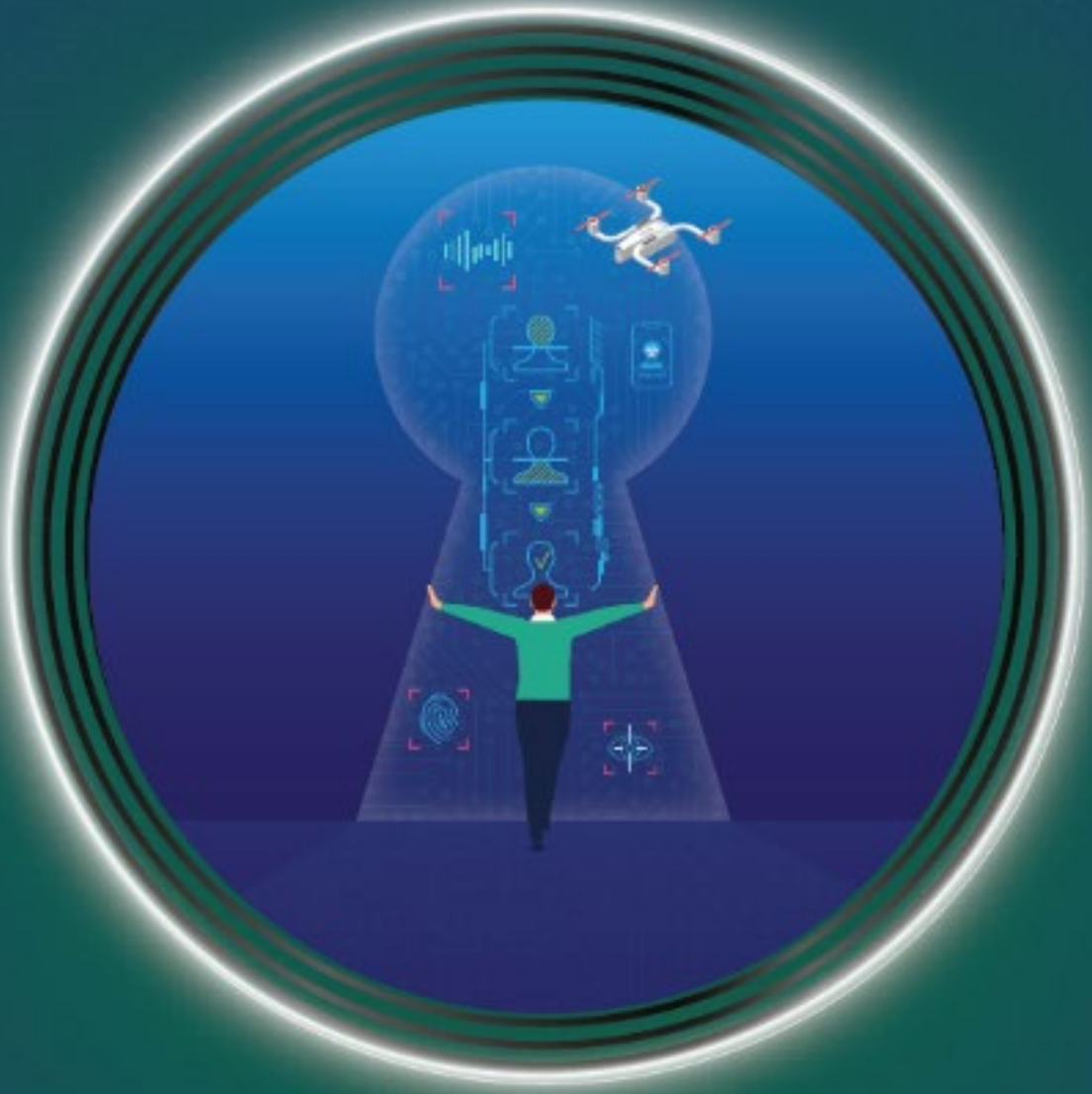
Deloitte. Insights

Un reporte del
Deloitte Center for Financial Services



Re-imaginando la privacidad del cliente para la era digital

Ir más allá del cumplimiento en servicios financieros

Contenidos

Cada vez más inteligentes acerca de la privacidad

"Las nuevas tecnologías están radicalmente avanzando nuestras libertadas, pero también están facilitando invasiones sin paralelo de la privacidad."[1]

- Electronic Frontier Foundation

La privacidad del cliente se ha vuelto un tema crecientemente complejo y polémico, dado que han proliferado herramientas y tecnologías que capturan datos acerca de cada faceta de nuestras vidas. Muchos consumidores ahora consideran que ya no tienen control de la información acerca de sí mismos[2] y están comenzando a prestar atención estrecha a cómo es recaudada la información acerca de ellos.

Tales preocupaciones también están impactando la industria de servicios financieros, donde los datos del cliente siempre han sido un activo central. Mucho antes que los datos se convirtieran en el combustible que alimenta la economía digital, las instituciones financieras han salvaguardado la información privada del cliente y han usado estos datos a niveles macro y micro para servir a los clientes.

A la luz de desarrollos regulatorios recientes, tales como la General Data Protection Regulation (GDPR) [regulación general de protección de datos] en la Unión Europea, y los avances en la tecnología, la privacidad del cliente se está volviendo un desafío aún más intrincado – para los individuos cuya información está en juego, para las compañías que se espera protejan esta información y también la usen responsablemente, y para los reguladores encargados de la defensa del consumidor que se están poniendo al día.

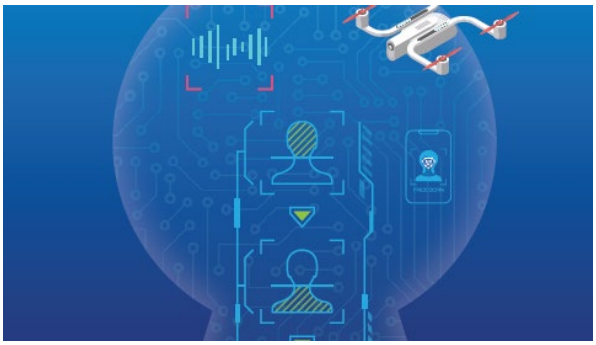
Muchos reguladores en todo el mundo están tomando interés sin precedentes en la privacidad.

De hecho, muchos reguladores en todo el mundo están tomando interés sin precedentes en la privacidad y han comenzado a establecer reglas nuevas. La GDPR es posiblemente el más notable de los últimos desarrollos, ofreciendo a los ciudadanos de la Unión Europea protecciones profundas para sus datos personales. Según la GDPR, todas las compañías que manejan información del consumidor de la Unión Europea – incluyendo las instituciones financieras – tienen que obtener consentimiento expreso de aceptación para recaudar sus datos y notificar prontamente a los ciudadanos sobre las violaciones de datos, o correr el riesgo de pagar fuertes multas. Los consumidores también tienen el "derecho a ser olvidados," una estipulación que requiere que, a partir de solicitud, las compañías borren todos los datos personales actualmente mantenidos, o si los datos ya no sirven al propósito original del negocio.[3]

Los Estados Unidos, mientras tanto, no tienen una regla que lo abarque todo como la GDPR. Las regulaciones federales de los Estados Unidos tienen a ser de alcance más estrecho y en general solo protegen tipos específicos de datos o son específicas para sector/industria (vea el Apéndice en la página 15 para un resumen de las leyes federales sobre privacidad financiera).

Algunos grupos comerciales, tales como la Association of National Advertisers[4] y la Internet Association[5] han comenzado a defender una ley federal de privacidad que lo abarque todo como la SGPR para evitar tener una legislación por parches. Los cabildantes, también, están comenzando a hablar. En el año 2018, la US Chamber of Commerce le pidió al Congreso que adopte una estructura federal de privacidad "para proporcionar certeza y consistencia a consumidores y negocios por igual."[6]

Mientras tanto, la cadera de un solo mandato federal ha colocado la responsabilidad en los estados para que diseñen sus propias políticas de privacidad. Por ejemplo, en el verano de 2018 California aprobó la Consumer Privacy Act, otorgándoles a los consumidores control profundo de todas las formas de sus datos personales[7] desde los identificadores tradicionales tales como direcciones y números de teléfono, hasta fuentes no-tradicionales de datos tales como "me gusta" en medios de comunicación social o interacciones con asistentes personales. Otros estados, tales como Delaware[8] y Vermont,[9] recientemente promulgaron sus propias leyes de privacidad. En la medida en que los consumidores demanden más control de sus datos personales, incluso si muchos puedan no estar familiarizados con las regulaciones existentes sobre privacidad, más estados seguirán su ejemplo.[10]



La rápida penetración de las tecnologías digitales en casi toda esfera de la vida ha revelado cómo las protecciones de privacidad concebidas para la era análoga hoy son fundamentalmente limitadas.

Agregando a esta incertidumbre regulatoria, las innovaciones digitales de hoy también están remodelando la noción de privacidad de maneras inesperadas. La rápida penetración de las tecnologías digitales en casi toda esfera de la vida ha revelado cómo las protecciones de privacidad concebidas para la era análoga hoy son fundamentalmente limitadas.[11] Nuestras ideas acerca de la privacidad – qué información debe ser considerada privada y qué se debe hacer para proteger la privacidad de uno – están evolucionando rápidamente con las nuevas tecnologías y con los nuevos datos que ellas generan.

Esta situación es adicionalmente exacerbada por el hecho de que la privacidad no tiene una definición única, universal. De hecho, varios académicos de la privacidad han observado que la verdadera idea de privacidad hoy es "un concepto en desorden,"[12] "vergonzosamente difícil de definir,"[13] y "un concepto esencialmente disputado."[14] Este desafío se debe, en parte, al hecho de que la privacidad no es solo un valor social y "un bien a ser logrado," sino también un derecho, con ramificaciones legales.

También hay debate acerca de la privacidad de los datos (*¿De quién son los datos?*) y de administración de los datos (*¿Quién debe salvaguardar mejor los datos del cliente?*).[15] Ambos de esos desafíos no tienen respuestas fáciles.

Uno solo puede imaginar la amplitud y la complejidad de los problemas de privacidad que pueden ser enfrentados desde hace una década, cuando la mayoría de las interacciones humanas, incluso las que ahora se consideran privadas, podían estar expuestas a que otros las recauden, minen, y compartan. Además, ¿ la privacidad podría convertirse en un "lujo," tal y como se discutió durante un panel en la reunión anual del World Economic Forum?[16]

Administrar la privacidad en este mundo cada vez más centrado-en-datos podría requerir pensamiento nuevo. En este reporte, discutiremos los siguientes acertijos:

- ¿Qué deben hacer las firmas de servicios financieros para re-imaginar la privacidad en esta era digital rápidamente cambiante?
- ¿Cómo pueden las instituciones aprovechar las nuevas fuentes de datos y las tecnologías emergentes para beneficiar tanto a cliente como a proveedores de servicio sin entrar en conflicto con las regulaciones sobre la privacidad u ofender las sensibilidades del consumidor?
- ¿Cómo las compañías deben ir más allá del cumplimiento para hacer de la administración de la privacidad un diferenciador competitivo?

En este reporte discutimos con detalle esas preguntas y otros desafíos.

Una nueva estructura para entender hoy la privacidad

La industria probablemente necesitará una estructura más robusta, expansiva, pragmática, y prospectiva para navegar exitosamente el panorama cambiante de la privacidad. Esta estructura debe ser tanto táctica como estratégica – una que soportaría la prueba del tiempo y continuaría adaptándose a futuras innovaciones tecnológicas.[17]

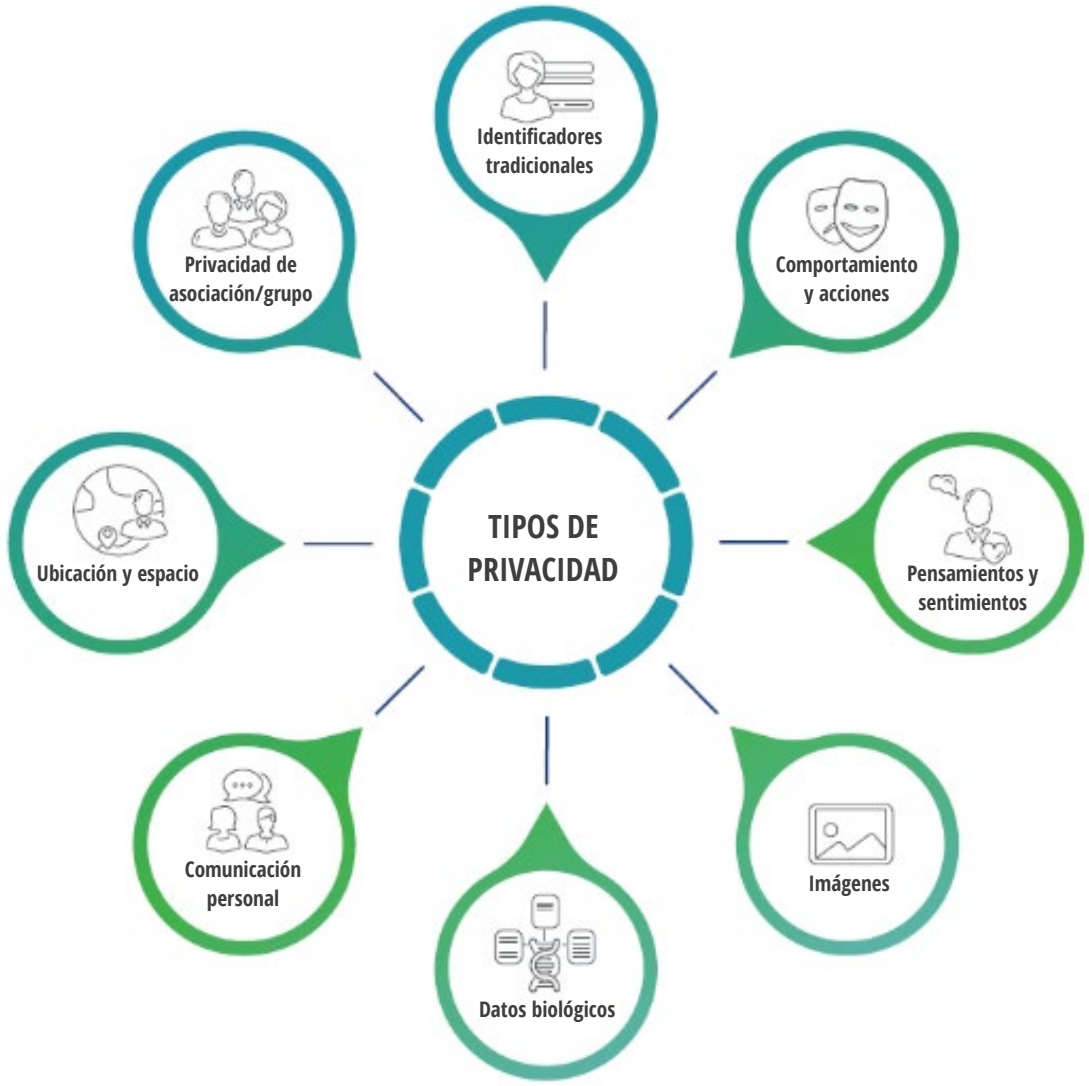
La estructura que se presenta adelante fue inspirada por el trabajo de tres investigadores - Rachel L. Finn, David Wright, y Michael Friedewald

– quienes identificaron siete tipos de privacidad – que varían desde *privacidad de ubicación hasta privacidad de asociación*. Para este reporte, nosotros modificamos y ampliamos su tipología para abarcar problemas relevantes de privacidad que la industria de servicios financieros actualmente enfrenta (figura 1). La Figura 2 ofrece explicaciones más detalladas de esos ocho tipos.

Esas ocho categorías resaltan la multi-dimensionalidad de la privacidad hoy. Subrayan la importancia de que los líderes de servicios financieros piensen de manera diferente, y más expansivamente, acerca de cómo sus organizaciones recaudan, almacenan, procesan, comparten, y protegen la información.

FIGURA 1

Los ocho tipos de privacidad



Fuente: Los ocho tipos de privacidad, de Deloitte se basan en el trabajo de Rachel R. Finn, David Wright, and Michael Friedewald, "Seven types of privacy" in Serge Gutwirth, Ronald Leenes, Paul de Hert, and Yves Poullet (eds), *European Data Protection: Coming of Age* (Dordrecht: Springer, 2013). Los autores postularon siete tipos de privacidad, pero nosotros modificamos su estructura para hacerla más relevante para los servicios financieros mediante modificar "datos e imágenes" para solo imágenes, y separando "privacidad de la persona" entre "identificadores tradicionales" y "datos biológicos."

Tome, por ejemplo, el uso de datos biométricos, tales como reconocimiento facial, de voz, y de iris para la identificación en servicios financieros.[18] Los datos provenientes de esas tecnologías podrían ser combinados con otra información personal, tal como ubicación o publicaciones en medios de comunicación social, para descifrar las necesidades y preferencias de un individuo por servicios financieros. En un contexto de privacidad, ¿cuáles son las expectativas en relación con el uso de tales datos? ¿Los consumidores necesitan ser informados de que está ocurriendo la fusión de fuentes privadas de información, y cómo este perfil combinado puede ser usado para servirles?

Tal examen no sería posible sin un entendimiento más rico, más matizado, de la privacidad para el mundo digital de hoy.

FIGURA 2

Entendimiento de los ocho tipos de privacidad

Identificadores tradicionales	Cualquier información estándar/tradicional personalmente identificable, incluyendo datos geográficos – tales como nombre, dirección, fecha de nacimiento, raza, género, y número de seguridad social – que la industria rutinariamente ha recaudado.
Comportamiento y acciones	Comportamientos tenidos en espacios públicos, semipúblicos, o privados – tales como compra, transacciones financieras, compra de productos financieros, hábitos de navegación en la red, y otros comportamientos fuera de la relación financiera.
Pensamientos y sentimientos	Opiniones de los clientes sobre una variedad de temas, incluyendo los expresados acerca de compañías o marcas; también conocidas en mercadeo como *sicográficas*.
Imágenes	Imágenes tomadas por individuos, aviones/drones, satélites, y dispositivos robóticos, en espacios privados o públicos.
Datos biológicos	Funciones corporales y características, incluyendo características físicas (tales como características faciales, iris, voz, y modo de andar), salud física y sicológica, y código genético.
Comunicación personal	Comunicaciones entre el cliente y la institución financiera y otras entidades – vía correo electrónico, mensajes de texto, medios de comunicación social, y teléfono – así como comportamiento de navegación en la red vía cookies.
Ubicación y espacio	Información acerca de la ubicación geográfica o de una persona o de una propiedad.
Privacidad de asociación/grupo	Grupos y subgrupos a los cuales el cliente pertenece o está asociado, incluyendo afiliaciones políticas, pasatiempos personales, grupos relacionados con el trabajo, y grupos religiosos.

Fuente: Deloitte Center for Financial Services.

Implicaciones de la privacidad para las tecnologías emergentes

Las nuevas fuentes de datos deben ser aprovechadas con cautela

En los últimos años, se espera que las instituciones financieras crecientemente usen las tecnologías cambiantes para servir a sus clientes, aprovechando asistentes virtuales, sensores personales y comerciales, y drones, en además de las actividades que ya son comunes, tales como revisar la navegación en la red y la actividad en los medios de comunicación social.

Un enorme desafío para las compañías es cómo optimizar el uso de todos los datos generados por las tecnologías legadas y heredadas al tiempo que permanecen dentro de las fronteras de las regulaciones de la privacidad.

En muchos casos, los clientes son conscientes de que sus datos personales están siendo recaudados – por ejemplo, cuando los propietarios de vehículos acuerdan permitir que los aseguradores monitoreen telemáticamente su modo de conducción en intercambio por descuentos en las primas de seguros de automóviles. Pero otros tipos de recaudo directo de datos y cómo tal información es usada puede no ser tan obvio para los consumidores. Esto es parcialmente porque las políticas estándar de privacidad usualmente emplean lenguaje legalista y no ofrecen muchos detalles, tales como si las compañías usarán cookies para hacer seguimiento de la navegación en la red o verificar los medios de comunicación social por inclinaciones comportamentales cuando se valore el riesgo de crédito de un cliente.[19]

¿Los clientes de administración de inversiones estarían de acuerdo si su firma asesora escanea sus publicaciones en medios de comunicación social, información de geolocalización, o historia de navegación en la red para determinar su interés en inversiones socialmente responsables, con base en los datos recaudados acerca de su trabajo de caridad o una aparición en una manifestación que protesta contra combustibles sólidos? ¿Se sentirían incómodos si su asesor de inversión conoció que navegaban sitios web astrológicos antes de tomar decisiones financieras? ¿Les importaría a los clientes de tarjetas de crédito si sus bancos revisaran sus patrones de gasto con billeteras inteligentes para detectar si a menudo van a casinos y pistas de carreras? Preocupaciones adicionales por la privacidad pueden surgir si las firmas de servicios financieros venden datos del cliente a terceros – datos de salud personal proveniente de un monitor portátil, por ejemplo. En tales casos, los consumidores pueden no ser conscientes de la extensión de la minería de datos para que ello califique como "consentimiento informado."

También, tal y como se observó antes, podemos ver más casos en que consumidores y defensores de la privacidad insisten en el "derecho a ser olvidado," codificado según la GDPR, donde los consumidores pueden pedir que las compañías de datos remuevan ciertas migas de pan digital de su historia en línea. Los consumidores, sin embargo, pueden optar por dejarlos si se les presenta una propuesta de valor que haga que valga la pena compartir tales datos.

Sin embargo, más generalmente, un enorme desafío para las compañías es cómo optimizar el uso de todos los datos generados por las tecnologías legadas y heredadas al tiempo que permanecen dentro de las fronteras de las regulaciones de la privacidad. Las instituciones financieras no se pueden centrar solo en el cumplimiento. Incluso si satisfacen todos los requerimientos legales, necesitan asegurar que sus esfuerzos de minería de datos provienen de un creciente número de fuentes no aleja a los consumidores ni a los legisladores.

El impacto de la tecnología en la privacidad variará

Nosotros analizamos ocho herramientas y tecnologías que ya son, o probablemente se volverán, ubicuas para determinar qué tan probable es que invadan la privacidad. (Por favor vea el recuadro "Acerca de nuestra investigación" en la página 8 para nuestra metodología de valoración).

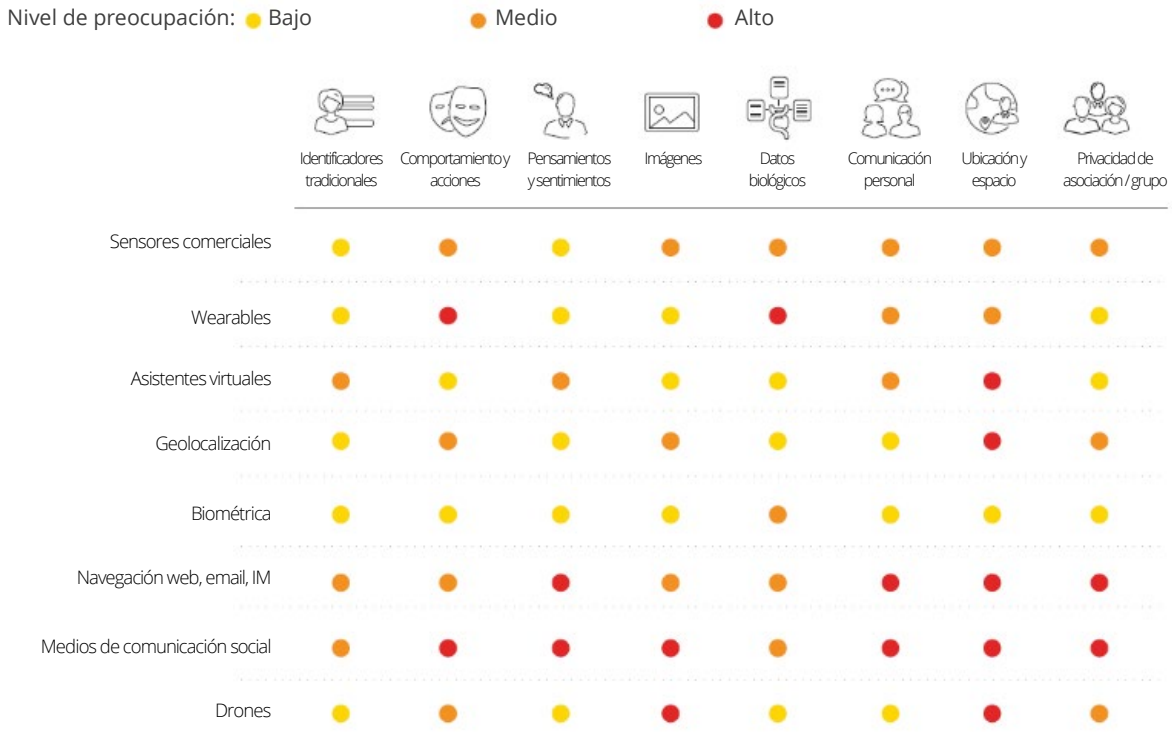
Si bien ningún área aparece completamente inmune de potenciales preocupaciones de privacidad (vea figura 3), el nivel de amenaza varía considerablemente de acuerdo con el tipo de herramienta o metodología empleada.

Nuestro análisis sugiere que algunas tecnologías es más probable que creen preocupaciones de privacidad que otras. El monitoreo de la navegación en la red y de los medios de comunicación social son los que más probablemente plantean objeciones. Sensores comerciales, wearables, asistentes virtuales, y drones son otros con importante potencial para invasión. Biométri es probablemente la tecnología con el potencial más bajo para invadir la privacidad.

Pero mirando los tipos de privacidad, las mayores causas de preocupaciones en este punto en el tiempo son *ubicación y espacio*, *comunicaciones*, *pensamientos y sentimientos*, y *asociación y grupo*. El monitoreo de *comportamiento y acciones* también podría ser desafiante con base en nuestra valoración.

FIGURA 3

Potencial de tecnología/herramienta para invadir la privacidad individual, por tipo de privacidad



Fuente: Deloitte Center for Financial Services

ACERCA DE NUESTRA INVESTIGACIÓN

Al valorar el potencial de cada tecnología o herramienta para plantear preocupaciones de privacidad, consideramos tres factores: 1. Qué tan fácil es recaudar datos del consumidor; 2. Qué tan prevalente es en la sociedad; y 3. Qué tan ampliamente es usada en servicios financieros.

Para cada tipo de privacidad, asignamos un valor entre 0 y 2 para cada uno de esos factores, con "0" siendo no-existente o bajo; "1" siendo de alguna manera; y "2" siendo alto. Los puntajes fueron luego resumidos a través de los tres factores, con igual peso, para llegar a un puntaje final para cada tecnología por tipo de privacidad.

El rango posible de este marcador total está entre 0 y 6. Si el puntaje total fue 0 o 1, nosotros denominamos el nivel potencial de amenaza como *bajo*; si fue 2, 3, o 4, nosotros lo denominamos *medio*; y si es 5 o 6, lo consideramos *alto*.

Es importante observar que nuestro análisis no es solo acerca del estado actual de las tecnologías existentes. Es muy posible que en los próximos años podrían desarrollarse otras herramientas que puedan tener implicaciones más importantes para la privacidad personal. Además, las herramientas existentes pueden ser usadas más ampliamente por firmas de servicios financieros en el futuro para obtener datos de clientes, y por lo tanto volverse más intrusivas en la privacidad.

La privacidad tiene que ver con el contexto

Más allá de cómo se recaudan los datos personales, las preocupaciones acerca de la privacidad a menudo son más acerca del contexto – por qué, quién, cuándo, y dónde. Por ejemplo, las compañías deben ser sensibles a lo que muchos refieren como el factor de escalofrío," donde los clientes pueden encontrar que la manera como las compañías obtienen datos acerca de ellos es demasiado intrusiva, tal como crear un perfil basado en la actividad en línea del individuo o mercadearlos para ellos de acuerdo con ello.[20] Las compañías necesitan ser conscientes de dónde trazar la línea y en sus políticas de privacidad comunicar claramente a los consumidores dónde está esa línea.

Entonces, ¿cómo pueden los líderes de servicios financieros determinar dónde debe estar esa línea? Aquí hay unos pocos escenarios para pensar al respecto: un dron puede ser usado para valorar la condición de una propiedad para propósitos de hipoteca o de inversión, o durante una investigación por reclamo de seguro, pero también podría ser desplegado para subrepticiamente determinar la ubicación de alguien o grabar qué está haciendo la persona (comportamientos y acciones) en un tiempo y lugar particular. De manera similar, la tecnología de geolocalización o la navegación en la red (cómo usted presiona, se desplaza, y escribe en la pantalla de un teléfono o en el teclado) puede ser usado para detectar acciones como fraude,[21] pero también para otros propósitos potencialmente invasivos, tales como seguimiento de los patrones de ubicación de uno y los hábitos en línea.

Los wearables*, otra fuente rica de datos del cliente, son usados por aseguradores de vida para motivar a los tomadores de pólizas para que se mantengan en buena condición física a cambio de primas más bajas,[22] y por los bancos para autenticación de identidad o para permitir pagos sin problemas.[23] Pero las compañías también podrían usar datos provenientes de wearables para ver si un cliente está gastando más tiempo en restaurantes de comida rápida que en gimnasio, lo cual algunos pueden considerar demasiado intrusivo. El análisis de la manera de caminar es otra manera para autenticar la identidad y mitigar contra el fraude, pero también podría ser usado para hacer inferencias acerca de la salud de una persona, lo cual para los consumidores podría ser un cruzar líneas.

Aún más controversial es cómo datos provenientes de diferentes tecnologías emergentes podrían ser combinados para hacer valoraciones mucho más precisas acerca de los clientes. Los datos biométricos provenientes de software de reconocimiento facial, podrían ser cruzados con publicaciones en medios de comunicación social para identificar el perfil de riesgo de quien aplica a un préstamo. Si bien las políticas de privacidad pueden implicar que una variedad amplia de herramientas y tecnologías estén siendo utilizadas para obtener datos, pocas, si algunas, explican por qué o cómo múltiples fuentes pueden ser correlacionadas como parte de un análisis más amplio de datos, o las potenciales implicaciones de hacerlo.

La mayoría de las veces, sin embargo, las instituciones financieras no tendrían que ir a los extremos para obtener los datos que necesitan para

* Elementos que se pueden usar. Cubre vestuarios, accesorios, equipos, dispositivos, etc. (N del t).

tomar una decisión acerca de un consumidor. Considere cómo el monitoreo de las publicaciones en medios de comunicación social podrían mostrar una bandera roja para un solicitante que publica fotografías de lecciones recientes de aventuras en paracaidismo o trapecio. Esas potencialmente podrían ser puntos valiosos de datos para un prestamista, asegurador, o incluso una firma de administración de inversión, dado que quienes buscan emociones también pueden ser menos adversos al riesgo en sus elecciones de inversión, o, de otro modo, ser demasiado riesgosos como para que un asegurador de vida los cubra.

Los reguladores de Nueva York recientemente les dieron a los aseguradores de vida luz verde para que usen publicaciones en medios de comunicación social, así como también otras fuentes no-tradicionales de datos, para ayudar a determinar cargos por primas, provisto que los aseguradores pueden probar que tales datos no discriminan injustamente con base en raza, género, color, u orientación sexual.[24] La mayoría de los consumidores puede no ser consciente de tal información íntima, si bien fácilmente disponible, podría ser accesada por su proveedor de servicios financieros.

Sin embargo, si los consumidores son hechos conscientes – no solo acerca de cómo sus publicaciones en medios de comunicación social son usadas, sino acerca del potencial valor que tal monitoreo puede proporcionarles – ello podría hacer una gran diferencia. En una encuesta realizada por Deloitte en el año 2016, solo el 15 por ciento de los consumidores estuvo dispuesto a compartir con los proveedores de servicios su actividad de navegación en la red y solo el 12 por ciento sus publicaciones en medios de comunicación social.[25] Pero si las instituciones financieras revelan plenamente la fuente de los datos y la razón para recaudarlos, y de manera clara comunican la ecuación del valor, quizás puedan superarse las preocupaciones por la privacidad.

Además, otro estudio encontró que cerca de dos tercios de quienes respondieron con 18 a 34 años de edad, y casi la mitad de quienes respondieron con 35 a 54 años de edad estarían dispuestos a permitir que los aseguradores tamicen a través de los datos provenientes de medios de comunicación social, hogares inteligentes, o incluso dispositivos de monitoreo de salud si pudieran reducir sus primas.[26] Pero, ¿qué pasa si tal monitoreo resultó en primas más altas? ¿Qué ocurriría entonces con la ecuación del valor? Esto es algo que tanto las instituciones como los consumidores deben considerar.

Mientras tanto, a pesar de la creciente popularidad y la naturaleza expansiva de los datos no-tradicionales del cliente, uno también debe cuestionar si esas fuentes actualmente proporcionan perspectivas diferenciadas: “No todos los datos generados por el Internet de las Cosas (IoT) serán útiles, y por lo tanto las compañías probablemente necesitarán ganar experiencia con algunos de esos nuevos tipos de datos... en orden a discernir cuáles son de naturaleza predictiva, y actualizar sus modelos analíticos de acuerdo con ello,” según un reporte de Deloitte sobre las potenciales oportunidades y trampas de la tecnología del IoT en servicios financieros.[27] Un ejemplo son los seguros basados-en-el-uso, donde no está claro si tales datos de la experiencia de conducción producen significativamente mejores resultados de suscripciones y fijación del precio que el uso de los identificadores tradicionales como factores de aproximación, tales como puntaje de crédito o edad.

Aun así, generalmente hablando, los consumidores pueden tener menos reparos acerca del uso de los datos por sus proveedores de servicios financieros si hay algún valor significativo ofrecido a cambio. Las instituciones financieras podrían intentar ganarse a los consumidores mediante la aplicación del enfoque de portafolio a la privacidad, mostrando varios escenarios que hablen del posible retorno que los clientes puedan recibir de compartir diversos tipos de datos versus el nivel de los riesgos involucrados.

Solo el 15 por ciento de los consumidores estuvo dispuesto a compartir con los proveedores de servicios su actividad de navegación en la red y solo el 12 por ciento sus publicaciones en medios de comunicación social.

Tome la suscripción acelerada de seguros de vida, donde los solicitantes pueden comprar cobertura sin tener que ir a exámenes médicos intrusivos.[28] Los aseguradores típicamente realizan un chequeo previo mediante accesar datos de oficinas de información médica, bases de datos de prescripciones, e incluso registros de vehículos a motor. Ellos pueden aprobar una póliza si están satisfechos con lo que encuentran, pero no pueden rechazar un candidato con solo base en datos de terceros. En el peor de los casos, el asegurador puede solicitar un examen médico completo si necesita más información antes de decidir si asegurar una persona, y si es así, a qué precio. La revelación y la transparencia prevalecen, con una clara propuesta de valor para proveedor y comprador.

Pero, ¿qué sucede si los consumidores no quieren que las instituciones financieras se entrometan en sus vidas personales, cualesquiera sean las migas de pan digitales que hayan dejado en

su estela? ¿Pueden ser sancionados de alguna manera por optar estar fuera de la economía conectada? Por ejemplo, ¿pueden los seguros de automóviles basados-en-uso expandirse hasta el punto en que los consumidores que rehúsen que su manera de conducción monitoreada en tiempo real sean automáticamente recargar porque los aseguradores no puedan valorar qué tan seguramente conducen? ¿Cómo pueden los consumidores, y los reguladores, reaccionar a ese escenario a lo largo del camino?

Las firmas de servicios financieros que carezcan de las apropiadas estrategias, políticas, y controles para tratar esas nuevas formas de datos y responder ante tales preguntas provocativas podrían estar en riesgo.

PREVISIBILIDAD INEXACTA: LA NECESIDAD DE GOBIERNO DE LOS DATOS

Una de las potenciales trampas de recaudar los denominados "grandes datos," particularmente cuando son proporcionados por terceros (por ejemplo, corredores de datos, agencias de reportes del consumidor, agregadores no-comerciales, oficinas de industria, y almacenes de datos específicos de industria/sector), es el riesgo de prospectos de micro-focalización o basar decisiones acerca de consumidores en información que resulte estar desactualizada o sea inexacta. Un estudio reciente realizado por Deloitte encontró inexactitudes importantes en datos suministrados por un corredor líder de información del consumidor, con errores variando entre el 10 y el 50 por ciento o más en una variedad amplia de puntos – incluyendo ingresos del hogar, riqueza neta, comportamiento de compra, propiedad de vivienda, vehículos conducidos, y número de hijos.[29]

El reporte de Deloitte alerta que "peligros que varían desde vergüenzas menores hasta completa alienación del cliente pueden esperar los negocios que crecientemente dependen de grandes datos para guiar decisiones de negocio y seguir estrategias de mercadeo de micro-segmentación y micro-focalización."[30]

Además, de acuerdo con el reporte, basar un mensaje personalizado o una decisión acerca de un cliente "en información equivocada o inexacta… puede no solo disminuir los esfuerzos de mercadeo, sino hacer más daño que bien… causando que el cliente se mueva desde una actitud neutral, no-existente, o positiva ante la compañía, hacia una negativa."[31]

Tales errores pueden tener implicaciones graves para consumidores e instituciones. ¿Qué pasa si los dígitos invertidos en una entrada acerca de la presión sanguínea señalan hipertensión cuando, de hecho, el individuo no tiene tal problema de salud? ¿Qué pasa si un doctor inadvertidamente presiona "seleccionar todo" en una lista de medicamentos cuando ello significa presionar "no-seleccionar"? Tales equivocaciones inocentes, incluso si son corregidas, podrían crear estragos para los individuos cuyos datos sean recogidos por compañías o por terceros.

Claramente, se necesita prestar más atención al gobierno de los datos, desde adquisición, hasta confirmación, hasta correlación de varias fuentes de datos e información. Para minimizar este riesgo, las instituciones financieras deben considerar una investigación más proactiva tanto de sus propios datos como de cualesquiera datos que reciban de terceros proveedores. Esto debe incluir una demanda por transparencia en el recaudo, el lineamiento de los datos, la validación, la oportunidad del refresco, y los métodos de corrección de los datos de una firma externa, entre una serie de pasos adicionales de diligencia debida.[32] Las firmas financieras también deben considerar verificar regularmente sus propios datos y los de proveedores externos con los clientes mismos. Esta práctica de llegar directamente podría no solo ayudar a mejorar la exactitud, sino que mostraría buena fe a los consumidores de que las instituciones financieras ponen una prima en conseguir que sus datos estén correctos.

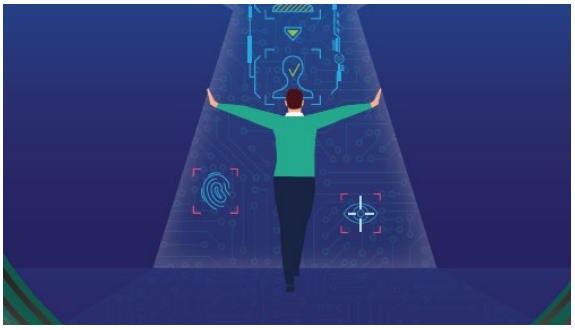
¿Las políticas existentes son adecuadas para la protección de la privacidad en la era digital?

Estado actual de las políticas de privacidad en servicios financieros

En la siguiente sección, miramos qué tan bien las firmas de servicios financieros pueden estar acondicionadas para abordar los desafíos de privacidad presentados por las tecnologías emergentes y los datos no-tradicionales. Analizamos las políticas de privacidad de una muestra aleatoria de 12 instituciones financieras grandes en banca, administración, seguros, e inmuebles para determinar qué datos se recaudan, cómo son almacenados, compartidos, y protegidos, y qué tan frecuentemente las políticas de privacidad son actualizadas.

¿QUÉ DATOS SON RECAUDADOS?

Universalmente, todas las compañías de la muestra recaudan identificadores tradicionales incluyendo (pero no limitados a) nombre, correo electrónico, dirección, número de teléfono, y número de seguridad social. Los datos recaudados por las firmas de seguros, particularmente, fueron más extensivos, dada la naturaleza de su trabajo y cómo los datos son usados para la selección del riesgo y para hacer determinaciones sobre fijación de precio y cobertura. Además de la información personalmente identificable [personally identifiable information (PII)], los aseguradores de la muestra también recaudan datos más personales tales como historia médica o de conducción, dependiendo de la línea de negocios. Todos los de la muestra también hacen seguimiento de analíticas de datos en la red, incluyendo tipo de navegador, dirección de IP, y uso de aplicaciones.



¿CÓMO LOS DATOS SON RECAUDADOS?

Las instituciones que analizamos afirman que su método primario para recaudo de datos es vía datos del consumidor "voluntariamente suministrados o revelados" – por ejemplo, datos que los consumidores manualmente ingresa cuando abren una cuenta en línea o solicitan un préstamo o una póliza de seguro. Cada compañía analizada también usa cookies y balizas de la red para recaudar y hacer seguimiento de datos de la red. Algunos también recaudan datos provenientes de recursos de terceros, tales como corredores de datos.

¿CÓMO LOS DATOS SON USADADOS?

Cada institución financiera incluida en nuestro análisis afirma que su uso de datos del consumidor es esencial para los propósitos y operaciones de negocio de cada día, y la mayoría enfatizó que la manera como usan los datos es permisible bajo la ley. La mayoría también observa que los datos son usados para entregar servicios de calidad, tales como administración de cuenta, prevención de fraude, y mercadeo.

¿LOS DATOS SON COMPARTIDOS Y LOS CLIENTES PUEDEN SALIR?

A través de la mesa, todos los de la muestra de alguna manera comparten datos. La mayoría estipula que los datos son compartidos con la misma familia de compañías y subsidiarias, o a través de unidades de negocio para "mejorar servicios."

Ellos revelan que los datos pueden ser compartidos con terceros proveedores tal y como es requerido o permitido por la ley. Además, para la mayor parte, los consumidores no pueden salir de este compartir de datos excepto cuando son usados para propósitos de mercadeo o publicidad.

¿CÓMO LOS DATOS SON PROTEGIDOS?

La mayoría de las compañías señalan que "mantienen salvaguardas físicas, electrónicas, y procedimentales" en línea con los estándares de la industria.

¿LOS CLIENTES SON NOTIFICADOS DE LOS CAMBIOS DE POLÍTICA?

Tal y como es requerido por ley, los aseguradores envían a los consumidores una política de privacidad actualizada anualmente. El resto de las compañías observa que se reservan el derecho a modificar sus políticas de privacidad a voluntad. Algunas notifican a los consumidores los cambios, mientras que otras aconsejan a los consumidores a regularmente referirse a sus sitios web para las actualizaciones de la política.

¿QUÉ TAN FRECUENTEMENTE SON ACTUALIZADAS LAS POLÍTICAS?

La mayoría de las políticas de privacidad habían sido actualizadas en el año anterior. Una compañía – un asegurador – no había actualizado su política de privacidad en línea desde el año 2013.

¿LAS INSTITUCIONES FINANCIERAS HAN IDO SUFICIENTEMENTE LEJOS CON LAS REVELACIONES SOBRE LA PRIVACIDAD?

¿Cuál de los ocho elementos de la privacidad esbozados antes son mencionados en las políticas de las compañías de la muestra? Nosotros realizamos un segundo análisis de texto sobre sus políticas de privacidad para identificar cuáles de métricas a las que se les hizo seguimiento se relacionaban con los tipos de privacidad que se describen en la página 5 (figura 2).

A primera vista, los resultados parecieron prometedores. Sin embargo, ninguna de las compañías de la muestra tuvo en cuenta todos los ocho tipos de privacidad, y la manera como fueron referenciados era posiblemente superficial. Aquí está por qué:

- Primero, las políticas sugieren que la privacidad opera a un nivel binario – si la compañía está en cumplimiento o no con las leyes existentes – y fallan en abordar las complejidades de la privacidad que han surgido gracias a los últimos avances tecnológicos.

- Segundo, ninguna de las políticas explícitamente menciona todas las tecnologías que se incluyen en nuestro análisis.

- Finalmente, ninguna de las políticas va más allá de detalle de nivel alto sobre cómo o por qué los datos son recaudados y compartidos, y mucho menos cuáles pueden ser los potenciales beneficios para los consumidores.

De hecho, encontramos que las políticas de privacidad en los sectores de servicios financieros – banca, seguros, y administración de inversiones – eran tan similares que fue difícil diferenciar entre firmas. Esto también sugiere que las actuales políticas de privacidad son solamente "verificar la caja" para satisfacer requerimientos de cumplimiento.

En el segmento bancario, por ejemplo, todos los bancos de la muestra proporcionan hojas informativas idénticas, repetitivas, sobre qué, cómo, y por qué los datos son compartidos. Además, excluyendo dos firmas de administración de inversiones que hacen parte de la muestra, que regularmente revisan y ajustan sus salvaguardas, la mayoría de las políticas de privacidad no son prospectivas y no tienen en consideración los avances en tecnología y nuevos datos – una oportunidad perdida.

Como la tecnología continúa avanzando y surgen nuevas formas de datos, ¿cómo las instituciones financieras deben adaptar sus políticas de privacidad? Si bien las formas tradicionales de datos del consumidor están cubiertas bajo las actuales leyes de privacidad financiera, los datos provenientes de la fusión de nuevas tecnologías no. Dada la ausencia de un estándar federal de los Estados Unidos comprensivo y prospectivo, parece que cada vez hay un mayor abismo de los datos que las políticas de las instituciones financieras no tienen en cuenta y, más importante aún, que las compañías no pueden estar obligadas a rendir cuenta. Por lo tanto, el estado actual de las políticas de privacidad existentes puede estar dándoles a los consumidores un sentido falso de comodidad, lo cual podría estar preparando el escenario para un rudo despertar y, en consecuencia, el potencial para una reacción violenta de la privacidad entre los consumidores.

Mirando hacia adelante: Una nueva manera para administrar la privacidad del cliente

EN ESTE REPORTE, proponemos que las instituciones financieras deben repensar la privacidad del cliente de una manera más expansiva, proactiva, y estratégica. En resumen, las firmas deben considerar lo siguiente:

- **Ampliar sus lentes.** Ir más allá de los puntos de chequeo tradicionales para tener en cuenta los múltiples tipos de privacidad y las herramientas y tecnologías capaces de invasión. Como primer paso, las instituciones financieras deben volverse más proactivas y deliberativas, explorando cómo las fuentes emergentes de datos y preocupaciones de privacidad probablemente evolucionarán con el tiempo en términos de actitudes del consumidor, innovación tecnológica, y restricciones regulatorias.

- **Revisar y modernizar las políticas actuales de privacidad.** Las políticas de hoy a menudo incluyen declaraciones simples de revelación para eliminar obstáculos regulatorios. En lugar de ello, las compañías deben usar esas políticas para ganarse la confianza del cliente mediante proporcionar suficiente transparencia para demostrar buena fe. Además, las instituciones podrían ayudar a aliviar cualesquiera dudas que persistan acerca de la privacidad mediante mostrarles a los consumidores cómo ellos también se podrían beneficiar de los diversos tipos de recaudo y análisis de datos, e incluir esos detalles en sus políticas.

- **Ser buenos administradores de los datos que recaudan y compran.** Las compañías podrían mejorar el control de calidad, la exactitud, y la relevancia de los datos que recaudan mediante establecer una estructura más comprensiva del gobierno de la privacidad. Esto incluiría investigación sistemática de los datos recaudados en casa y provenientes de terceros.

- **Explorar nuevas técnicas de la ciencia de datos para proteger información sensible.** Como un ejemplo, las instituciones podrían adicionar ruido aleatorio o crear conjuntos sintéticos de datos para proteger la información personal o sensible de los consumidores.[33]

- **Hacer uso positivo de las tecnologías emergentes y de las nuevas fuentes de datos.** Las instituciones financieras deben mirar maneras para que los datos puedan ser de beneficio para proveedores *y* consumidores. Los clientes deben mantenerse informados cuando las compañías exploren nuevas fuentes de datos y métodos analíticos, y las instituciones deben abiertamente revelar y explicar la propuesta de valor que se hace a los consumidores.

Las instituciones financieras deben volverse más proactivas y deliberativas, explorando cómo las fuentes emergentes de datos y preocupaciones de privacidad probablemente evolucionarán con el tiempo.

- **Finalmente, los directores de privacidad jefes deben ser empoderados** para desarrollar nuevas estrategias de administración

de la privacidad. Si tales posiciones no existen, puede ser necesario que las instituciones designen a alguien para que lidere la administración de la privacidad.

Cuando todo está dicho y hecho, las instituciones financieras deben ser capaces de satisfacer los requerimientos regulatorios básicos al tiempo que también hacen honor a las sensibilidades del consumidor acerca de la inviolabilidad de su información personal. Tales sensibilidades es probable que evolucionen con el tiempo y podrían diferir a través de segmentos y distintos tipos de privacidad.

Más que asumir que las percepciones que los clientes tienen sobre la privacidad son inmutables y no son susceptibles de persuasión, las firmas de servicios financieros pueden darle forma a cómo los clientes ven el valor de sus datos. Ellas pueden engendrar confianza mediante comunicar claramente qué están haciendo con los datos del consumidor y mediante dar algo a cambio, tal como ofertas personalizados, nuevos servicios, mejor fijación del precio, o tiempo reducido para la entrega de servicio.

Estos pasos pueden ayudar a que las instituciones financieras estén preparadas para un futuro caracterizado por innovación tecnológica continua, rápida. Armadas con este enfoque nuevo, más estratégico, las instituciones financieras deben estar mejor preparadas para administrar de manera efectiva la privacidad en un mundo crecientemente digital, para diferenciarse ellas mismas, y, muy importante, para servir más efectivamente a sus clientes.

Apéndice: Desarrollos recientes en la regulación de la privacidad

EL DESARROLLO MÁS NOTABLE en la regulación de la privacidad del consumidor es posiblemente la adopción de la GDPR en la Unión Europea, que entró en efecto en mayo de 2018. Esta regulación radical impacta cada negocio que maneje datos personales de ciudadanos de la Unión Europea, incluyendo las instituciones financieras. La GDPR protege los datos personales de todos los residentes en la Unión Europea, al tiempo que estipula que las compañías tienen que notificar a los ciudadanos de la Unión Europea las violaciones de los datos y obtener consentimiento expreso para sus datos, o correr el riesgo de pagar fuertes multas. Los consumidores también tienen "derecho a ser olvidados," y las compañías están requeridas a borrar, a solicitud, todos los datos personales actualmente mantenidos o si los datos ya no sirven al propósito original del negocio.[34]

En los Estados Unidos, las regulaciones tienden a ser de alcance más estrecho y generalmente solo protegen tipos específicos de datos o tienden a ser específicas de sector o de industria. La Federal Trade Commission (FTC), una autoridad legal independiente, tiene la tarea de hacer forzosa una serie de esas leyes, incluyendo las que regulan la privacidad del consumidor en cuanto se relaciona con niños, prácticas de tele-mercadeo, fraude del consumidor, recaudo de deuda, y prácticas de crédito y de préstamo no-justas, para mencionar solo unas pocas.[35]

A comienzos del año 2019, no hay un estándar federal de privacidad único, comprensivo, que proteja todos los tipos de datos del consumidor, que esté en efecto en los Estados Unidos, dejando que los estados diseñen sus propios mandatos. California, liderando el cargo, en el verano de 2018 aprobó la Consumer Privacy Act. Similar a la GDPR, les otorga a los consumidores control radical de todas las formas de sus datos personales,[36] desde direcciones y números de teléfono hasta "me gusta" en medios de comunicación social o interacciones con asistentes personales. La nueva ley de California tendrá efecto en el año 2020, y si bien solo aplica a los residentes en California, muchas compañías que operan nacionalmente se espera que enmienden sus políticas de privacidad para evitar estándares en conflicto para los consumidores en otros estados.[37]

En California ha sido presentado un proyecto de ley – AB981 – diseñado para eliminar la superposición entre la nueva ley de California y la Insurance Information and Privacy Protection Act de 1980, pero grupos de consumidores están haciendo cabildeo contra cualquier exclusión para los aseguradores.[38]

Fuera de California, existe una serie de otras leyes estatales de privacidad, pero las leyes no son tan amplias como la de California. Vermont, por ejemplo, promulgó en el año 2018 una ley de privacidad de los datos de los corredores [*brokers*], que tiene la intención de proteger a los consumidores de corredores de datos que son terceros y que recogen y venden su información sin su consentimiento.[39] Delaware, mientras tanto, promulgó en el año 2016 la Delaware Online Privacy and Protection Act, que requiere que todas las firmas que recauden PII publiquen políticas de privacidad.[40]

Leyes de privacidad financiera

A pesar de la carencia de un estándar federal único, que lo abarque todo, un conjunto robusto de regulaciones gobierna el sector de servicios financieros de los Estados Unidos. Una ley importante es la Gramm-Leach-Bliley Act (GLBA), que regula cómo las instituciones financieras (incluyendo bancos, valores, y entidades de seguros) manejan y protegen la PII del consumidor que no es pública. La GLBA manda, según su "Regla de privacidad financiera," que las instituciones financieras proporcionen notificación de sus políticas de privacidad y limitan su revelación de PII a terceros afiliados y no-afiliados.[41] Las compañías también están requeridas a darles a los consumidores notificación y una "oportunidad razonable" para salir del compartir algunos tipos de datos con terceros. Las firmas financieras también tienen que proporcionar y mantener salvaguardas para proteger la PII del consumidor según otra determinación de la GLBA conocida como la "Regla de salvaguardas."[42]

A la Consumer Financial Protection Bureau (CFPB) le fue dada autoridad de reglamentación para hacer forzoso el cumplimiento de buena parte de la GLBA según la Dodd-Frank Wall Street Reform and

Consumer Protection Act (Dodd-Frank).[43] La FTC también hace forzoso el cumplimiento de las determinaciones de la GLBA.[44]

Leyes adicionales de privacidad financiera incluyen la Fair Credit Reporting Act (que regula los datos personales tenidos por agencias de información del consumidor),[45] la Bank Secrecy Act (que obliga a que las compañías ayuden al gobierno en la prevención y prevención del lavado de dinero mediante compartir reportes de actividad del consumidor),[46] y la Right to Financial Privacy Act (que les otorga a los consumidores un grado de privacidad ante el gobierno).[47]

A pesar de la plétora de reglas de privacidad, la conciencia del público permanece limitada. Una encuesta realizada a 6,999 personas en seis países, incluyendo los Estados Unidos, encontró que más de la mitad no estaban familiarizados con las regulaciones de la privacidad concernientes a sus datos personales.[48]

Notas finales

[1] Electronic Frontier Foundation, "Privacy," accessed March 4, 2019.

[2] Lee Rainie, "Americans' complicated feelings about social media in an era of privacy concerns," Pew Research Center, March 27, 2018.

[3] EUGDPR, "The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years," accessed March 5, 2019.

[4] Alexandra Bruell, "Advertisers' top trade group pushes for Federal Data Privacy Regulation," Wall Street Journal, December 19, 2018.

[5] Internet Association, "Internet Association proposes privacy principles for a modern national regulatory framework," press release, September 12, 2018.

[6] U.S. Chamber of Commerce, "U.S. Chamber privacy principles," accessed April 8, 2019.

[7] Californians for Consumer Privacy, "What does the California Consumer Privacy Act do?," accessed April 22, 2019.

[8] Bryan Cave Leighton Paisner, "The top three privacy takeaways of the New Delaware Online Privacy and Protection Act," August 3, 2016.

[9] Harry Valetk, Brandon Moseberry, and Bernard L. Hengesbaugh, "Vermont enacts first US Data Broker Privacy Law," Lexology, August 3, 2018.

[10] Deloitte Canada, "Privacy for sale: To the highest bidder," accessed April 8, 2019.

[11] Will Thomas DeVries, "Protecting privacy in the digital age," *Berkeley Technology Law Journal* 18, no. 1 (2003): pp. 283–311.

[12] Daniel J. Solove, "A taxonomy of privacy," *University of Pennsylvania Law Review* 154, no. 3 (2006).

[13] William M. Beaney, "The Right to Privacy and American Law," accessed April 8, 2019.

[14] Deirdre K. Mulligan, Colin Koopman, and Nick Doty, "Privacy is an essentially contested concept: A multidimensional analytic for mapping privacy," The Royal Society Publishing, December 28, 2016.

[15] Carissa Véliz, "What if banks were the main protectors of customers' private data?" *Harvard Business Review*, November 20, 2018.

[16] World Economic Forum, "World Economic Forum annual meeting," accessed April 8, 2019.

[17] Val Srinivas, "Privacy in the post-GDPR world: How should banks and other financial institutions rethink customer privacy and make it a differentiator?," QuickLook blog, Deloitte Center for Financial Services, March 14, 2018.

[18] Matt Burgess, "Your next bank card will have a fingerprint scanner built-in," *Wired*, May 2, 2018.

[19] Scram Software, "Does my internet activity affect my insurance and credit ratings," March 18, 2015.

[20] Knowledge@Wharton, "Privacy on the Web: Is It a losing battle?," June 25, 2008.

[21] Tanaya Macheel, "Are you really there? U.S. bank tries geolocation to stop fraud," *American Banker*, October 17, 2016; Stacy Cowley, "Banks and retailers are tracking how you type, swipe and tap," *New York Times*, August 13, 2018.

[22] Lisa F. Carver, "Why Life Insurance companies want your Fitbit data," Medical Xpress, September 24, 2018.

[23] Avin Arumugam, "Paying with wearables: The next big thing in IoT," Visa, accessed February 28, 2019.

[24] Jessica Baron, "Life Insurers can use social media posts to determine premiums, as long as they don't discriminate," *Forbes*, February 4, 2019.

[25] Gina Pingitore et al., *To share or not to share: What consumers really think about sharing their personal information*, Deloitte University Press, September 5, 2017.

[26] Tim Sandle, "Are you happy with digital spying for reduced insurance prices?" *Digital Journal*, June 21, 2018.

[27] Jim Eckenrode, *The derivative effect: How financial services can make IoT technology pay off*, Deloitte University Press, October 13, 2015.

[28] Greg Lacurci, "Technology is streamlining the process of issuing life insurance policies," InvestmentNews, January 10, 2018.

[29] John Lucker, Susan K. Hogan, and Trevor Bischoff, "Predictably inaccurate: The prevalence and perils of bad big data," *Deloitte Review* 21, July 31, 2017.

[30] Ibid.

[31] Ibid.

[32] Ibid.

[33] Sachin Gupta and Matthew Schneider, "Protecting customers' privacy requires more than anonymizing their data," *Harvard Business Review*, June 1, 2018.

[34] EUGDPR, "The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years," accessed April 22, 2019.

[35] Federal Trade Commission, *Privacy and data security update: 2016*, 2016.

[36] Californians for Consumer Privacy, "What does the California Consumer Privacy Act do?"

[37] Marc Vartabedian, "California passes sweeping data-privacy bill," *Wall Street Journal*, June 29, 2018.

[38] Timothy Darragh, "California lawmaker, APCI defend insurance privacy bill," BestWire, April 4, 2019.

[39] Valetk, Moseberry, and Hengesbaugh, "Vermont enacts first US Data Broker Privacy Law."

[40] Paisner, "The top three privacy takeaways of the New Delaware Online Privacy and Protection Act."

[41] FDIC Consumer Compliance Examination Manual, "Gramm-Leach-Bliley Act (Privacy of Consumer Financial Information)," June 2016.

[42] Federal Trade Commission, "Financial privacy," accessed April 5, 2019.

[43] FDIC Consumer Compliance Examination Manual, "Gramm-Leach-Bliley Act."

[44] Federal Trade Commission, "Financial privacy."

[45] Federal Trade Commission, "A summary of your rights under the Fair Credit Reporting Act," accessed March 5, 2019.

[46] Federal Deposit Insurance Corporation, "Bank Secrecy Act, Anti-Money Laundering and Office of Foreign Assets Control," accessed March 5, 2019.

[47] FDIC Consumer Compliance Examination Manual, "Gramm-Leach-Bliley Act."

[48] Deloitte Canada, "Privacy for sale."

Acerca de los autores

VAL SRINIVAS es el líder de investigación en banca y mercados de capital en el Deloitte Center for Financial
Services. En su rol, Srinivas trabaja estrechamente con el centro y el equipo extendido de servicios financieros para apoyar y continuar el desarrollo de nuestras iniciativas de liderazgo del pensamiento en la industria, coordinando nuestros diversos esfuerzos de investigación y ayudando a diferenciar a Deloitte más efectivamente en el mercado. Srinivas tiene más de 15 años de experiencia en investigación y estrategia de mercadeo. Tiene su sede en New York.

SAM FRIEDMAN es el líder de investigación en seguros en el Deloitte Center for Financial Services, donde analiza las últimas tendencias e identifica los principales desafíos que enfrentan las industrias de daños a la propiedad, seguros de vida, y anualidades. Firdman se unió a Deloitte en octubre de 2010 después de 29 años en National Underwriter P&C, donde fue editor en jefe. Ha escrito varios artículos para Deloitte Insights, incluyendo reportes sobre administración del riesgo cibernético en servicios financieros y obstáculos al desarrollo de seguros cibernéticos. Tiene su sede en New York.

TIFFANY RAMSAY es analista senior de perspectivas de mercado en el Deloitte Center for Financial Services, Deloitte Services LP, donde contribuye a iniciativas de investigación que diferencian al centro como líder del pensamiento en la industria de servicios financieros. Tiene más de cinco años de experiencia en investigación. Ramsay tiene una licenciatura en sociología y una maestría en administración pública de Cornell Universiy. Tiene su sede en New York.

Agradecimientos

Los autores desean dar las gracias a los siguientes profesionales de servicio al cliente de Deloitte por sus contribuciones a este artículo:

Michelle Chodosh, gerente senior, Deloitte Services LP

Patricia Danielecki, gerente senior, Deloitte Services LP

Chris Faile, gerente senior, Deloitte Services LP

Erin Loucks, gerente, Deloitte Services LP

Omer Sohail, directivo, Deloitte Consulting LP

Acerca del Deloitte Center for Financial Services

El Deloitte Center for Financial Services, que apoya la práctica de US Financial Services de la organización, proporciona perspectiva e investigación para ayudar a tomadores de decisión de nivel senior de bancos, firmas de mercados de capital, administradores de inversión, aseguradores, y organizaciones inmobiliarias. El centro está compuesto por un grupo de profesionales con un conjunto amplio de experiencias de industria en profundidad, así como también investigación de vanguardia y habilidades analíticas. Mediante nuestra investigación, mesas redondas, y otras formas de compromiso, buscamos ser una fuente de confianza para perspectivas relevantes, oportunas, y confiables. Lea las publicaciones recientes y conozca más acerca del centro en Deloitte.com.

Contactos

LIDERAZGO DE INDUSTRIA
Kenny Smith
Principal
US Financial Services leader
Deloitte Consulting LLP
+1 415 783 6148
kesmith@deloitte.com

PATROCINADOR EJECUTIVO
John Lucker
Principal
Deloitte and Touche LLP
+1 860 725 3022
jlucker@deloitte.com

DELOITTE CENTER FOR FINANCIAL SERVICES
Jim Eckenrode
Managing director
Deloitte Center for Financial Services
Deloitte Services LP
+1 617 585 4877
jeckenrode@deloitte.com

Val Srinivas, PhD
Banking and capital markets research leader
Deloitte Center for Financial Services
Deloitte Services LP
+1 212 436 3384
vsrinivas@deloitte.com

Sam Friedman
Insurance research leader
Deloitte Center for Financial Services
Deloitte Services LP
+1 212 436 5521
samfriedman@deloitte.com

Deloitte.
Insights

Suscríbase para actualizaciones de Deloitte Insights en www.deloitte.com/insights.
Siga a @DeloitteInsight

Colaboradores de Deloitte Insights

Editorial: Karen Edelman, Blythe Hurley, Nairita Gangopadhyay, y Abrar Khan
Creativo: Emiliy Moreano
Promoción: Ankana Chakraborty
Artes: Emily Moreano

Documento original: "***Reimagining customer privacy for the digital age. Going beyond compliance in financial services?***", Deloitte Insights, May 2019.
https://www2.deloitte.com/insights/us/en/industry/financial-services/protecting-customer-privacy-financial-institutions.html
Traducción realizada por Samuel A. Mantilla, asesor de investigación contable de Deloitte &Touche Ltda., Colombia.