Consumers’ privacy, selling of information, and security in digital markets

Tesis Doctoral

María Dolores Sánchez Romero

Departamento de Análisis Económico
ERI Comportamiento Económico-Social (ERI-CES)

Universidad de Valencia

Directora: María Amparo Urbano Salvador
Doctorado en Economía Industrial

Facultad de Economía Julio 2019

A mis padres, Francisco y Remedios,

por su amor y apoyo incondicional durante toda mi vida.

“No debemos tener miedo a equivocarnos,

hasta los planetas chocan y del caos nacen las estrellas.”

Charles Chaplin

Acknowledgements

Siempre he dado las gracias por todas las oportunidades que se me han brindado y por la confianza depositada en mí. Uno de los mayores aprendizajes que me llevo durante estos años de tesis doctoral es que hay que ser agradecidos y responsables por el tiempo que muchas personas nos dedican.

Primeramente, me gustaría agradecer a mi directora de tesis, Amparo Urbano Salvador, por todo lo que ha hecho por mí. Su dedicación, energía, profesionalidad, saber hacer, experiencia y su persona han contribuido a que ganase seguridad y conocimientos con el paso del tiempo. Gracias Amparo.

También agradecer a las instituciones y demás personas que hacen de todo esto algo posible como ERI-CES y el Departamento de Análisis Económico de la Universidad de Valencia, por el apoyo económico, acceso a instalaciones y materiales, y la posibilidad de impartir docencia. Sobre todo, al equipo humano que lo compone, y en especial a los de la púa E con los que he compartido muy buenos momentos estos últimos años.

La estancia doctoral en Brown University, EEUU, ha sido una de las experiencias más enriquecedoras que he tenido en este proceso a nivel profesional y personal. Me gustaría agradecer a Roberto Serrano quién hizo posible esta experiencia. Así mismo, agradecer a muchas personas que encontré allí, como Antoinette Breed y a la Dra. Sofía Pérez Luján, por hacer esta experiencia aún más mágica.

Me gustaría agradecer a Pepa Melià, técnica lingüística de la Universidad de Valencia, por su profesionalidad y apoyo infinito. Gracias a ti he conseguido un objetivo pendiente de hace muchos años, el nivell C1 de valencià!

Durante el camino, he encontrado a muchas personas con el mismo destino. Unos ya llegaron, otros están por llegar. Gracias Adri, Adriana, Álex, Alicia, Ana, Andrea, Belén, Daniela, Eli, Ernesto, Javi, Jesús, Jose, Laura, Lucía, Luis, Marta Solaz, Marta Suarez, Mauricio, Paula, Rubén, Víctor por compartir conmigo esta travesía. A mis vecinos de la puerta 9, Alicia y Sergio, a Ragnar y a Lili. Me llevo grandes amigos de este camino.

Pero hay algunos que han estado en esta etapa y estarán en muchas más. Tengo la gran suerte de contar con Adri, con quién he compartido tanto, también este camino repleto de incertidumbres. Gracias cariño. Gracias a Marta Solaz, por estar ahí desde el principio, por seguir ahí pase lo que pase. También a Josan. A Laura, por construir una realidad mejor y posible. A Ernesto, por vivir locuras dentro de la cordura, nunca olvidaré el paseo bajo la lluvia en Manhattan.

Quiero agradecer de todo corazón a los que siempre han estado al otro lado, a mi gente de la Vega Baja por darme las ganas de volar. A mis amigos de siempre, Nadia, Jesús, Marta, Amanda, Sonia, Christian, Estefanía, Rafalín, Sabinica, Mari Virtu, Pablo y Pilar. A mis vecinos-familia, a mi mami, que sé que no voy a verla mucho, pero que sepa que la tengo presente siempre.

Agradecer a mi familia todo lo que han hecho y hacen por mí, a los Sánchez y a los Romero. A mi madre, a mi hermano y a mi sobrina por estar siempre a mi lado. A mi madre, por su fortaleza, lucha y entrega durante muchos años difíciles. Todo lo que soy y he conseguido en esta vida es gracias a ti, mamá. A mi padre, que sé que está conmigo desde el otro lado del infinito. La ausencia en la que he estado durante tantos años no es fácil de llevar. Sin vosotros, no soy nada.

Y, por último, a mi pareja Adrián Nerja, que también ha sido compañero de travesía. Gracias por estar conmigo siempre, por dar luz a la oscuridad, por hacer que todo tenga un poco más de sentido.

Show must go on.

Table of contents

List of figures

List of tables

Chapter 0

Introducción: un enfoque general

0.1 El derecho a la privacidad en la era digital

El 18 de diciembre de 2013, la Asamblea general de las Naciones Unidas aprobó la resolución titulada *El derecho a la privacidad en la era digital* para todas las personas.[1] Esta resolución establece que la vigilancia global indiscriminada implica una grave violación de los derechos humanos, y pretende reafirmar los principios fundamentales adoptados en la Declaración Universal de Derechos Humanos de 1948 (art. 12), el Pacto Internacional de Derechos Civiles y Políticos (art. 17), y el Pacto Internacional de Derechos Económicos, Sociales y Culturales. En concreto, esta resolución deja claro que "la vigilancia y la interceptación ilícitas o arbitrarias de las comunicaciones, así como la recopilación ilicita o arbitraria de datos personales, al constituir actos de intrusión grave, violan los derechos a la privacidad y a la libertad de expresión y pueden ser contrarios a los preceptos de una sociedad democrática".

Al reconocer la privacidad como un derecho fundamental en la era digital, se pone de relieve la existencia de antecedentes que denotan un perjuicio y vulnerabilidad claros para el

[1] Texto completo: https://www.ohchr.org/SP/HRBodies/HRC/RegularSessions/Session34/Pages/ResDecStat.aspx.

conjunto de las personas de la sociedad.

Entre las vulnerabilidades y los posibles costes a los cuales se pueden enfrentar las personas, por un mal uso de la información personal, se encuentran, entre otros:

a) Robo de identidad: se trata del uso deliberado de la identidad de otra persona, generalmente como un método para obtener una ventaja financiera u obtener crédito y otros beneficios en nombre de la otra persona. Se puede dar desde el caso más común como es el robo de identidad en el permiso de conducción o robo de identidad en los empleos. Generalmente, se utilizan los datos personales como los del DNI (documento nacional de identidad) o NIF (número de identificación fiscal).[2]

b) Riesgo de abuso: desconcierto personal y profesional, acceso restringido a los mercados laborales o acceso restringido a mejores precios, (Chaudhry et al. 2015).

c) Violaciones de privacidad («privacy breaches» en inglés): un incidente en el que un individuo no autorizado ha visto, robado o usado información confidencial, sensible o protegida. En los últimos años, encontramos casos muy llamativos en este contexto como el de Yahoo en 2013 con 3 billones de datos robados, eBay en mayo de 2014 con 145 millones o Uber en 2016 con 57 millones.[3]

La consecución de un equilibrio entre la privacidad y la seguridad, y cómo éste afecta a la libertad y a la democracia, es uno de los paradigmas más estudiados actualmente.[4]

[2] Las 20 formas de robo de identidad y fraude: https://www.experian.com/blogs/ask-experian/20-types-of-identity-theft-and-fraud/.

[3] Los 18 mayores «data breaches» en el siglo XXI. https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

[4] Veáse, por ejemplo: the fourth Princeton Fung Global Forum, celebrado en marzo 2017 en Berlin. https://www.princeton.edu/news/2017/04/13/princeton-fung-global-forum-asks-if-liberty-can-survive-digital-age.

0.2 Breve historia de la privacidad

Para entender el problema al cual nos enfrentamos ante una posible violación de nuestra privacidad en los entornos digitales, y su efecto en la libertad y a la democracia, debemos primeramente acercarnos a un par de conceptos: el de lo público y el de lo privado. Ya que esta dicotomía está estrechamente vinculada con la libertad, en el sentido de que dependiendo de cual sea nuestra concepción de lo que es público y privado, y de la valoración que de uno y de otro ámbito realicemos, así entenderemos la libertad, así la defenderemos. Y a su vez, según la concepción que tengamos de la libertad, así valoraremos uno y otro aspecto de nuestra vida, y, por tanto, nuestra privacidad.

Por otro lado, no es extraño que, además, la resolución señale que la no defensa de la privacidad en la era digital puede ser contraria a los preceptos de una sociedad democrática. De hecho, los orígenes de las primeras nociones de privacidad, y de la distinción entre lo privado y lo público, está en la Antigüa Grecia. Sería con el nacimiento de las polis (denominación griega de las ciudades) y más concretamente, con la democracia de Pericles, donde estos conceptos de libertad, democracia y la polaridad entre lo privado y lo público se consoliden. Un ejemplo de distinción entre lo público y lo privado, lo podemos encontrar en la literatura griega y de la mano de Homero, con la famosísima obra La Odisea.[5] El tema de la privacidad ya se podía ver en los escritos de Sócrates y también en otros filósofos.[6] Aristóteles, por ejemplo, fue quien hizo la célebre distinción entre la esfera pública, correspondiente a la actividad política, y la esfera privada de la familia y la vida doméstica.

Dado esto, un ingrediente base en la defensa de la libertad y, por ende, de la privacidad y de lo relativo a ella, es la democracia. Nació de la democracia, y “dichas delineaciones no

[5] La primera oposición explícita entre lo público y lo privado en la literatura griega ocurre en la Odisea, págs. 8-9.

[6] Moore Jr., B.: Studies in Social and Cultural History. M.E. Sharpe, Inc., Armonk (1984)

podrían haber sido hechas en las teocracias del antiguo cercano oriente, porque en dichas culturas el concepto de dios-soberano lo permea todo y no es posible la noción de lo privado", como recoge la autora Susan Ford Wiltshire.[7]

En su forma más fundamental, la privacidad estaba relacionada con los aspectos más íntimos del ser humano. Casi todas las actividades domésticas se realizaban en frente de familiares y amigos, y la privacidad podía implicar alejarse de la sociedad. Esto tiene sentido si pensamos en los orígenes de la humanidad, donde los primeros humanos se organizaban en pequeños grupos, donde el deseo de supervivencia no daba lugar a el nacimiento de la necesidad de privacidad. Siempre ha habido, como apunta Holvast (2007), una especie de conflicto entre el deseo subjetivo de soledad y reclusión y el objetivo de depender de los demás. Además, esta distinción se reflejaba, como señala la historiadora Samantha Burke, incluso en la arquitectura de las casas, donde se intentaba equilibrar la luz natural con la mínima exposición posible.[8]

Por el contrario, más tardíamente, en la época del imperio Romano, nos encontramos ostentosas casas de los adinerados, alejadas de las ciudades, que se caracterizaban por amplios espacios abiertos que permitían ver y escuchar lo que sucedía en sus interiores. Las casas se caracterizaban por tener unas paredes en las que se podía escuchar hasta los sonidos más sutiles.

En los siglos posteriores, la privacidad ha estado relacionada con la casa, con la vida familiar y con la correspondencia personal. De hecho, desde el siglo XIV hasta principios

[7] Ford Wiltshire, S.: Public and private in Vergil's Aeneid, op. cit. "Tales delineamientos no se podrían haber hecho en las teocracias del antiguo Cercano Oriente, porque en tales culturas el dios-como-gobernante impregna todo y ninguna noción de lo privado es posible. La polaridad apareció en la lengua griega, sin embargo, tan pronto como Homero y se desarrolló en el período democrático de la Atenas clásica. [...]"

[8] Burke, Samantha. Delos: Investigating the notion of privacy within the ancient Greek house. Diss. University of Leicester, 2000.

del siglo XIX, muchos son los casos llevados a los tribunales de justicia relacionados con escuchas o por abrir y leer cartas personales. Un ejemplo muy significativo de esto en el siglo XIX, fue el escándalo de espionaje de la oficina de correos en 1844, cuando el nacionalista italiano Giuseppe Mazzini acusó al gobierno británico de abrir sus cartas. La confirmación de su sospecha hizo que presentara una queja al tribunal cuya reinvidicación principal se basó en dos atributos principales de las cartas: que son privadas y que las mismas contienen secretos. El aspecto más importante de este acontecimiento fue, sin duda, y como señala Kate Lawson, es que esas dos reinvidicaciones acerca de las cartas ayudaron al nacimiento de definiciones de privacidad en las comunicaciones personales y que el escándalo propició el surgimiento de preguntas acerca expectativas razonables de privacidad que son a la misma vez Victorianas y claramente contemporáneas.[9]

Desde finales del siglo XIX, el énfasis dado al término de la privacidad se dirigió más hacia la información personal y al control de la misma. Y es por eso, que la privacidad tal como solemos entenderla no tiene mucho más de 200 años. Incluso hoy, a pesar de ser un concepto común, es difícil de dar una definición última de privacidad. Y lo que es más relevante, más allá del consenso mundial sobre la importancia de la privacidad y la protección de datos, no existe una definición universal de la misma (Kasneci 2008).

0.3 ¿Qué se entiende por privacidad?

Entre las primeras definiciones del concepto de privacidad, tal y como lo entendemos hoy en día, podemos encontrarla en el famoso ensayo de Brandeis and Warren (1890), en el que se describe la privacidad como “el derecho de dejarte sólo o en paz”. Aunque, como bien establece Daniel (2006), la privacidad significa diferentes cosas para gente diferente. Una de

[9] Kate Lawson. Personal Privacy, Letter Mail, and the Post Office Espionage Scandal, 1844. Branch: Britain, Representation and Nineteenth-Century History. Ed. Dino Franco Felluga. Extension of Romanticism and Victorianism on the Net. Web. 16 March 2013.

las definiciones más famosas y aceptadas, se debe a Westin and Ruebhausen (1967), en la que la privacidad es entendida como "la reclamación de individuos, grupos o instituciones para determinar por sí mismos cuándo, cómo y en qué medida la información sobre ellos se comunica a otros". En esta línea, Boyd (2010) se refiere a privacidad como, fundamentalmente, el control sobre cómo fluye la información. Por otro lado, la privacidad ha sido definida como un aspecto de dignidad, y últimamente, libertad humana (Schoeman 1992).

La importancia en su definición se encuentra, específicamente, en marcar los límites entre lo que es privado y lo que es público. En esto, como se decía anteriormente, radica la importancia para la regulación y la protección de los datos personales.

Desde un punto de vista regulatorio, la necesidad de una definición precisa de este concepto es vital. La seguridad en los mercados digitales, lo que comúnmente se conoce como seguridad en la tecnología de información o ciberseguridad, y su regulación indirecta a través de la privacidad, ha hecho necesario un mayor esfuerzo a la hora de definir los límites que marcan la privacidad, o dicho de otra manera, los límites entre el yo y los demás, entre lo privado y lo público.

La ENISA (Agencia de Seguridad de las Redes y de la Información de la Unión Europea), en un reciente informe pone en relieve la importancia que tiene la estandarización de conceptos como la privacidad o ciberseguridad. Su importancia es máxima a la hora de desarrollar normas que permitan una mayor adaptación internacional, transferencia de buenas practicas entre organizaciones, la promoción de la integración y/o la interoperabilidad de los sistemas.[10]

[10] Union, E.,& For, A. (2018). Guidance and gaps analysis for European standardisation.

0.4 Mercados de datos personales

La Era de Internet viene acompañada de una nueva forma de concebir la privacidad, adaptada a la realidad imperante de un entorno global y digital.

Contrariamente a lo que se pudiera pensar, las bases de datos personales de los consumidores han existido durante el siglo XX (Smith 2000), solamente que con el progreso de la tecnología de la información y el surgimiento de Internet, se ha propiciado que haya crecido considerablemente el ámbito y alcance de dichas bases de datos. Hoy en día, se pueden almacenar una variedad de información personal muy amplia y rica.

La pregunta es: ¿qué tipo de información personal se puede almacenar? Se pueden guardar, analizar y/o vender datos personales relativos a nuestros perfiles y datos demográficos, cuentas bancarias, registros médicos y datos de empleo. Nuestras búsquedas en la web, los sitios que visitamos, nuestros gustos y aversiones y las historias de compras. Nuestros tweets, textos, correos electrónicos, llamadas telefónicas y fotos, así como las coordenadas de nuestras ubicaciones del mundo real.

De acuerdo a las estadísticas de World Population, el 56.1% de la población mundial tiene acceso a Internet, ascendiendo esa cifra al 81% en el mundo desarrollado, por lo que a mayor acceso a Internet mayor generación de datos personales y por tanto, mayor potencial de hacer negocio con los mismos.[11] Sin embargo, todavía no somos plenamente conscientes de la gran exposición a la que nos encontramos en los entornos digitales. Como subraya «The World Economic Forum» en su informe Rethinking Personal Data (2012), la mayoría de las personas no tienen conocimiento suficiente sobre lo que puede suceder con sus datos personales al usar teléfonos inteligentes (smartphones) o Internet. Y consecuentemente, esto

[11] Estadísticas disponibles en: https://www.internetworldstats.com/stats.htm

tiene sus efectos en el entorno digital: lleva al miedo, a la incertidumbre y al declive de la confianza y, por ende, al conjunto de actividades económicas desarrollada en los mercados digitales.

En palabras de la ex Comisaria Europea Meglena Kuneva, “los datos personales son el nuevo petróleo de internet y la nueva moneda del mundo digital”. La información personal es poder y dinero, y es lo que ha llevado al nacimiento de un nuevo ecosistema de mercado con organizaciones que recopilan, fusionan, limpian, analizan, compran y venden datos de consumidores.

La tecnología y la migración a cada vez más a una vida en línea, ha propiciado la transimisión y revelación de manera masiva de grandes cantidades de información privada por parte de los usuarios de las diferentes plataformas, aplicaciones o cualquier dispositivo móvil. Con todo esto surge, la creación de un nuevo mercado: el mercado de datos personales. Este ecosistema es complejo y descentralizado (Olejnik et al. 2014), haciendo que no sea un mercado único y unificado.

Entre los diferentes términos y actores en este ecosistema, muy utilizados en nuestro día a día, encontramos los términos «big data», minería de datos (*data mining* en inglés), agregadores de datos (*data aggregators* en inglés), corredores de datos, etc., que juegan un papel fundamental en la economía digital. «Big data» se refiere a los enormes conjuntos de datos que no se pueden almacenar, procesar y acceder tan fácilmente. De hecho, y para poner en perspectiva la cantidad de datos que se generan y se procesan en el mundo, de acuerdo a Hilbert (2012) “estamos llegando al punto en que nuestra propia capacidad de procesar información rivaliza con la que la naturaleza utiliza para mantener una vida inteligente”. Esto implica que estamos viviendo un tiempo durante el cual se están alcanzando los extraordinarios órdenes de magnitud con los que la madre naturaleza procesa la información para sostener una vida inteligente. A través de lo que se conoce como «data mining», es posible identificar estructuras y patrones dentro de las cantidades masivas de datos, como puede ser hábitos de compra, preferencias políticas o el historial crediticio. Conociendo esa información, las empresas son capaces de generar importantes ingresos económicos.

Los datos son un activo valioso para las empresas (Moody and Walsh 1999).

La monetización del dato, que se refiere al uso de los datos para obtener un beneficio económico cuantificable, puede realizarse de dos formas primarias:

- La primera es interna y se enfoca en aprovechar los datos para mejorar las operaciones, la productividad, los productos y los servicios de una empresa, y también permite el diálogo continuo y personalizado con los clientes.

- La segunda ruta es externa e implica crear nuevas fuentes de ingresos al hacer que los datos estén disponibles para los clientes y socios.[12]

La forma de recolección y acceso es sencilla, y el precio por disfrutar de servicios en línea gratuitos es importante. De hecho, la mayoría de servicios en línea (Google, Facebook etc.) operan proporcionando servicios gratuitos a los usuarios, y a cambio, recopilan y monetizan su información personal. Este modelo operacional es inherentemente económico, ya que el bien que se comercializa y monetiza es la información personal (PI, por sus siglas en inglés).

Sin embargo, es esa misma accesibilidad y todas las actividades posteriores que se realizan con los datos personales, lo que hace que nazcan preguntas relacionadas con la privacidad y seguridad en este ecosistema, que tienen una relación innegable con la tecnología. Aquí es donde la privacidad entra en juego y donde los usuarios tienen una posición poco ventajosa. En resumidas cuentas, mientras exista un mercado para el intercambio de dicha

[12] Más información en: https://sloanreview.mit.edu/article/demystifying-data-monetization/

información personal entre empresas, los usuarios, que en realidad son los proveedores de dicha información, no estan invitados a la mesa negociadora (Spiekermann et al. 2012).

0.5 Privacidad y economía digital

En la "Era digital", hablar de privacidad lleva aparejado hablar de la economía digital. Esto se debe a que la economía digital está hasta cierto punto financiada por parte de las organizaciones que poseen grandes cantidades de datos no estructurados, algunos de carácter personal, que facilitan la orientación de las ofertas de productos por parte de las empresas a los consumidores individuales. Por ejemplo, los buscadores («search engines» en inglés) confían en los datos de búsquedas repetidas y pasadas para mejorar los resultados de búsqueda; los vendedores confían en compras pasadas y actividades de navegación para hacer recomendaciones de productos, y las redes sociales confían en vender datos a los vendedores para generar ingresos.

Una de las primeras definiciones de la economía digital la encontramos en Tapscott (1996). En esta nueva economía, las redes digitales y la infraestructura de comunicación proporcionan una plataforma global sobre la cual, las personas y organizaciones crean estrategias, interactúan, se comunican, colaboran y buscan información. Además del día a día de las personas, la digitalización ha transformado la manera en la que entendiamos los negocios; transformado industrias, incluido venta minorista, medios de comunicación y productos de entretenimiento.

Entre la nueva generación de empresas que han sabido adaptarse a las nuevas tecnologías y a los cambios del siglo XXI, el siguiente cuadro muestra el top 10 de marcas más valiosas del mundo en 2018, junto con la información del sector al que pertenecen y el valor de la marca.[13] El incremento en uso de datos, el desarrollo de la inteligencia artificial y de realidad

[13] Información disponible en: https://marketing4ecommerce.net/marcas-mas-valiosas-2018/

Table 1 Top 10 de marcas más valiosas del mundo en 2018.

Ranking	Marca	Sector	Valor de Marca 2018 (millones de $)
1	Google	Tecnológico	302.063
2	Apple	Tecnológico	300.595
3	Amazon	Retail	207.594
4	Microsoft	Tecnológico	200.987
5	Tencent	Tecnológico	178.990
6	Facebook	Tecnológico	162.106
7	Visa	Pagos	145.611
8	McDonald's	Comida rápida	126.044
9	Alibaba	Retail	113.401
10	AT&T	Telecomunicaciones	106.698

aumentada son aspectos que han favorecido a las marcas. Como se puede apreciar, ocho de las diez primeras marcas en este ranking son marcas que están relacionadas con la tecnología.

En Peitz and Waldfogel (2012) se estudian los cuatro pilares básicos para el desarrollo de la economía digital desde un punto de vista teórico y empiríco: infraestructuras, plataformas, transformaciones en las ventas, que abarca tanto la transformación de la venta tradicional como la nueva aplicación generalizada de herramientas tales como subastas generadas por el usuario y, las amenazas en el nuevo entorno digital. Como los autores apuntan, la privacidad y la piratería digital se encuentran entre los principales retos en los mercados digitales.

En los últimos años, la importancia de la economía digital en el PIB (Producto Interior Bruto) pone en relieve que es un innegable motor de crecimiento económico en el mundo. De acuerdo con Accenture Strategy, se estima que la economía digital supondrá el 20% del PIB en España para 2020.[14] Sin embargo, también es cierto que existen dificultades a la hora

[14] Más información; http://www.expansion.com/economia-digital/innovacion/2016/02/24/56cddc9446163fc1618b45f2.html

de medir la implicación real de la economía digital como una base importante de crecimiento en las economías. Y esto se debe, a que el PIB es esencialmente una medida de producción. “Si bien es adecuado cuando las economías están dominadas por la producción de bienes físicos, el PIB no captura adecuadamente la creciente participación y variedad de servicios y el desarrollo de soluciones cada vez más complejas en nuestra economía digital del siglo XXI”.[15]

En concreto, la dificultad para su medida se debe a dos razones: i) las formas tradicionales de medida de cualquier sector en el conjunto del PIB muestran la necesitad de un nuevo modelo para la imputación de productos digitales; y ii) por otro lado, de acuerdo a Ahmad and Schreyer (2016), se estarían dejando fuera de lo que actualmente se computa como PIB de la economía digital, muchas actividades y/o negocios, por su complejidad de control, rastreo o medida.

Además, la economía digital presenta un nuevo paradigma que complica su medición como motor de crecimiento y aportación al PIB, que es la existencia de externalidades digitales.[16] Los mecanismos por los que esto está sucediendo son complejos y en continua evolución. Más allá del aumento directo de la productividad que las empresas disfrutan de las tecnologías digitales, también se produce una cadena más profunda de beneficios indirectos, a medida que el impacto se extiende dentro de una empresa, a sus competidores y en toda su cadena de suministro.

En resumen, la economía digital juega un papel fundamental en la economía mundial y ha sido materia de estudio por muchos académicos y no académicos desde hace unos años. Su impacto real en el crecimiento de los países, aunque podría estar midiéndose de

[15] Información disponible en: https://medium.com/mit-initiative-on-the-digital-economy/re-thinking-gdp-in-the-digital-economy-8b309609f20c

[16] Oxford Economics. (2017). Digital Spillover.

forma incompleta y/o imprecisa, apunta a su importancia cada vez mayor como motor de crecimiento económico en los próximos años. Sin embargo, a medida que va creciendo en importancia, también se enfrenta a numerosas amenazas que ponen en riesgo su sostenibilidad y funcionamiento, como la piratería digital, violación y fuga de datos privados y los ciberataques. Esas amenazas, que en muchos casos afecta a los datos de carácter personal de millones de usuarios, necesita de cierta regulación y protección que den unas garantías de funcionamiento en el futuro. Y de esto se deriva la necesidad de un equilibrio entre privacidad y seguridad.

0.6 Regulación y protección de datos personales

El «Data Privacy Day» (día de la privacidad de los datos) o «Data Protection Day» (día de la protección de datos), como se conoce en Europa, es un día internacional que se celebra cada 28 de enero iniciado por el Consejo Europeo y reconocido por el senado de Estados Unidos, Canadá e Israel.[17,18,19] El objetivo del «Data Privacy Day» es incrementar la sensibilización y promover las mejores prácticas de privacidad y protección de datos.

Lo importante de la existencia de este acontecimiento internacional es el acuerdo e intención de caminar juntos hacia una ley de privacidad global. Esta celebración internacional ofrece, como se recoge en su manifiesto, “muchas oportunidades de colaboración entre gobiernos, industrias, instituciones académicas, organizaciones sin fines de lucro, profesionales de la privacidad y educadores” para asegurar que los principios de la protección de datos están todavía en línea con las necesidades actuales.[20]

[17] http://www.coe.int/t/dghl/standardsetting/dataprotection/Data$_protection_day_en.asp$

[18] https://googleblog.blogspot.com/2008/01/celebrating-data-privacy.html

[19] https://www.gov.il/he/departments/topics/international$_privacy_day$

[20] https://en.wikipedia.org/wiki/Data$_Privacy_Day$

Actualmente existen tres marcos operativos con respecto a la privacidad que, aunque no son mutuamente excluyentes, son suficientemente distintos entre si; están representados principalmente por China, Estados Unidos y Europa. Veámos brevemente que recogen las legislaciones para los dos casos últimos.

0.6.1 Regulación en la Unión Europea: RGPD

Despúes de seis años de debate y otros dos de haber sido promulgado, el 25 de mayo de 2018 entró en vigor el Reglamento General de Protección de Datos de la Unión Europea (GDPR, por sus siglas en inglés). La nueva legislación, enunciada antes de escándalos como el de Facebook-Cambridge Analytica, es una ley de privacidad multidimensional, robusta y muy estricta, con el objetivo de establecer nuevas reglas sobre la gestión y la forma de compartir los datos personales.[21] Entre las disposiciones del RGPD, destacan:

- Portabilidad de Datos: Requerirá que los usuarios den continuamente su consentimiento explícito de que acepten o no cómo se utiliza, comparte y analiza su información. Además, tendrán el derecho a poder darse de baja de los servicios sin detrimento, y se podrán llevar sus datos si asi lo desean, incluyendo los datos personales, los encriptados, los metadatos, la geolocalización, la IP, entre otras.

- Derecho (voluntario) al olvido. Los usuarios podrán exigir que se elimine la información que una empresa tenga de ellos, como si nunca hubieran usado el servicio.

- Derecho a la Rendición de Cuentas y exigencia de claridad en los términos. Los usuarios tendrán derecho a pedir explicaciones a las empresas sobre las decisiones que los algoritmos tomen sobre ellos. Además, se demanda que las condiciones sean inequívocas y específicas, por lo que claúsulas como "sus datos serán utilizados para mejorar nuestros servicios" serán insuficientes.

[21] Más información en: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

- Nuevas responsabilidades que derogan la autorregulación. El RGPD expande la responsabilidad de las companías a toda la cadena de procesamiento de datos, incluyendo compradores, proveedores, agentes y sub-contratistas. Además, exige la creación de un «Data Protection Office» (Oficina de procección de datos) para dar mantenimiento a la información resguardada y ser el punto de contacto ante autoridades.

- Cambios en el resguardo y filtrado de los datos. Obliga a las compañías a tener más "higiene de datos", al exigir que continuamente justifiquen para que tienen un dato. También da el mandato de resguardar la información únicamente en países que tengan legislaciones similares. Por otro lado, obliga a las empresas a informar cualquier fuga de datos en menos de 72 horas de haber sido identificada.

Lo interesante de esta regulación, es que en principio, el RGPD sólo aplica a ciudadanos europeos, pero la naturaleza global de Internet siginifica que casi todos los servicios estén afectados. Además, otro de los puntos más importantes, es que las empresas deben de dar la oportunidad a cada uno de los usuarios, de poder descargar todos los datos que la compañía posee sobre el mismo. Por ejemplo, la siguiente figura representa el mapa de visitas que yo misma realicé durante una estancia corta en EEUU. Este mapa es resultado de todos los datos de geolocalizaciones que Google Maps tiene almacenado de mis ubicaciones y que he podido descargar, de acuerdo a la legislación del RGPD. Los datos descargados, informan sobre las coordenadas precisas (longitud y latitud), dirección concreta, nombre oficial del edificio, código país y dato exacto de ubicaciones.

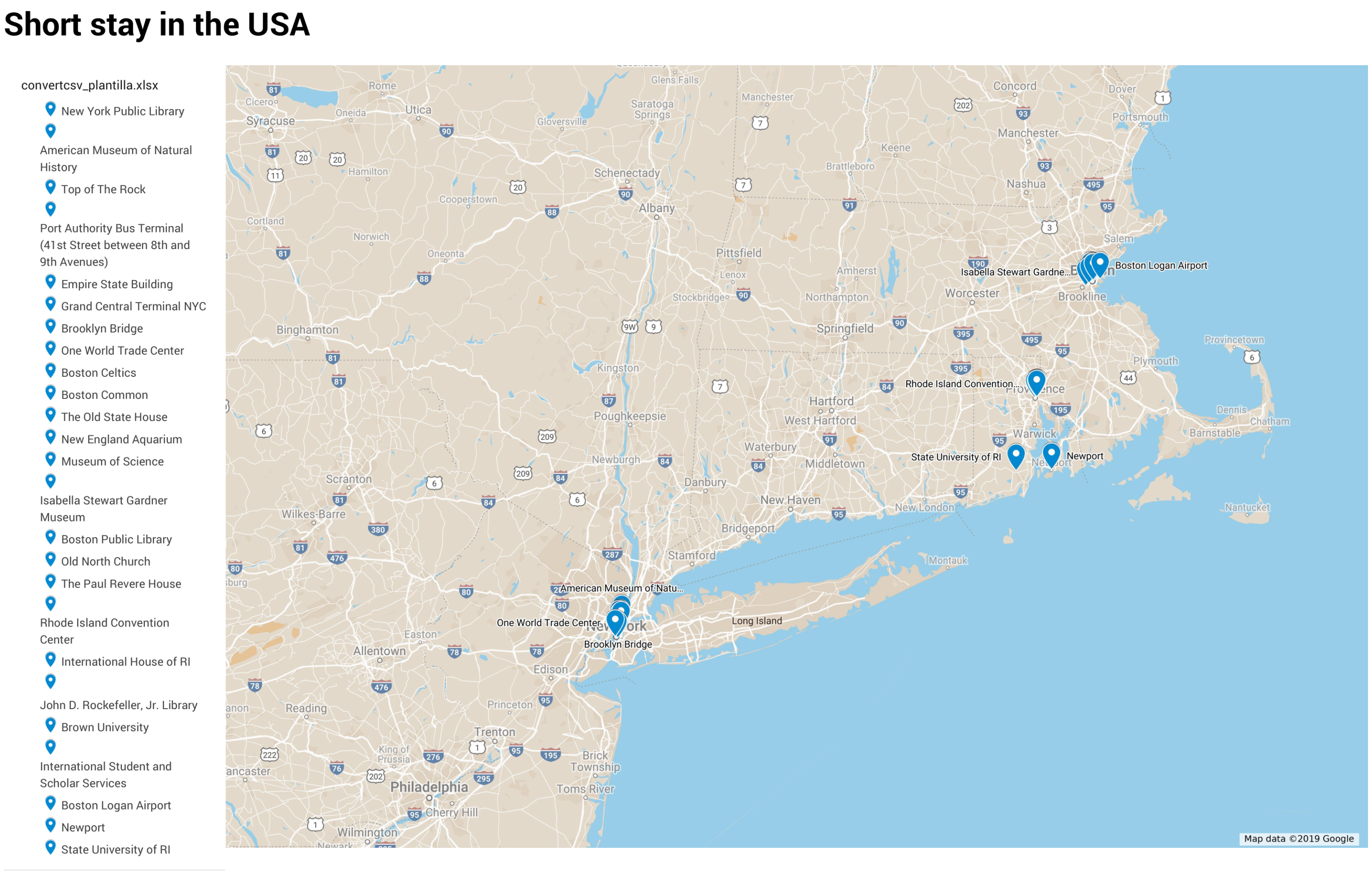
Esta regla o norma expande medidas anteriores de la Unión Europea , como el «privacy shield» (escudo de privacidad) y «data protection directive» (directiva de protección de datos).[22] En concreto, esta expansión va en dos direcciones:

[22] Página oficial para saber más información: https://www.privacyshield.gov/welcome

a) Cada vez que la empresa recopila datos personales de un ciudadano de la UE, necesitará el consentimiento explícito e informado de esa persona. La importancia de esto radica a que afecta a empresas con sede fuera de la UE.

b) El nuevo Reglamento de Protección de Datos afecta a las empresas y se merece toda la atención de la industria, porque se aumenta la cuantía de las sanciones, que pasan a ser de hasta 20 millones de euros o de una cuantia equivalente al 4% de la facturación anual del ejercicio financiero anterior de la compañia, lo cual supone un gran incremento con respecto a las sanciones que se tenía anteriormente.

Fig. 1 Estancia breve en EE.UU



Short stay in the USA

convertcsv_plantilla.xlsx

- New York Public Library
- American Museum of Natural History
- Top of The Rock
- Port Authority Bus Terminal (41st Street between 8th and 9th Avenues)
- Empire State Building
- Grand Central Terminal NYC
- Brooklyn Bridge
- One World Trade Center
- Boston Celtics
- Boston Common
- The Old State House
- New England Aquarium
- Museum of Science
- Isabella Stewart Gardner Museum
- Boston Public Library
- Old North Church
- The Paul Revere House
- Rhode Island Convention Center
- International House of RI
- John D. Rockefeller, Jr. Library
- Brown University
- International Student and Scholar Services
- Boston Logan Airport
- Newport
- State University of RI

Fuente: datos personales almacenados en Google Maps.

Sin embargo, el RGPD no ha estado libre de controversias, no sólo por el tema de la privacidad, sino por la explosión de costes que puede acarrear. El nuevo reglamento ha creado una importante demanda de profesionales de la privacidad, especialmente en las empresas que se enfrentan a la regulación de la privacidad por primera vez (Hughes and Saverice, 2018).[23] Además, de acuerdo con un estudio de la IAPP (International Association of Privacy Professionals) en conjunción con EY (Ernst & Young), las empresas de la Fortune 500 tendrán que destinar un promedio de 16 millones de dólares por corporación para cumplir la nueva regulación. El no hacerlo podría tener el coste de no tener acceso al mercado europeo, a mecanismos para compartir información o a servicios de terceros. A nivel de competitividad, podriá retrasar el desarrollo de tecnologías clave como la Inteligencia Artificial, donde China está ganando velocidad por el gigantesco volumen de información que generan sus habitantes.

0.6.2 Regulación en los EE.UU

La protección de datos en Estados Unidos es un escenario complejo. En Estados Unidos las normas y reglas para el tratamiento de datos varían entre estados, lo que implica diferentes niveles de seguridad y exigencias dependiendo de donde opere cada empresa. Hace año y medio, la protección de datos en Estados Unidos volvió a saltar a las portadas cuando Donald Trump firmó una ley para permitir a los proveedores de servicios de Internet (ISP, por sus siglas en inglés) vender datos de los consumidores sin consentimiento previo, invalidando así una norma impulsada por Obama que dictaba lo contrario. Aunque las empresas de Internet como Facebook y Google ya tenían acceso a este tipo de información y recopilaban datos de los consumidores sin tener que pedir permiso, ahora los ISP pueden ir más allá y acceder a la información completa sobre todos los sitios web que visita un consumidor.

[23] Hughes, T., & Saverice-Rohan, A. (2018). IAPP-EY Annual Privacy Governance Report 2018. Iapp-Ey, 1–132.

La Comisión Federal de Comunicaciones (FCC, una agencia independiente del gobierno de EE. UU) apoyó la decisión de invalidar esta parte del plan de la era Obama para regular Internet.[24] Este hecho supuso un paso atrás en la protección de datos personales. Defensores de los derechos de Internet, incluidos el ex-presidente del FCC, se han mostrado indignados por esta ley, que tachan de norma para beneficiar a las corporaciones frente a los internautas.

0.6.3 Diferencias entre la UE y los EE.UU

La gran diferencia entre Estados Unidos y la Unión Europea radica en las competencias a la hora de legislar, que en el caso de Europa recaen sobre el Parlamento Europeo y en el caso de Estados Unidos compete a los estados. Esto provoca que mientras que en la UE contamos con “una norma para gobernarlos a todos”, en EE. UU. cada estado cuenta con su propia legislación de protección de datos a la que debe acogerse.

A raíz de la aprobación del RGPD, y las presiones desde Europa para un endurecimiento de las normativas, varios estados modificaron sus leyes o introdujeron clausulas nuevas. Sin embargo, el gran cambio llegó en verano de 2018, cuando California aprobó el «California Consumer Privacy Act» (CCPA, por sus siglas en inglés), una norma inaudita en Estados Unidos por imponer, por primera vez, niveles de protección de datos muy similares a los presentes en el RGPD.[25]

Aunque el caso de California sigue siendo único, no es el único estado que ha endurecido su normativa en los últimos tiempos. Por ejemplo, Arizona ha introducido un nuevo sistema de notificación en caso de fallo de seguridad, mientras que Vermont ha aprobado leyes para

[24] Más detalles en: https://www.fcc.gov/document/fcc-releases-rules-protect-broadband-consumer-privacy

[25] Detalles sobre esta regulación disponible en: https://www.caprivacy.org/

exigir mayor transparencia a quienes tratan con información personal de los usuarios. [26,27]

Antes de la llegada del RGPD, la transferencia de datos entre Estados Unidos y la Unión Europea estaba regulada por el trado de «Privacy Shield» comentado anteriormente, que ofrecía a las empresas una forma de auto-certificarse anualmente para garantizar el cumplimiento de una serie de normativas de protección de datos.

Hoy en día, sin embargo, «Privacy Shield» ha quedado en un segundo plano por la obligatoriedad de cumplir con el RGPD. Aunque se revisa anualmente y ha sufrido múltiples modificaciones en los últimos tiempos para adecuarse a los estándares de la normativa europea, la auto-certificación sigue generando dudas por sus pocas garantías legales a efectos prácticos. Hoy en día, el escudo de privacidad ha quedado como un extra para aportar mayor fiabilidad a sus clientes.[28]

0.7 Objetivos de la Tesis

El objetivo principal de esta tesis doctoral es analizar la privacidad desde una perspectiva de la economía de la información y también como fuente de ineficiencias en el mercado. Para ello, se define la privacidad como un argumento en la función de utilidad que es idiosincrático e individual para cada uno de los consumidores en el mercado y que, además, varía a lo largo del tiempo. En la mayoría de los trabajos de la literatura, la importancia de la privacidad para el consumidor no está definida de manera nítida. Es decir, los consumidores no poseen una función de utilidad, en la que uno de sus argumentos sea la privacidad y es en este aspecto donde esta tesis quiere incidir. La tesis ofrece un análisis sobre las decisiones óptimas de los agentes

[26] Detalles sobre esta regulación disponible en: https://www.azleg.gov/ars/18/00552.htm

[27] Detalles sobre esta regulación disponible en: https://gizmodo.com/vermont-passes-first-of-its-kind-law-to-regulate-data-b-1826359383

[28] Fuente: https://es.mailjet.com/blog/news/noticiasproteccion-de-datos-eeuu/

económicos considerando la actual necesidad imperante de una **“demanda por privacidad”.**

En la Era digital del siglo XXI, tal como se ha descrito en esta introducción, esta marcada por la gran producción de datos (algunos datos personales) a gran escala. La vulnerabilidad y exposición se esta dando a un ritmo sin precendentes, produciendo grandes incentivos económicos para los poseedores de esos datos. Sin embargo, los proveedores de dichos datos, que son a menudo consumidores de contenido gratuito en las plataformas digitales, no están llamados a la mesa negociadora para poner valor exacto a su privacidad, y por ende, la delimitación entre la información que podría ser considerada pública o privada. Esto hace que se desarrolle una cierta inquietud o intranquilidad y el posterior detrimento de la confianza en los mercados digitales. Por tanto, la consideración de esta desazón en la toma de decisiones y la regulación, la protección y la ciberseguridad, son claves para la construcción de un mercado y una economía digital, con garantías y con futuro. Así mismo, por ejemplo, la costruccion del Mercado Digital Único en Europa («Digital Single Market» en inglés), contempla la ciberseguridad y la privacidad como pilares fundamentales para lograrlo.

En definitiva, esta tesis presenta las siguientes líneas de investigación. i) Modelizar el proceso de adquisición de información sobre las características del consumidor, por parte de la empresa o empresas, como un modelo de aprendizaje, con experimentación, siguiendo los modelos de la literatura de aprendizaje, (véase, Urbano 2018), en el que la variable relevante son los precios (discriminación de precios). Los precios, por un lado, juegan el papel de las variables de decisión para experimentar, es decir, reducir los beneficios de los primeros años para aumentar el de los beneficios futuros; por otro lado, sirven de señales en el mercado para los consumidores acerca de la cantidad de información que la empresas (el monopolista) tiene acerca de ellos y que utiliza para realizar discriminación de precios en mecados tracionales y mercados en Internet («Brick and Click Markets»). ii)

Estudiar los incentivos de las empresas en invertir en seguridad en las plataformas digitales (conocido como ciberseguridad) como una manera de incrementar las demandas futuras de los consumidores al aumentar su confianza. De igual manera, se investiga los incentivos a invertir en la precisión de la información acerca del "valor" de la privacidad de los consumidores y explorar la posibilidad posterior de la manipulación de la información en el mercado. Finalmente, iii) el estudio de una demanda por privacidad endógena a partir de la elección que los consumidores hacen sobre si comprar productos en mercados secuenciales, y en los que la compra en el primer mercado puede implicar la venta de sus datos personales en el segundo. Los consumidores pueden elegir no comprar («opt out option» en inglés) en la empresa en el primer mercado (empresa «upstream»), y evitar, por tanto, la venta de su información personal al segundo mercado (empresa «downstream»).

0.7.1 Resumen de los capítulos

En el **segundo Capítulo** se analiza el papel de la privacidad en la discriminación de precios en mercados digitales. La empresa puede operar en dos mercados, el digital y el no-digital (tradicional). El consumidor es racional e inteligente, y la privacidad entra como un argumento en su función de utilidad para aquellos que compran en el mercado digital. El juego es dinámico, contando con dos periodos, permitiendo valorar la evolución temporal de la privacidad y de los precios. El modelo construido es un modelo de extracción de señal sobre comportamiento del consumidor y de aprendizaje. El trabajo intenta mostrar como un monopolista utiliza el precio para señalizar la información privada perteneciente a los consumidores (previamente revelada en el primer periodo de la relación entre empresa y consumidor) para realizar discriminación de precios entre dos canales de compra diferentes («Brick and Click markets» en inglés) y apropiarse de la disposición máxima a pagar por los consumidores. Dado esto, podemos decir que los consumidores que van a comprar en un mercado on-line o a través de Internet, tienen a priori, una cierta inquietud por la privacidad que es desconocida cuando realizan su compra en el primer periodo. Los precios que diseñe el monopolista en el segundo periodo, servirán de señal al consumidor acerca del uso de su privacidad, y esto, junto a su experiencia en el primer periodo, determinará su demanda. Por otro lado, el monopolista recibe una señal con ruido (noisy signal) acerca de la privacidad media, lo que le permitirá ajustar el precio en ambos canales de venta. Con este trabajo, se modelizan los equilibrios bayesianos bajo varios escenarios y se analiza la revelación de la incertidumbre, así como la precisión de las señales que se reciben.

En el **tercer Capítulo** se estudia la decisión del monopolista a realizar una inversión en seguridad para de esta manera influir en los consumidores, aumentando su confianza en materias de seguridad y privacidad. La ciberseguridad en los mercados digitales, de acuerdo a la ENISA, hace refencia a múltiples áreas, desde la seguridad en las tecnologías de información a la seguridad del emplazamiento físico donde se encuentras los datos almacenados. Es por ello, que en este capítulo se estudia la decisión de inversión en seguridad en los mercados digitales de una manera global, contemplando cualquier movimiento que la empresa haga para este fin. La relación entre privacidad y seguridad es innegable, y esto se debe a que una de las formas de regular la seguridad es a través de la privacidad, ya que ambas comparten áreas en sus definiciones. De nuevo, el consumidor es racional e inteligente, y la privacidad entra como un argumento en su función de utilidad. Primeramente, se modeliza el equilibrio bayesiano en ausencia de inversión en seguridad, que sirve de escenario base, en un contexto dinámico pero finito con dos periodos. Más tarde, se modeliza el valor óptimo de inversión en seguridad, que se resuelve teniendo en cuenta el impacto que dicha inversión tendrá en las creencias del consumidor en el segundo periodo. Uno de los principales resultados es que el coste de inversión en seguridad se traslada a los consumidores a través del precio en el periodo 1. Además, se produce un aumento de la demanda en el periodo 2, debido a una mejor experiencia previa en términos de privacidad. Por último, se explora la posibilidad de una inversión del monopolista en la precisión de la información de la señal que recibe, con el objetivo de influir sobre el comportamiento del consumidor respecto a la privacidad. Esta posibilidad podría llevar a la empresa a tener incentivos a manipular la información en el mercado, dándole poder de mercado y resultando en un abuso de posición en detrimento de los consumidores.

El **cuarto Capítulo** estudia el comportamiento estratégico que realizan los consumidores, en un mercado formado por una empresa «upstream» o en un primer mercado, y una empresa «downstream» o en un segundo mercado, donde la empresa «upstream» puede tener unos ingresos por vender información personal de los consumidores a la empresa «downstream». En un primer escenario, los consumidores compran a ambas empresas y se derivan los beneficios, excendente del consumidor y el bienestar social cuando los consumidores se comportan de forma miópica o no se les da la posibilidad de no comprar en el primer mercado. Se obtiene el equilibrio bayesiano perfecto bajo el modelo de venta de información. En segundo lugar, se considera que los consumidores eligen a dónde comprar un bien, esto causa que algunos de los consumidores oculten sus tipos al no comprar en el primer mercado, lo que genera una demanda endógena por la privacidad y hace que la demanda del segundo mercado, sea más inelástica. La venta de de información da lugar a que la empresa en el primer mercado tenga incentivos a bajar el precio para propiciar que más gente compre y que por tanto, se pueda vender más información al segundo mercado. El resultado es un aumento del precio en el segundo mercado que extrae la máxima disposición a pagar de los consumidores. Se determina si la venta de información mejora los beneficios, el excedente del consumidor y el bienestar total, y se analiza las consecuencias de permitir que los consumidores opten por no ofrecer su información a la empresa en el primer mercado.

El **quinto Capítulo** ofrece las conclusiones de esta tesis doctoral.

Chapter 1

Introduction: a general approach

1.1 The right to privacy in the digital age

On December 18th, 2013, the General Assembly of the United Nations approved the resolution entitled *The right to privacy in the digital age* for all people.[1] This resolution establishes that indiscriminate global surveillance implies a serious violation of human rights, and seeks to reaffirm the fundamental principles adopted in the Universal Declaration of Human Rights of 1948 (article 12), the International Covenant on Civil and Political Rights (article 17), and the International Covenant on Economic, Social and Cultural Rights. In particular, this resolution makes it clear that "unlawful or arbitrary surveillance and/or interception of communications, as well as the unlawful or arbitrary collection of personal data, as highly intrusive acts, violate the right to privacy, can interfere with other human rights, including the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association, and may contradict the tenets of a democratic society".

[1] Resolution available on:
https://www.ohchr.org/SP/HRBodies/HRC/RegularSessions/Session34/Pages/ResDecStat.aspx.

Recognizing privacy as a fundamental right in the digital age highlights the existence of antecedents that denote clear harm and vulnerability for all. Among the vulnerabilities and the possible costs to which people can face, due to a misuse of personal information, they include, among others:

a) Identity theft: the deliberate use of someone else's identity, usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name. It can be given from the most common case such as identity theft in the driving license (Driver's License Identity Theft) or identity theft in jobs (Employment Identity Theft). Generally, your personal data is used as your ID.[2]

b) Risk of abuse: personal and professional embarrassment, restricted access to labor markets, and restricted access to best value pricing, (Chaudhry et al. 2015).

c) Privacy breaches: an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so. In the last years, there are very striking cases in this context as Yahoo in 2013 with 3 billion stolen data, eBay in May 2014 with 145 million or Uber in 2016 with 57 million.[3]

The attainment of a balance between privacy and security, and how it affects freedom and democracy, is one of the paradigms most studied today.[4]

[2] 20 types of identity theft and fraud: https://www.experian.com/blogs/ask-experian/20-types-of-identity-theft-and-fraud/.

[3] The biggest data breaches of the 21st century. https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

[4] As an example of these efforts in order to look for this achievement: the fourth Princeton Fung Global Forum, held in March 2017, in Berlin. https://www.princeton.edu/news/2017/04/13/princeton-fung-global-forum-asks-if-liberty-can-survive-digital-age.

1.2 A brief history of Privacy

To understand the problem we face with a possible violation of our privacy in digital environments, and its effect on freedom and democracy, we must first approach a couple of concepts: the public and the private. This dichotomy is closely linked to freedom. Depending on what our conception of what is public or private, and the evaluation that we make of one or another area, we understand freedom, so we will defend it. And in turn, according to the conception that we have of freedom, we will thus value one and another aspect of our life, and, therefore, our privacy.

On the other hand, it is not strange that the resolution indicates that the non-defense of privacy in the digital age can be contrary to the precepts of a democratic society. In fact, the origins of the first notions of privacy, and of the distinction between private and public, can be found in Ancient Greece. It was with the birth of the "polis" (Greek denomination to the cities), and more concretely with the democracy of Pericles, where these concepts of freedom, democracy and the polarity between private and public were consolidated. An example of this distinction between the public and private can be found in the Greek literature and in the hand of Homer, with his famous work *The Odyssey*.[5] The privacy issue can already be seen in the writings of Socrates and other philosophers too.[6] For example, Aristotle was the one who made the famous distinction between the public sphere corresponding to political activity, and the private sphere of family and domestic life.

Democracy is a basic ingredient in the defense of freedom and thus, privacy. Privacy was born of democracy, and "these delineations could not have been made in the theocracies of the ancient Near East, because in such cultures god-as-ruler permeates everything and no

[5] The fist explicit opposition between public and private in Greek literature occurs in the Odyssey, pags. 8-9.

[6] Moore Jr., B.: Studies in Social and Cultural History. M.E. Sharpe, Inc., Armonk (1984)

notion of the private is possible", as the author Susan Ford Wiltshire notes.[7]

In its most fundamental form, privacy was related to the most intimate aspects of the human being. Almost all domestic activities were carried out in front of family and friends, and privacy could mean getting away from society. This makes sense if we think about the origins of humanity, where the first humans were organized in small groups, where the desire for survival did not give rise to the need for privacy. There has always been, as pointed out by Holvast (2007), a kind of conflict between the subjective desire for solitude and seclusion, and the objective to depend on others. Furthermore, this distinction was reflected, as the historian Samantha Burke points out, even in the architecture of the houses, where an attempt was made to balance natural light with the minimum possible exposure.[8]

On the contrary, later, at the time of the Roman Empire, we found ostentatious houses far from the cities of the rich, which were characterized by wide open spaces that permited to see and hear what was happening in their interiors. The houses were characterized by having walls where you could hear even the most subtle sounds.

In later centuries, privacy has been related to the home, family life and personal correspondence. In fact, from the fourteenth century until the beginning of the nineteenth century, many cases were brought to the court related to listen or to open and read personal letters. A very significant example of this in the nineteenth century was the scandal of espionage of the post office in 1844, when the Italian nationalist Giuseppe Mazzini accused the British government of opening its letters. Confirmation of his suspicion caused him to file a complaint with the court whose main appeal was based on two key attributes of the letters: that

[7] Ford Wiltshire, S.: Public and private in Vergil's Aeneid, op. cit. "Polarity appeared in the Greek language, however, as early as Homer and it developed in the democratic period of classical Athens. [. . .]"

[8] Burke, Samantha. Delos: Investigating the notion of privacy within the ancient Greek house. Diss. University of Leicester, 2000.

they were private, and that letters contained secrets. The most important aspect of this event was, without a doubt, and as Kate Lawson points out, that these two claims about the letters helped to create definitions of privacy in personal communications and that the scandal led to the emergence of questions about reasonable expectations of privacy that are at the same time Victorian and clearly contemporary.[9]

Since the end of the 19th century, the emphasis given to the term of privacy was directed more towards personal information and the control of it. And that's why, privacy as we usually understand it does not have much more than 200 years. Even today, despite being a common concept, it is difficult to give a final definition of privacy. And what is more relevant, beyond the global consensus on the importance of privacy and data protection, there is no universal definition of it (Kasneci 2008).

1.3 What does privacy mean?

We find among the first definitions of the concept of privacy, as we understand it today, the one in Warren and Brandeis' famous essay of 1890 (Brandeis and Warren 1890), in which they describe privacy "as the right to be let alone". Although, as established by , privacy means different things to different people. One of the most famous and accepted definitions is the one by Westin and Ruebhausen (1967), iwhere privacy is stated as "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extend information about them is communicated to others". In this line, Boyd (2010) said that fundamentally "privacy is about having control over how information flows". On the other hand, privacy has been defined as an aspect of dignity, and ultimately, human freedom

[9] Kate Lawson. Personal Privacy, Letter Mail, and the Post Office Espionage Scandal, 1844. Branch: Britain, Representation and Nineteenth-Century History. Ed. Dino Franco Felluga. Extension of Romanticism and Victorianism on the Net. Web. 16 March 2013.

(Schoeman 1992).

The importance in its definition stand in setting the limits between what is private and what is public. Because from the definition lies the importance for the regulation and protection of personal data.

From a regulatory point of view, the need for a precise definition of this concept is vital. Security in digital markets, what is commonly known as security in information technology or cybersecurity, and its indirect regulation through privacy, has required a greater effort when defining the limits that mark privacy, or, in other words, the boundaries between the self and the others, between the private and the public.

In this aspect, and in order to create a common path in the definitions, the European Union Agency for Network and Information Security (ENISA) in a recent report highlights the importance of the standardization of concepts such as privacy or cybersecurity. Its importance is maximum when it comes to developing standards that allow for greater international adaptation, transfer of good practices among organizations, promotion of integration and/or interoperability of systems.[10]

1.4 Markets for personal data

The Internet age is accompanied by a new way of conceiving privacy, adapted to the realities of a global and digital environment. Contrary to what one might think, personal databases of consumers have existed during the twentieth century (Smith 2000). However, due to the progress of information technology and the emergence of the Internet, the scope and reach of those databases have grown considerably. Nowadays, you can store a variety of very large

[10] Union, E.,& For, A. (2018). Guidance and gaps analysis for European standardisation.

and rich personal information.

The question is: What kind of information can be stored? From our profiles and demographic data, bank accounts to medical records or employment data. Our web searches, the sites we visited, our likes and dislikes and purchase histories. Our tweets, texts, emails, phone calls and photos as well as coordinates of our real world locations.

According to the World Population stats, 56.1% of the world's population has internet access, and 81% of the developed world. Therefore, greater access to the Internet generates more personal data and, therefore, greater potential to do business with them.[11] However, we are still not fully aware of the great exposure we have in digital environments. As the World Economic Forum points out in its report Rethinking Personal Data (2012), most people do not have enough knowledge about what can happen with their personal data when using smartphones or the Internet. Consequently, this has effects on the digital environment: this leads to fear, uncertainty and the decline of trust and, therefore, to the economic activities developed in digital markets.

In words of the former European Commisioner Meglena Kuneva, "personal data is the new oil of the Internet and the new currency of the digital world". Personal information is power and money, and that is what has led to the birth of a new market ecosystem of organizations that gather, merge, clean, analyze, buy and sell consumer data.

Technology and the migration to an increasingly online life, let to the massive transmission and disclosure of large amounts of private information by users of different platforms, applications, or any mobile device. These factors have determined the creation of a new market: the personal data market. This ecosystem is complex and decentralized (Olejnik

[11] Statistics available on: https://www.internetworldstats.com/stats.htm

et al. 2014), making it not a unique and unified market.

There are different terms and players in this ecosystem widely used in our daily life such as big data, data mining, data aggregators, data brokers, etc., which play a fundamental role in the digital economy. Big data refers to huge data sets that can't be as easily stored, processed and accessed as former collections of data. In fact, and to put into perspective the amount of data that is generated and processed in the world, according to Hilbert (2012) "we are reaching the point at which our own capacity to process information rivals that which nature uses to sustein intelligent life". This implies that we are living through a time during which we are reaching the point the extraordinary orders of magnitude with which mother nature processes information in order to sustain intelligent life. It is through what is known as data mining, that it is possible to identify structures and patterns within the massive amounts of data, such as buying habits, political preferences or credit history. Companies are able to generate important economic profits knowing this information.

Data is a valuable asset for companies (Moody and Walsh 1999).

The monetization of the data, which refers to the use of data to obtain significant economic profits, can be done in two primary ways:

- The first one is internal and focuses on leveraging data to improve operations, productivity, and products and services, and also enable ongoing, personalized dialogs with customers.
- The second one is external and involves creating new revenue streams by making data available to customers and partners.[12]

The form of collection and access is simple, and the price for enjoying free online services are important. Indeed, most online services (Google, Facebook etc.) operate by providing a

[12] Find out more in: https://sloanreview.mit.edu/article/demystifying-data-monetization/

service to users for free, and in return they collect and monetize personal information (PI) of the users. This operational model is inherently economic, as the good being traded and monetized is PI.

However, it is this accessibility, and all subsequent activities that are carried out with personal data, which leads to the emergence of questions related to privacy and security in this ecosystem, having an undeniable relationship with technology. This is where privacy comes to play and where consumers have an unfavorable position. In short, while there is a market for trading such personal information among companies, the users, who are actually the providers of such information, are not asked to participate in the negotiation table (Spiekermann et al. 2012).

1.5 Privacy and digital economics

In the digital age, to talk about privacy involves talking about the digital economy. This is due to the fact that the digital economy is financed to a certain extent by organizations with large amounts of unstructured data, some of a personal nature, which facilitate the best adaptation of product offers to individual consumers. For example, search engines rely on data from repeated and past searches to improve search results, sellers rely on past purchases and browsing activities to make product recommendations, and social networks rely on selling data to sellers to generate revenues.

One of the first definitions of the digital economy is found in Tapscott (1996). In this new economy, digital networks and communication infrastructure provide a global platform on which people and organizations create strategies, interact, communicate, collaborate and seek information. In addition, digitalization has transformed the way we understand business; it

Table 1.1 Top 10 most valuable brands in the world in 2018.

Ranking	Brand	Sector	Brand Value 2018 (millions of $)
1	Google	Technology	302,063
2	Apple	Technology	300,595
3	Amazon	Retail	207,594
4	Microsoft	Technology	200,987
5	Tencent	Technology	178,990
6	Facebook	Technology	162,106
7	Visa	Payments	145,611
8	McDonald's	Fast Food	126,044
9	Alibaba	Retail	113,401
10	AT&T	Telecommunication	106,698

has transformed industries including retail, media and entertainment products.

Companies have adapted to new technologies and to changes of the 21st century. Table 1.1 shows the top 10 most valuable brands in the world in 2018 along with the information of the sector they belong to and the value of the brand.[13] The increase in the use of data, the development of artificial intelligence and augmented reality are aspects that have favored brands. As can be seen, eight of the top 10 brands in this ranking are brands that are related to technology.

Peitz and Waldfogel (2012) study four main topics in the development of the digital economics from an empirical and theoretical point of view: infrastructure; standards and platforms; transformations of traditional selling and new widespread application of tools such as auctions, user generated contents; and, threats in the new digital environment as digital piracy and privacy in the digital markets.

[13] Information available on https://marketing4ecommerce.net/marcas-mas-valiosas-2018/

The importance of the digital economy in the GDP (Gross Domestic Product), an essential index to measure the economic growth of the countries, emphasizes that it is an undeniable engine of economic growth in the world. According to Accenture Strategy, it is estimated that the digital economy accounts for 20 % of GDP in Spain by 2020.[14] However, it is also true that there are difficulties in measuring the real implication of the digital economy as an important aspect for growth in the economy. And this is due to the fact that GDP is essentially a measure of production. While suitable when economies were dominated by the production of physical goods, GDP does not adequately capture the growing share and variety of services and the development of increasingly complex solutions in our 21st-Century digital economy.[15]

In particular, the difficulty in measuring it is due to two reasons: i) the traditional forms of measurement of any sector in the GDP as a whole show the need for a new model for the imputation of digital products; and ii) on the other hand, according to Ahmad and Schreyer (2016), many activities, and/or businesses, due to their complexity of control, tracking or measurement will be left out of what is currently computed as GDP of the digital economy.

In addition, the digital economy presents a new paradigm that complicates its measurement as an engine of growth and contribution to GDP, which is the existence of digital spillovers.[16] The mechanisms by which this is happening are complex and evolving. Over and above the direct productivity boost that companies enjoy from digital technologies, a more profound chain of indirect benefits also takes place as the impact spillovers within a firm, to its competitors, and throughout its supply chain.

[14] Full text available on http://www.expansion.com/economia-digital/innovacion/2016/02/24/56cddc9446163fc1618b45f2.html

[15] To see more https://medium.com/mit-initiative-on-the-digital-economy/re-thinking-gdp-in-the-digital-economy-8b309609f20c

[16] Oxford Economics. (2017). Digital Spillover.

In summary, the digital economy plays a fundamental role in the world economy and has been the subject of study by many academics and non-academics for some years. Its real impact on the growth of the countries, although it could be incompletely and/or imprecisely measured, points to its growing importance as an engine of economic growth in the upcoming years. However, as it grows in importance, it also faces numerous threats that set its sustainability and functioning at risk, such as digital piracy, violation and leakage of private data and cybersecurity. These threats, which in many cases affect the personal data of millions of users, require some regulation and protection that can establish operating guarantees in the future. Finally, there is a challenge, the need for a balance between privacy and security in our digital age.

1.6 Regulation and protection of personal data

The Data Privacy Day or Data Protection Day, as it is known in Europe, is an international day that is celebrated every 28th of January initiated by the European Council and recognized by the United States Senate, Canada and Israel.[17,18,19] The objective of the Data Privacy Day is to increase awareness and promote the best privacy and data protection practices.

The important thing about the existence of this international event is the agreement and intention to walk together towards a law of global privacy. This international celebration offers, as stated in its manifesto, "many opportunities for collaboration between governments, industries, academic institutions, non-profit organizations, privacy professionals and educators" to ensure that the principles of data protection are still in line with current needs.[20]

[17] http://www.coe.int/t/dghl/standardsetting/dataprotection/Data$_{p}rotection_{d}ay_{e}n.asp$

[18] https://googleblog.blogspot.com/2008/01/celebrating-data-privacy.html

[19] https://www.gov.il/he/departments/topics/international$_{p}rivacy_{d}ay$

[20] https://en.wikipedia.org/wiki/Data$_{P}rivacy_{D}ay$

Nowadays, there are three operational frameworks with respect to privacy, while not mutually exclusive, are sufficiently different from each other. They are mainly represented by China, the United States and Europe. Let us see briefly the legislation for the last two cases.

1.6.1 Regulation in EU: GDPR

After 6 years of debate and another 2 years of having been promulgated, on May 25, 2018, the General Data Protection Regulation (GDPR) of the European Union came into force. The new legislation, spelled out before scandals such as Facebook-Cambridge Analytica, is a multidimensional privacy law, robust and with an almost radical strictness with the aim of putting new rules on the management and the way of sharing personal data.[21]

Among the provisions of the GDPR, the following stand out:

- Data Portability: Require users to continuously give their explicit consent that they accept or not how their information is used, shared and analyzed. In addition, users will have the right to be able to unsubscribe from services without detriment, and they can take their data if they wish, including personal data, encrypted data, metadata, geolocation, and IP among others.

- Right to be forgotten: The users could demand that the information that a company has of them be eliminated, as if they had never used the service.

- Right to access and clarity in terms: Users will have the right to request explanations from companies about the decisions that algorithms make about them. In addition, it is demanded that the conditions be unequivocal and specific, so that clauses like "your data will be used to improve our services" will be insufficient.

[21] More information in https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

- New responsibilities that repeal self-regulation: The GDPR expands the responsibility of the companies to the entire chain of data processing, including buyers, suppliers, agents and sub-contractors. In addition, it requires the creation of a Data Protection Officers to maintain the protected information and be the point of contact with authorities.

- Changes in the protection and filtering of data: It forces the companies to have more "data hygiene" by demanding that they continually justify why they have a piece of information. It also gives the mandate to safeguard the information only in countries that have similar legislation. On the other hand, it obliges companies to report any data breach in less than 72 hours after being identified.

The interesting thing about this regulation is that, in principle, the GDPR only applies to European citizens, but the global nature of the Internet means that almost all services are affected. Furthermore, another of the most important points is that companies should give the opportunity to each user, to be able to download all the data that the company has about him. For example, Figure 1.1 represents the map of visits that I made during a short stay in the USA. This map is the result of all geolocation data that Google Maps has stored from my locations in 3 months. I have been able to download the data file with this personal data according to the GDPR legislation. Downloaded data contains information regarding to the precise coordinates (longitude and latitude), specific address, official name of the building, country code and exact location data.

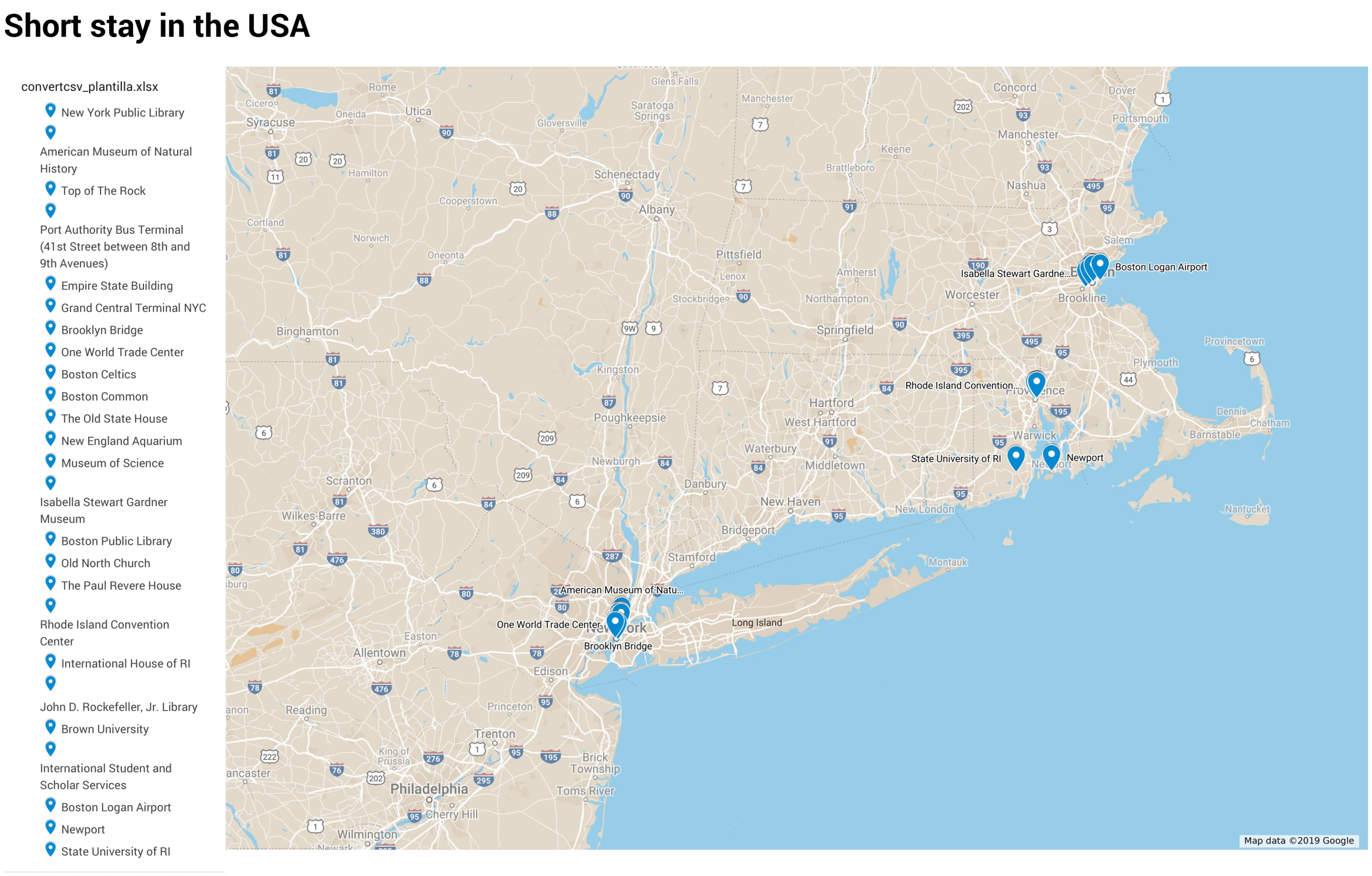
This rule, GDPR, expands on previous measures of the European Union, such as the privacy shield and data protection directive.[22] Specifically, this expansion goes in two directions:

[22] Official Website: https://www.privacyshield.gov/welcome

a) Every time the company collects personal data from an EU citizen, it will need the explicit and informed consent of that person. The importance of this is that it affects companies based outside the EU.

b) The GDPR's penalties are severe enough to get the entire industry's attention; 4% of a company's global turnover or $ 20 million whichever is larger, which represents a large increase with respect to the sanctions that were previously held.

Fig. 1.1 Short stay in the USA



Short stay in the USA

convertcsv_plantilla.xlsx

- New York Public Library
- American Museum of Natural History
- Top of The Rock
- Port Authority Bus Terminal (41st Street between 8th and 9th Avenues)
- Empire State Building
- Grand Central Terminal NYC
- Brooklyn Bridge
- One World Trade Center
- Boston Celtics
- Boston Common
- The Old State House
- New England Aquarium
- Museum of Science
- Isabella Stewart Gardner Museum
- Boston Public Library
- Old North Church
- The Paul Revere House
- Rhode Island Convention Center
- International House of RI
- John D. Rockefeller, Jr. Library
- Brown University
- International Student and Scholar Services
- Boston Logan Airport
- Newport
- State University of RI

Source: personal data stored in Google Maps.

However, the GDPR has not been free of controversies, not only because of the issue of privacy, but because of the explosion of costs that it will bring. The new regulation has created a significant demand for privacy professionals, especially in companies that face privacy regulation for the first time (Hughes and Saverice-Rohan 2018). Moreover, according to the study by the IAPP (International Association of Privacy Professionals) in conjunction with EY (Ernst & Young), the Fortune 500 Companies will have to allocate an average of 16 million dollars per corporation to comply with the new regulation. The failure to do so could have the cost of not having access to the European market, mechanisms to share information or services of third parties. At the level of competitiveness, it could delay the development of key technologies such as artificial intelligence, where China is gaining speed due to the gigantic volume of information generated by its inhabitants.

1.6.2 Regulation in the US

Data protection in the United States is a complex scenario. In the United States, standards and rules for data processing vary between states, which implies different levels of security and demands depending on where each company operates.

In 2017, data protection in the United States came back to the front pages when Donald Trump signed a law to allow Internet Service Providers (ISP) to sell consumer data without prior consent, invalidating a norm promoted by Obama that dictated otherwise. Although Internet companies such as Facebook and Google already had access to this type of information and collected data from consumers without having to ask for their permission, now ISPs can go further and access the full information on all websites they visit.

The Federal Communications Commission (FCC, an independent agency of the US government) supported the decision to invalidate this part of the Obama era plan to regulate the Internet.[23] This fact was a backward step in the protection of personal data. Defenders of the Internet rights, including the former president of the FCC, have been outraged by this law, which is considered to benefit corporations against the Internet users.

1.6.3 Differences between the EU and the United States

The great difference between the United States and the European Union lies in the powers to legislate, which in the case of Europe fall on the European Parliament and in the case of the United States it is up to the states. This fact causes that, while in the EU we have a rule to govern them all, in the US each state has its own data protection legislation.

Following the approval of the GDPR, and pressures from Europe for a tightening of regulations, several states modified their laws or introduced new clauses. However, the big change came in the summer of 2018, when California passed the California Consumer Privacy Act (CCPA), an unprecedented standard in the United States for imposing, for the first time, levels of data protection very similar to those present in the GDPR.[24]

Although the case of California remains unique, it is not the only state that has tightened its regulations in recent times. For example, Arizona has introduced a new notification system in the event of a security breach, while Vermont has passed laws to require greater transparency for those who deal with users' personal information.[25], [26]

[23] More info in https://www.fcc.gov/document/fcc-releases-rules-protect-broadband-consumer-privacy

[24] More info in https://www.caprivacy.org/

[25] Details available on https://www.azleg.gov/ars/18/00552.htm

[26] Full text available on https://gizmodo.com/vermont-passes-first-of-its-kind-law-to-regulate-data-b-1826359383

Prior to the arrival of the GDPR, the transfer of data between the United States and the European Union was regulated by the Privacy Shield mentioned above, which offered companies a way to self-certify annually to ensure compliance with a series of regulations of data protection. Nowadays, however, Privacy Shield has been left in the background due to the obligation to comply with the GDPR. Although it is reviewed annually and has undergone multiple modifications in recent times to adapt to the standards of European regulations, self-certification continues to generate doubts because of its few legal guarantees for practical purposes. Today, Privacy Shield has remained as an extra to provide greater reliability to its customers.[27]

1.7 Objectives of the Thesis

The main objective of this doctoral thesis is to analyze privacy from an informational perspective and source of inefficiencies in the market. For this, privacy is defined as an argument in the utility function that is idiosyncratic and individual for each of the consumers in the market, and, in addition, varies over time. In the related literature, the importance of privacy for the consumer is not clearly defined. That is, consumers do not have a utility function in which one of their arguments is privacy, and it is in this aspect where this thesis wants to influence. The thesis offers an analysis of optimal decisions of economic agents considering the current prevailing need for a **demand for privacy**.

In the digital era of the 21st century, as has bees explained in this introduction, it is characterized by the large production of data (some of them of private nature) on a large scale. The vulnerability and exposure is occurring at an unprecedented rate, producing great economic incentives for the owners of these data. However, the providers of such data, who are often consumers of free content on digital platforms, are not called to the negotiating table to put or negotiate an exact value on their privacy, and therefore, the

[27] Source: https://es.mailjet.com/blog/news/noticiasproteccion-de-datos-eeuu/

delimitation between the information that could be considered public or private. This leads to the development of concerns and the subsequent reduction of confidence in digital markets. Therefore, the consideration of these concerns in decision-making and regulation, protection and cybersecurity, are key to the construction of a market and a digital economy with guarantees and with a future. Likewise, for example, the construction of the Digital Single Market considers cybersecurity and privacy as fundamental pillars to achieve it.

To sum up, this thesis presents the following main objectives: i) To model the process of acquisition of information -company's learning process- on consumers' characteristics following the models of the learning literature (see Urbano 2018), in which the relevant variable is prices (price discrimination). On the one hand, prices play the role of the decision variables to experiment, that is, reduce the profits at the beginning to increase them in the future. So far, they have not been modeled as such. On the other hand, they serve as signals in the market for consumers about the amount of information that companies have about them, and that they use to price discriminate in traditional markets and on the Internet (Brick and Click Markets). ii) To study companies' incentives to invest in security in digital platforms (known as cybersecurity) as a way to increase the future demands of consumers by increasing confidence. Similarly, the incentives to invest in the accuracy of the information about the "value" of consumers' privacy and explore the possibility of manipulation of information in the market. Finally, iii) To study a demand for endogenous privacy in the marketplace. This fact is analyzed from the choice that consumers make about whether to buy products from two companies that operate in two succesive monopolies. The firm in the first market can obtain information from consumers and sell it to the second monopolist. Consumers can choose to opt out in the first market (upstream firm) and avoid, therefore, the sale of their personal information to the second market (downstream frim).

1.7.1 Chapter summaries

Chapter two analyzes the role of privacy in channel-based price discrimination and price dispersion. The company operates in two markets, online (on the Internet) and offline (traditional market). The representative consumer is rational and intelligent, and privacy enters as an argument in its utility function for those who buy in the digital market. The game is dynamic, with two periods, allowing to assess the temporal evolution of privacy and prices. The model analyzed is a model of signal extraction on consumer behavior and learning. The Chapter studies how a monopolist uses the price to signal the private information belonging to the consumers (previously revealed in the first period of the relationship between company and consumer) that is being used in order to practice price discrimination between the two purchase channels, Brick and Click markets. Given this, we can say that consumers who buy in an online market or through the Internet have, a priori, a concern for privacy that is unknown when they make their purchase in the first period. The prices that the monopolist designs in the second period will serve as a signal to the consumer about the use of their privacy, and this, together with their experience in the first period, will determine their demand. On the other hand, the monopolist receives a private signal with noise (noisy signal) about the average privacy, which will allow him to adjust the price in the online channel. In this Chapter, the Bayesian equilibria are modeled under various scenarios and the uncertainty revelation is analyzed, as well as the precision of the signals that are received.

Chapter three investigates the monopolist's decision to invest in security in digital markets in order to influence consumers increasing their confidence in matters of security and privacy. Cybersecurity in digital markets, according to the ENISA, refers to multiple areas from security in information technologies to the security of the physical location where the stored data is located. For that reason, the investment decision in security in digital markets is studied in a globally contemplating any movement that the company makes for this purpose. The relationship between privacy and security is undeniable, and this is because one of the ways to regulate security is through privacy, since both share areas in their competition. Again, the representative consumer is rational and intelligent, and privacy enters as an argument in its utility function. First, the Bayesian equilibrium is modeled in the absence of security investment, which serves as the base scenario, in a dynamic but finite context with two periods. Later, the optimal value of investment in security is modeled, which is solved taking into account the impact that this investment would have on consumer beliefs in the second period. One of the main results is that the cost of investment in security is transferred to consumers through the price in period 1. Moreover, a higher expected demand results in period 2, due to a better previous experience in terms of privacy. Finally, we explore the possibility of an inversion in the precision of the information that the monopolist receives. This strategy could lead the company to have incentives to manipulate the information in the market resulting in an abuse of position to detriment of consumers.

Chapter four studies the strategic behavior of consumers in a market composed by an upstream market and a downstream market. We consider consumers choosing whether to buy a good when they know that information about them can be sold to another firm selling another good they might also buy. Firstly, we analyze the scenario where consumers buy from both companies and we derive the benefits, the consumer surplus, and the social welfare when consumers behave in a myopic way or they are not given the possibility of not buying from the upstream company. The subgame perfect bayesian prices are derived under the model of information sales as well as its prices. Secondly, consumers are offered an opt-out option to avoid having their information sold. This causes some consumers to hide their types by not buying the first good, which delivers an endogenous demand for privacy and renders the demand for the second good more inelastic. The information sales give the firm in the first market a greater incentive to harvest consumers to sell to the second firm, and, therefore, the upstream price can go down while increasing the downstream price. We determine whether information selling improves upstream profits, consumer surplus, and total welfare, and we find the consequences of allowing consumers to opt out of having their information sold by the upstream firm.

Chapter five offers the conclusions of this doctoral thesis.

Chapter 2

Consumers' privacy concerns and price dispersion among channels

2.1 Introduction

We all live in a networked society, where we perform a set of routine activities thanks to our devices and different applications that allow online shopping, communication and social relations, access to global information instantly, geolocations, etc.

Lately, different media point out the great public exhibition to which the new digital age obliges us. Many news emphasize the vulnerability in privacy that this display entails, even questioning devices that resort to facial recognition, that is, the ability to read faces.[1] This fact, consequently, has been developing privacy concerns in the whole society where privacy and its definition has become a moving target over time, difficult to specify, and in expensive treasure to cherish. In words of Danah Boyd, "The balance of forces has shifted in the networked age. People are now public by default and private by effort".

From the economic point of view, this production of data are being recorded, stored and analyzed for the sake of obtaining a competitive advantage for those who own them. Yet,

[1] https://www.economist.com/leaders/2017/09/09/what-machines-can-tell-from-your-face

there is still no general agreement to establish the social benefit of the participants involved. The online presence of companies has become a strategic necessity, creating, therefore, great opportunities and challenges for them thanks to the rapid development of information technology. Given the economic interests, a new personal data market has emerged creating new actors, such as data brokers, that collect personal information about consumers, and sells that information to other organizations. For that individual who still wonders how online companies should generate revenues the answer is simple: "(...) That of a web where everything is free, but we pay for it through our privacy".[2]

It is not strange, then, to think that given the increasing importance of the monetary value of our private information, there is an increasing demand for privacy. And companies, should start giving guarantees to those consumer concerns. As an example of this, in 2018, Mark Zuckerberg, co-founder and CEO of Facebook, announced: "(...) We will continue to invest heavily in security and privacy because we have a responsibility to keep people safe".[3] This announcement came after the shares of the company lose 20%, glaring 120 billion dollars in market capitalization because of the user disenchantment. The reason for that was the fact of becoming public that Facebook shared data of 50 million users with the consultancy Cambridge Analytica.[4] Therefore, it is necessary to study the economic implications of these privacy concerns as an important variable in decision-making; not only for consumers but also for firms.

The existence of privacy concerns can affect consumer behavior in a digital environment. Although 69% of the Internet users in the European Union shopped online in 2018 according to Eurostat, most of them avoid purchasing online because of security matters.[5] Figure

[2] https://www.forbes.com/sites/kalevleetaru/2018/12/15/what-does-it-mean-for-social-media-platforms-to-sell-our-data/# 3d35db4b2d6c

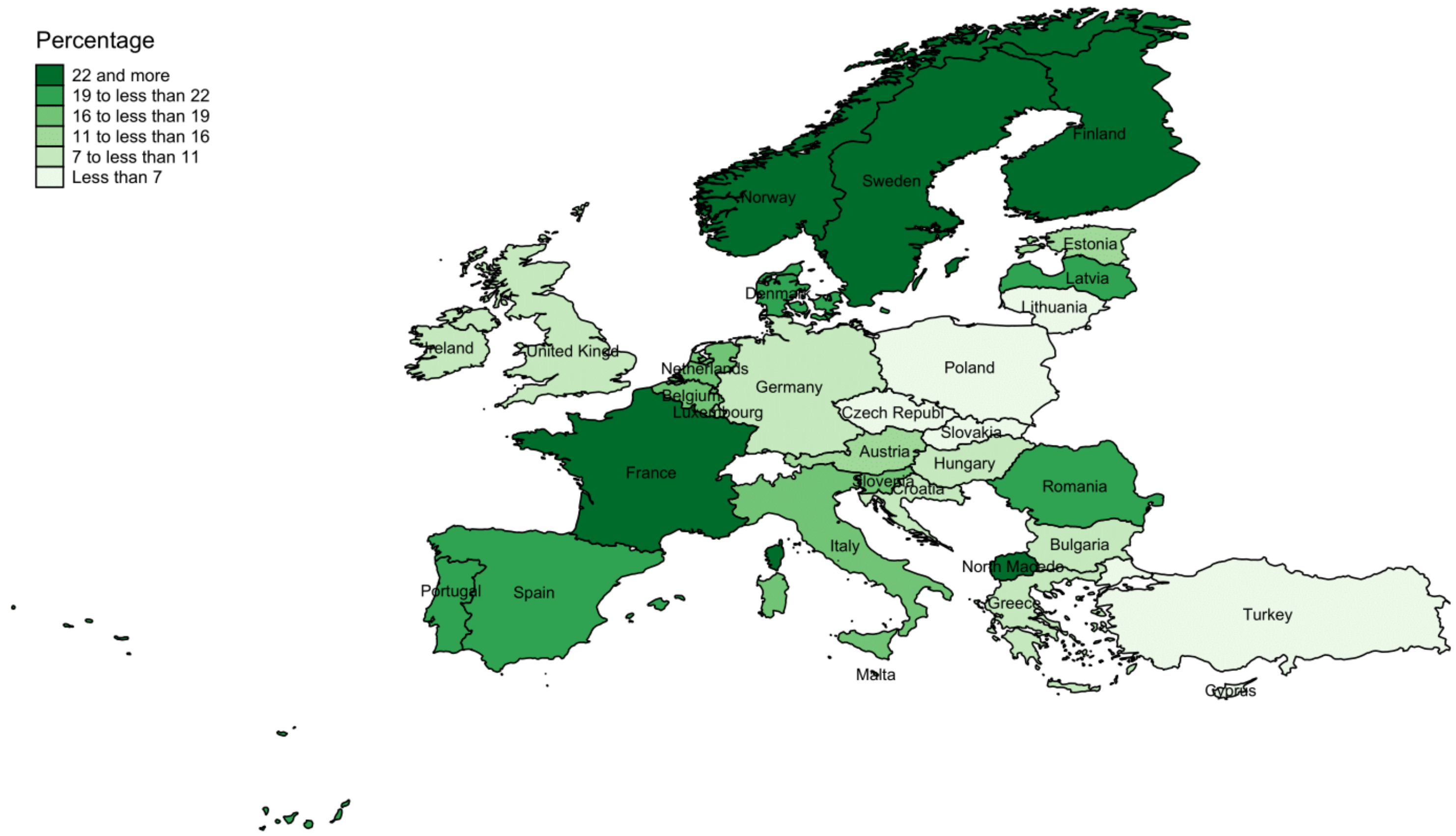
[3] https://www.nytimes.com/2018/07/25/technology/facebook-revenue-scandals.html

[4] https://www.bbc.com/mundo/noticias-43472797

[5] E-commerce statistics for individuals: https://ec.europa.eu/eurostat/statistics-explained/pdfscache/46776.pdf

1 shows the percentage of individuals in the EU where security concerns kept them from ordering or buying goods or services for private use online in 2015.

Fig. 2.1 Percentage of individuals where security concerns kept them from ordering or buying goods for private use online in 2015



Source: Own elaboration and data from EUROSTAT.

France, Norway, Sweden, Finland and North Macedonia present a high percentage of people who avoid purchasing online, more than 22%. They are followed by countries where the percentage presents values between (16%-22%), among them, Portugal, Denmark, Spain and Latvia. The most important fact is that this is not a negligible percentage of individuals, and should be taken into consideration by e-commerce firms when they draw their retail's strategies.

Our goal in this chapter is to study how privacy concerns affect the prices schedule of a monopolist over two purchase channels in two periods of time. We specifically address the following questions:

- How the existence of consumers' privacy concerns affect their willingness to pay in the online channel? Privacy concerns are idiosyncratic to each consumer and evolve over time.

- How the learning process derived from the consumers' online experiences and the signals in the market (prices) affect the privacy concerns of the consumers, whose value is unknown at the beginning of the first period?

- What is the monopolist's optimal pricing strategy, to set uniform pricing or to price discriminate?

- Does it exist price dispersion among different sales channels?

There are three retailing strategies mainly studied in the literature: i) Only bricks, (Brick-and-Mortar channel). Physical or traditional store. ii) Only clicks, (Click-and-Mortar channel). Online sales channel -via the Internet-. And iii) Combination of both, (Bricks-and-Clicks). An example of a recent company, which bets on this strategy is Amazon.[6]

Amazon, the largest e-commerce company in the world, has recently surprised the world with the news of opening physical stores. Everything suggests that the multichannel strategy

[6] https://www.forbes.com/sites/annaschaverien/2018/12/29/amazon-online-offline-store-retail/#5535ef315128

will mark the strategic design of retail companies in the future characterized by different channel types, relationships and structures. There is a complementary effect across the different retailing strategies, therefore companies would increase their profits if they had presence on several channels.

The contribution of this chapter is to analyze these questions. We model a game with a monopolist that faces a decision to operate on two sale channels, dual channel distribution, also known as the brick-and-click strategy but taking into account the presence of heterogeneous consumers in the online channel with respect to privacy. Namely, consumers have a idiosyncratic privacy concerns that evolve over time. There are noisy signals in the market over these privacy concerns, that both the monopolist and consumers do not know at the beginning of the game.

Our work is primarily related to two streams of research. The first examines the decision-making in a context of dual-channel distribution. Although our work is positioned in the literature on dual channels distribution and operations, we do not focus on the aspects commonly taken in this specific field of literature. For many of them, the figure of the manufacturer is not the same as the retailer, and study the strategic relationship between them and their effects on dual channels’ prices, profits, variety of products, etc. Xiao et al. (2014) develop a retailer-Stackelberg pricing model to investigate manufacturers’ product variety and channel structure strategies in a circular spatial market; Chiang et al. (2003) elaborate a consumer choice model and studied a pricing game involving a manufacturer and a retailer in a dual-channel supply chain. Focusing on the study of consumer behavior, we analyze a context similar to that of Fruchter and Tapiero (2005) in the sense that consumers are heterogeneous in their virtual acceptance, and derive utility according to the channel they choose. In the same line, Chiang et al. (2003) assume that consumers have a lower valuation for the product purchased online than for that bought in the physical channel. Li et al. (2015a) also made such an assumption because the consumers have a lower acceptance for the online channel. In a particular way, this idea is also captured in our model, because assuming a willingness to pay known to all participants in the market, the only difference is that consumers derive some uselessness for the purchase in the online channel, and therefore, they will derive in a propensity to pay less, depending on the accuracy in the information and the previous experience.

Consumer shopping experience has also been incorporated as an important part in decision-making. Li et al. (2015b) study the appropriate distribution channel given assortment (breadth, depth, prices of assortment), logistic (inventory cost, delivery cost, delivery time) and consumers characteristics. Ofek et al. (2011) incorporates other variables that can alter the consumer behavior, such as shopping trip cost or the consumer cost of returning a mismatched product.

The second stream of literature that our work is related to is “privacy”. Matters related with privacy and economics is not something new. Recent studies have focused primarily on the protection of information about consumer’s preferences or type, and the relationship between privacy and pricing. For a complete survey and to check out the evolution over decades, see Acquisti et al. (2016). Their work review the theoretical and empirical economic literature investigating individual and societal trade-off with sharing and protecting personal data. They consider that privacy sensitivities “are subjective and idiosyncratic, because what constitutes sensitive information differs across individuals” and that is our focus with this article. Villas-Boas (2014) and Chen and Zhang (2009) study “price for information” strategies in dynamic models, where firms price less aggressively in the first period in order to learn more about their customers and price discriminate in later periods. Acquisti and Varian (2005) and Conitzer et al. (2012) study models in which merchants have access to “tracking” technologies and consumers have access to “anonymizing” (or record-erasing) technologies, and show that welfare can be non-monotonic in the degree of privacy. In Belleflamme and Vergote (2016) a monopolist has also access to “tracking” technologies but with different grades of tracking, and consumers have access to privacy with a cost. They show that the use of a hiding technology harm those consumers that do not hide, because of the increase in the level of prices due to the "hidders". We do not model privacy as a cost to the customer; our approach is that the concern of privacy is something idiosyncratic for the consumer as in the model in Judd and Riordan (1994). Taylor (2004a) and Calzolari and Pavan (2006) examine the exchange of consumer information among companies that are interested in discovering their reservation prices, and Taylor and Wagman (2014) show that even in competitive markets firms may collect excessive amounts of information about individuals.

Our results emphasize the importance of privacy concerns in decision-making in a dual-channel context. This setting aims to give insight on the important role that privacy can have on prices and the monopolist's optimal strategy. In particular, our findings point out that the monopolist gets higher profits if she discriminates over channels, and sets different prices in a market with signals. Furthermore, it exists price dispersion among channels, and online prices can be higher or lower than the offline ones depending on the average privacy concerns in the market. Thus, privacy matters may be a relevant explanation to the existence of price dispersions. On the other hand, we find that non-homogeneity in the set of consumers' information diminishes social welfare in the market: having consumers informed in the market is welfare improving.

The chapter is organized as follows: Section 2.2 and 2.3 explains the general and benchmark model. Section 2.4 and 2.5 analyze the monopolist's two main strategies on prices. Section 2.6 offers some comparative statics and Section 2.7 analyze the scenario of informationally heterogeneous consumers.

2.2 The Model

Our model is a two-period signaling game where a monopolist and consumers learn from market signals the privacy concerns of the latter. We apply the classical signaling games framework to analyze the informational content of prices and the market performance under imperfect information and privacy concerns.

The monopolist has an overall demand composed by consumers purchasing from two channels, the traditional channel (the brick and mortar channel, the brick, in short) and the Internet one (the click channel). All consumers know their willingness to pay -it is a manner to say that the product is not new and they are familiarized with its quality or taste- but they may have an element that diminishes their utility i.e., their privacy concerns.

We assume that if individual i decides to purchase through the brick channel, then there will not be concerns for privacy. That is, we assume that the traditional channel does not represent any threat to consumers about the usage of their personal information. Let q_{it} be consumer i's demand in period t. Then, the demand in the brick channel in period t is,

$$q_{it} = \theta_i - p_t, \tag{2.1}$$

where p_t is the price in period t. As mentioned above, consumers know their willingness to pay for the product represented by θ_i. Therefore, consumer i would be willing to pay $q_{it}\theta_i - \frac{q_{it}^2}{2}$ for q_{it}. However, if individual i decides to purchase through the click channel he does not know their precise privacy concerns, represented by α_{it}, at the time of the purchase. Thus, consumer i's demand in the click channel in period t is

$$E\left\{\theta_i - \alpha_{it} - p_t | \Omega_{it}\right\}, \tag{2.2}$$

where Ω_{it} is consumer i's information at time t. The privacy to an individual i who decides to purchase a product in period $(t = 1,2)$ through the online channel is represented by an index α_{it}, equal to

$$\alpha_{it} = \tilde{x} + \widetilde{\omega_i} + \widetilde{v_{it}} \tag{2.3}$$

Random variable $\tilde{x}$, $\widetilde{\omega_i}$ and $\widetilde{v_{it}}$ represent the population-average privacy in that specific product market, the individual i's persistent deviation from that population average privacy and his specific-time deviation, respectively. The random variables have the following distributions $\widetilde{\omega_i} \sim N\left(0, \sigma_{\tilde{\omega}}^2\right)$, $\widetilde{v_{it}} \sim N\left(0, \sigma_v^2\right)$ and $\tilde{x} \sim N\left(\bar{x}, \sigma_x^2\right)$. Therefore, $E\left\{\tilde{\omega}\right\} = E\left\{\tilde{v_{it}}\right\} = 0$. We also assume that they are all normally and independently distributed. Normality has the unpleasant feature of an unbounded support, allowing the possibilities of negative demand and prices. On the other hand, normality has the highly desirable feature of implying linear updating rules for consumers, which simplifies our analysis considerably.

Variable $\tilde{\omega_i}$ catches up differences between consumers. Of course, some consumers do not care about privacy at all. However, some others consumers may consider privacy policy of vital importance and, in particular, if a consumer detects that some private information is used in a harmful way, it will increment the value of α_{it} and hence will lower the utility of this channel. Variable $\tilde{v_{it}}$ is a external shock. For example, there may be an official announcement about a new privacy policy or a new security system that permit consumers to avoid being followed by cookies.

Moreover, we study a context where consumers' demand of products is positive. Thus, the willingness-to-pay for the product, θ_i, in the brick channel is large enough in order to have a positive demand in period 1 and 2, i.e., $\theta_i > p_t$. Furthermore, in the same way, in the click channel, in period $t = 1,2$ we assume that the willingness to pay is higher than the expected privacy concerns with respect to the set of information in each period t, i.e., $\theta_i > E\left\{\alpha_{i1}|\Omega_{i1}\right\} + p_1$ in period 1, and $\theta_i > E\left\{\alpha_{i2}|\Omega_{i2}\right\} + p_2$ in period 2.

We assume that privacy concerns are something private or individual to each consumer. Furthermore, the fact that the willingness to pay is equal and known between channels allows us to focus on the privacy concerns as distorting element of the market equilibrium analysis.

Namely, we study how privacy concerns can influence the consumer's purchasing behavior, which, in turns, influences the monopolist price setting behavior in both channels.

It is also assumed that the monopolist can get some type of extra mark-up on the price charged in the online market depending on the units sold through this specific channel. For example, she can sell the private information regarding consumers' data using this channel and get some extra profit. This mark-up is denoted by $r \in (0,1)$, with $r = 0$ meaning that she does not sell the information and, therefore, does not get any extra mark-up. Thus, $r = 1$ represents the case when the monopolist sells information and the mark up is a total percentage over the price.

The firm receives a private signal about consumers' privacy concerns after period 1. In addition, if consumers buy on the Internet, the monopolist will have another signal about the average privacy operating on this channel. The signal received by the monopolist is

$$z = \tilde{x} + \tilde{\varphi}, \tag{2.4}$$

where $\tilde{x}$ represents the same random variable showing, as before, the average privacy in the market, and $\tilde{\varphi}$ is an external shock which is distributed normally $\tilde{\varphi} \sim N\left(0, \sigma_{\varphi}^{2}\right)$. Information about privacy concerns is important to the monopolist since she will be able to storage consumers' personal data, selling them to a third party or use this information in her interest to price discriminate. Therefore, signal z represents an important information to the monopolist's second period action and it will be observed after first-period sales. With this particular definition of z we can now give a more complete interpretation of $\tilde{x}$ and the random variable $\tilde{\varphi}$. Thus, $\tilde{x}$ is the portion of the mean effect on the population which is detectable through z. Therefore, if $\tilde{x}$ is independent and not correlated with $\tilde{\varphi}$, then the monopolit's private signal, z, will signal exactly the actual average population privacy concerns of consumers purchasing in the online channel. If $\tilde{\varphi}$ were correlated, then $\tilde{x}$ would not be the average privacy concerns about using this specific channel, but its ex-ante expectation.

The overall sales of the monopolist come from the two channels. Let the parameter λ represent the sales coming from the brick channel and $(1-\lambda)$ the proportion of sales from the online channel. We assume that λ is exogenous and the total mass of consumers is normalized to 1.[7] Therefore $\lambda \in (0,1)$.

We also assume that the unit production cost in each period is common knowledge and normalized to zero. The timing of the game is as follows:

In period 1, the market for the product opens. The monopolist has to decide her price strategy -whether to practice price discrimination or not- for both channels and announce the first-period price(s). In this first period, there is no information generated by any player i.e., there is nor private information for the monopolist neither learning for the customers. Therefore, information set Ω_1 consists of simple expectations: the monopolist has an expected demand from the online channel, Ω_{m1}, where m indicates the set of information for the monopolist. Representative consumer $i's$ who purchases in the click channel, has an expected privacy concern and his set of information is given by Ω_{i1}. These consumers observe the market price and decide how much to purchase of the product given his expectations on privacy concern. The remaining consumers observe the market price and buy in the traditional -brick- channel.

Note that at the beginning of the first period, consumers of the click channel are uncertain about their concerns on privacy and need some experience to update their information. Since it is common knowledge that the monopolist will receive a private signal about the privacy mean at the end of period 1, then at the beginning of period 2, both consumers and the firm will have some new information.

In period 2, the set of information is Ω_2. First, the firm observes the private signal about the average privacy concern from the online channel, $z = \tilde{x} + \tilde{\varphi}$, and first period purchases. Both elements constitute the set of information for the firm in $t = 2$, Ω_{m2}, and then, the firm

[7] We assume λ fixed in order to obtain close form solutions. If λ were not fixed, we should specify it as a function depending on prices.

announces her period 2 price schedule. Second, consumers learn about their real concerns for privacy from their purchases in the first period and from the second period price -they are able to make an inference of z through the price(s)- and finally, they make a decision. Therefore, the consumers' information set, Ω_{i2}, consists of their previous purchase experience, α_{i1} and the inference made over z from the second period price(s), once this price is announced.

The above two-period game with imperfect information is a dynamic Bayesian game. In addition, given that consumers signal their (probabilistic) knowledge about their privacy concerns through their demands, and the monopolist signals her information on consumers' privacy concerns through the second period price, the imperfect information dynamic game is a noisy signaling game. Therefore, the corresponding equilibrium concept, Perfect Bayesian Equilibrium, specifies to that of a Noisy Signaling Equilibrium (NSE). The Noisy Signaling Equilibrium prescribes equilibrium strategies for the firm and consumers which are sequentially rational to the other players' equilibrium strategies at each of their information sets (their beliefs about the consumers' privacy concerns), and beliefs which are consistent with the equilibrium strategies, that is, they come from Bayesian updating.

The next section offers the Bayesian updating of beliefs.

2.3 Updating of beliefs

Given our equilibrium concept, consistent beliefs are obtained by certain Bayesian updates. Since all random variables are normally distributed, the Bayesian updates are just regression equations. First, we have the Bayesian updating of the random variable α_{i1} once the private signal, z, has been observed. To start with, we have to compute the expected value, the variance and the correlation of α_{i1} and z taking into consideration that these random variables are specified in (2.3) and (2.4):

1. The expected values of α_{i1} and z are $E\{\alpha_{i1}\} = E\{z\} = \bar{x}$.

2. The variance of α_{i1} and z are $Var(\alpha_{i1}) = \sigma_x^2 + \sigma_\omega^2 + \sigma_\upsilon^2$ and $Var(z) = \sigma_x^2 + \sigma_\varphi^2$. In order to simplify, we just call $Var(\alpha_{i1}) = \sigma_\alpha^2$ and $Var(z) = \sigma_z^2$

3. The correlation between the two variables is specified by the index ρ. Calculations gives that $\rho = \frac{\sigma_x^2}{\sigma_\alpha \sigma_z}$.

   Now, note that, following DeGroot (2005), the Bayesian updating of the mean with normal random variables when the variance is known, is

$$\mu' = \frac{\tau\mu + ns\bar{x}}{s + ns}, \tag{2.5}$$

   where μ and τ are the prior mean and precision, respectively, and s is the poterior precision given n observations of a random sample. In our scenario with correlated variables, the Bayesian updating translates to:

$$E\{\alpha_{i1}|z\} = E\{\alpha_{i1}\} + \rho\frac{\sigma_\alpha}{\sigma_z}(z - E\{z\}), \tag{2.6}$$

   with $\rho(\alpha_{it}, z) = \frac{Cov(\alpha_{it}, z)}{\sqrt{Var(\alpha_{i1})Var(z)}}$.

   Substituting in (2.6) the corresponding terms, we get the following expression:

$$E\{\alpha_{i1}|z\} = \bar{x}\left(1 - \frac{\sigma_x^2}{\sigma_z^2}\right) + z\left(\frac{\sigma_x^2}{\sigma_z^2}\right).$$

Letting γ_z be the relative precision of signal z, i.e., $\gamma_z = \frac{\sigma_x^2}{\sigma_z^2}$, and γ_x the relative precision of the prior distribution of α_{i1}, i.e, $\gamma_x = 1 - \gamma_z = \left(1 - \frac{\sigma_x^2}{\sigma_z^2}\right)$

$$E\{\alpha_{i1}|z\} = \gamma_z z + \gamma_x \bar{x}. \tag{2.7}$$

Clearly, the Bayesian updates of α_{i1} conditional to z is a linear combination of z and $\bar{x}$, weighted by their respective relative precisions (γ_x and γ_z).

Second, at the beginning of period 2, new information comes into the market. This fact means that the updating of α_{i2} by the firm will come after the observation of z and q_1. On the other hand, consumers' update of beliefs comes after the observation of p_2 from an inference of z, and their previous experience α_{i1}.

The Bayesian updating in period 2 is,

$$E\left\{\alpha_{i2}|\alpha_{i1},z\right\} =$$

$$E\left\{\alpha_{i2}\right\}+\begin{pmatrix} Cov\left(\alpha_{i2},\alpha_{i1}\right) & Cov\left(\alpha_{i2},z\right)\end{pmatrix}\begin{pmatrix} Var\left(\alpha_{i1}\right) & Cov\left(\alpha_{i2},\alpha_{i1}\right) \\ Cov\left(\alpha_{i2},\alpha_{i1}\right) & Var\left(z\right)\end{pmatrix}^{-1}\begin{pmatrix}\alpha_{i1}-E\left\{\alpha 1\right\} \\ z-E\left\{z\right\}\end{pmatrix}. \tag{2.8}$$

Let us calculate the expected values, variances and the variance-covariance matrix:

1. Recall that expected values are $E\left\{\alpha_{i2}\right\}=E\left\{\alpha_{i1}\right\}=E\left\{z\right\}=\bar{x}$.

2. Variances are $Var\left(\alpha_{i1}\right)=\sigma_x^2+\sigma_\omega^2+\sigma_\upsilon^2$, $Var\left(\alpha_{i2}\right)=\sigma_x^2+\sigma_\omega^2$ and $Var\left(z\right)=\sigma_z^2$.

3. It is important to note that the updating of α_{i2} is conditional to α_{i1} and z i.e., we have three random variables distributed normally and correlated, where the variance-covariance matrix is as follows:

$$\begin{pmatrix}\alpha_{i1} \\ \alpha_{i2} \\ z\end{pmatrix}\sim N\left(\begin{pmatrix}\bar{x} \\ \bar{x} \\ \bar{x}\end{pmatrix},\begin{pmatrix}\sigma_\alpha^2 & \sigma_x^2+\sigma_\omega^2 & \sigma_x^2 \\ \sigma_x^2+\sigma_\omega^2 & \sigma_\alpha^2 & \sigma_x^2 \\ \sigma_x^2 & \sigma_x^2 & \sigma_z^2\end{pmatrix}\right). \tag{2.9}$$

4. Substituting in (2.8) all the terms above, we get the following expression:

$$E\left\{\alpha_{i2}|\alpha_{i1},z\right\}=\bar{x}\left(1-\frac{\sigma_x^2\sigma_\varphi^2+\sigma_\omega^2\sigma_z^2}{|\Sigma|}-\frac{\sigma_x^2\sigma_\upsilon^2}{|\Sigma|}\right)+\alpha_{i1}\left(\frac{\sigma_x^2\sigma_\varphi^2+\sigma_\omega^2\sigma_z^2}{|\Sigma|}\right)+z\left(\frac{\sigma_x^2\sigma_\upsilon^2}{|\Sigma|}\right),$$

where $|\Sigma| = \sigma_\alpha^2\sigma_z^2 - \sigma_x^4$ is the determinant of the variance-covariance matrix specified in (2.9). Let

$$\delta_\alpha = \frac{\sigma_x^2\sigma_\varphi^2 + \sigma_\omega^2\sigma_z^2}{\sigma_\alpha^2\sigma_z^2 - \sigma_x^4},$$

$$\delta_z = \frac{\sigma_x^2\sigma_v^2}{\sigma_\alpha^2\sigma_z^2 - \sigma_x^4},$$

and

$$\delta_x = 1 - \delta_\alpha - \delta_z,$$

and substituting above, we get the Bayesian updating of privacy concerns in period 2, conditional on z and α_{i1} .

$$E\{\alpha_{i2}|\alpha_{i1}, z\} = \bar{x}\delta_x + \alpha_{i1}\delta_\alpha + z\delta_z. \tag{2.10}$$

In these equations $\sigma_\alpha^2 = \sigma_x^2 + \sigma_\omega^2 + \sigma_\vartheta^2$ and $\sigma_z^2 = \sigma_x^2 + \sigma_\varphi^2$. Therefore, we can rewrite as

$$\delta_z = \gamma_z(1 - \delta_\alpha). \tag{2.11}$$

$$\delta_x = (1 - \gamma_z)(1 - \delta_\alpha). \tag{2.12}$$

In period 2, the consumers' posterior distribution of their privacy concerns comes from the information obtained through their purchases in period 1 and their updating of privacy concerns in period 1, α_{i1}. In other words, from their previous experience in period 1 and their inference made on z from the monopolist's second period price. Thus, it is a linear combination of three relevant variables: the private's signal of the monopolist, z, the previous experience in period 1 on privacy issues of the consumers, α_{i1}, and the average mean privacy in the population, $\bar{x}$, weighted by their relative precision, δ_z, δ_α and δ_x, respectively. Particularly, δ_α is the relative precision of the previous experience in period 1, γ_z is the relative precision of the signal in period 2 and γ_x is the relative precision of the prior distribution of α_{i2}.

Intuitively, equations (2.11) and (2.12) show that updated beliefs depend on two key parameters which are δ_α and γ_z. Parameter δ_α is how much weight consumers put in their experience on privacy concerns from the online channel. Parameter γ_z is the precision of the monopolist's private information i.e., the signal's precision of z. Note that an improvement in the precision of γ_z, means a decrease in the precision of γ_x, i.e., the precision of the true average privacy concern.

Before proceeding with the analysis under the different scenarios and equilibrium prices, it is interesting to think about the nature of equilibrium prices in period 2.

At the beginning of period 2, both consumers and the firm have information. Each consumer i remembers his first period experience, which yielded an observation of α_{it}, and the firm has observed z. A high z indicates a high x, which in turn indicates that the observation of α_{it}, is likely to be high. Thus, the firm concludes from a high z that second period demand is likely to be low (the difference between the willingness-to-pay for the product and privacy concerns), which supports a low expected profit maximizing price. Hence, the firm has an incentive to know the average privacy concerns in the market given that the expected price in period 2 and his expected benefits depend on it. Consumers understand these incentives of the firm, and therefore, naturally infer something about the firm's observation of z from the price. Information about z is useful to the consumers since it provides an independent signal of the true value of x, a component of their utility.

However, since each consumer's utility experience with the good is idiosyncratic, he will continue to use his personal information α_{it}, in making privacy concerns inferences. We conclude below that equilibrium does in fact posses these features; however, the presence of idiosyncratic signals to the consumers is crucial.

Next, two main scenarios or strategies are analyzed, where the monopolist can choose in this setting either to practice price discrimination between the brick and the click channel, or to set up a uniform price in both channels. First, we analyze the uniform price strategy and then the price discrimination strategy between channels, taking into account that the proportion of channels, λ, is exogenous. Note that the firm's second-period price will be a linear function of its private information. At equilibrium, linear inference rules by the consumer make linear decision rules optimal.

2.4 Uniform pricing

In this section, we analyze how the monopolist sets up a uniform price in period $t = 1,2$ given the set of information available for both the monopolist and consumers.

In period 1, consumers have expected demand given their set of information in $t = 1$. As above specified, no additional information for both the monopolist and consumers has been yet generated, and consumers' expected demand and firm's expected profits consists of simple expectations. Let p_1^u be the uniform price expected by consumers in period 1, and q_{iB1} and q_{iC1} the demands in period 1 of the brick and the on-line channels, respectively. Then,

1. Demand in the brick channel,
$$q_{iB1}^u = \theta_i - p_1^u.$$

2. Expected demand of consumer i in the online channel, conditional to her information set is,
$$E\left[q_{iC1}^u | \Omega_{i1}(\alpha_{i1})\right] = \theta_i - \bar{x} - p_1^u.$$

The monopolist does not have any additional information neither, therefore, letting Π_1^u be the two-channels profits in period 1, then her expected profits, conditional to her information set are,

$$E\left[\Pi_1^u|\Omega_{m1}\left(\alpha_1\right)\right]=\lambda\left(\theta_i-p_1^u\right)p_1^u+\left(1-\lambda\right)\left(\theta_i-\bar{x}-p_1^u\right)p_1^u\left(1+r\right). \qquad (2.13)$$

Similarly, let q_{iB2}^u and q_{iC2}^u be the demands in period 2 of the brick and the on-line channels respectively, and p_2^u is the uniform price expected by consumers in period 2. Then,

1. Demand for the brick channel in period 2,

$$q_{iB2}^u=\theta_i-p_2^u.$$

2. Expected demand by consumer i in the online channel conditional on his information set at the beginning of period 2 is,

$$E\left[q_{iC2}^u|\Omega_{i2}\left(\alpha_{i1},p_2^u\right)\right]=\theta_i-E\left\{E\left\{\alpha_{i2}|\alpha_{i1},z\right\}|\alpha_{i1},p_2^u\right\}-p_2^u,$$

which, given the updated beliefs of $E\left\{\alpha_{i2}|\alpha_{i1},z\right\}$ (see equation 2.10 above) specifies to,

$$E\left[q_{iC2}^u|\Omega_{i2}\left(\alpha_{i1},p_2^u\right)\right]=\theta_i-E\left\{\bar{x}\delta_x+\alpha_{i1}\delta_\alpha+z\delta_z|\alpha_{i1},p_2^u\right\}-p_2^u.$$

Again, the expected demand curve of the monopolist in period 2 is the sum of the two channels expected demands. After period 1, she gets some new information about the consumers' average privacy and uses this information to set the second period's price. As it is explained before, in period 2, λ is again the proportion of consumers buying in the brick channel and, r represents the extra benefits of sales of data. Letting Π_2^u be the two-channels profits in period 2 and, q_2^u period 2 demand, then, the expected demand faced by the firm and the monopolist's second-period expected profits are, respectively,

$$E\left[q_2^u|\Omega_{m2}\left(z,p_2\left(z\right)\right)\right]=\lambda\left(\theta_i-p_2^u\right)+\left(1-\lambda\right)\left(\theta_i-E\left\{\bar{x}\delta_x+\alpha_{i1}\delta_\alpha+z\delta_z|z\right\}-p_2^u\right), \qquad (2.14)$$

and,

$$E\left[\Pi_2^u|\Omega_{m2}\left(z,p_2\left(z\right)\right)\right] = \lambda\left(\theta_i - p_2^u\right)p_2^u + \left(1-\lambda\right)\left(\theta_i - E\left\{\bar{x}\delta_x + \alpha_{i1}\delta_\alpha + z\delta_z|z\right\} - p_2^u\right)p_2^u(1+r). \tag{2.15}$$

2.4.1 Equilibrium

Once specified the consumers' expected demands and the monopolist's expected profits in $t = 1,2$ under the uniform pricing strategy, we look for the market equilibrium of our noisy signaling game. As already said, the equilibrium concept is that of Noisy Signaling Equilibrium (NSE) and consists of: the monopolist's pricing strategy at each period, given her set of information Ω_{mt} in $t = 1,2$, the consumers' expected demands coming from their utility maximization, given their set of information Ω_{it} in $t = 1,2$, and beliefs of both consumers and the monopolist, consistent with the equilibrium strategies. In equilibrium, posterior beliefs are consistent with Bayes' rule and the firm and the consumers' strategies.

The first step to compute the NSE consists of exactly specify what consumer i believes when he decides to purchase the product on the on-line channel at any possible information set, Ω_{i2}. A consumer that purchases the product on the brick channel knows exactly his utility, and thus he has no privacy concerns. However, a consumers information set at the beginning of period 2, of those buying on the online channel, consist of their own experience over α_{it} plus the commonly observed p_2^u which possibly indicates the firm's observation of the monopolist's private signal, z. Furthermore, note that signal z provides an independent "signal" of the true value of x, component of their utility function. Thus, they understand that a high z, indicates a high value of x, which in turn indicates that each consumer's observation of privacy, α_{i1} is likely to be high.

Suppose that consumers make inferences on z from p_2^u following Bayes rule and according to the linear rule $z = a + bp_2^u$. Then, the online channel second period expected demand is,

$$E\left[q_{iC2}^u|\Omega_{i2}\left(\alpha_{i1}, p_2^u\right)\right] = \theta_i - \left\{\bar{x}\delta_x + \alpha_{i1}\delta_\alpha + \left(a + bp_2^u\right)\delta_z\right\} - p_2^u \tag{2.16}$$

and thus, the overall expected demand in period 2 perceived by the monopolist is given by

$$E\left[q_2^u|\Omega_{m2}\left(z, p_2\left(z\right)\right)\right] = \lambda\left(\theta_i - p_2^u\right) + \left(1 - \lambda\right)\left(\theta_i - \left(\bar{x}\gamma_x + \delta_z\left(a + bp_2^u\right) + z\delta_\alpha\gamma_z\right) - p_2^u\right). \tag{2.17}$$

Finally, the monopolist's second-period expected profits, taking into account the extra profits form data sales are,

$$\begin{aligned} E\left[\Pi_2^u|\Omega_{m2}\left(z, p_2\left(z\right)\right)\right] &= \lambda\left(\theta_i - p_2^u\right)p_2^u \\ &\quad + \left(\left(1 - \lambda\right)\left(\theta_i - \left(\bar{x}\gamma_x + \delta_z\left(a + bp_2^u\right) + z\delta_\alpha\gamma_z\right) - p_2^u\right)\right)p_2^u(1 + r). \end{aligned} \tag{2.18}$$

As can be seen from (2.17), the expected demand in period 2 under uniform price setting shows that an increase in price has two distinct effects on demand. Reordering terms, we get that

$$E\left[q_2^u|\Omega_{m2}\left(z, p_2\left(z\right)\right)\right] = \theta_i - \left(1 - \lambda\right)\left(\bar{x}\gamma_x + \delta_z a + z\delta_\alpha\gamma_z\right) + p_2^u\left(-1 - b(1 - \lambda)\delta_z\right).$$

In the above expression, the term (-1) represents the direct effect that the price has on the expected demand in period 2. The indirect effect on the second period price, which is the term $(-b(1 - \lambda)\delta_z)$, will depend on its sign.[8] Plugging "b" in (2.23) and δ_z from (2.11), highlight that this term is positive. That means that an increase in prices translates to higher inference made by consumers about the expected level of α_{i2}, leading to a decrease in demand. If the

[8] It is required that $\delta_z b(1 - \lambda) < 1$, thus the monopoly price always exists and the second-period pricing problem is always well defined.

value of $(-b(1-\lambda)\delta_z)$ is very high, i.e., if consumers put a lot of weight on p_2^u in drawing inferences about z, then, the demand curve will become steeply sloped and the monopoly price will be high.

The important point to keep in mind is that when there is an increase in prices, it will not reduce demand by as much as it would be in the absence of signaling. In other words, the fact than consumers draw inferences about privacy concerns from the price makes demand less elastic at any particular quantity. It is important to point out that our model imposes uncertainty in the intercept of the demand and not in its slope. Notice that some uncertainty in the slope would give consumers incentives to increase their purchases in order to increase their information (learning by experimentation). We leave experimentation issues in this chapter. aside. For a complete review on this field, see Urbano (2018) The existence of signaling in this market makes the expected demand more inelastic.

Definition 1 *The tuple $(p_1^{u*}, q_1^{u*}, p_2^{u*}, q_2^{u*})$ and beliefs $(\alpha_{1t}, \alpha_{2t})$ is a Noisy Signaling Equilibrium with uniform pricing strategy if*

1. *Given $E\left[\Pi_1^u|\Omega_{m1}(\alpha_1)\right]$ in $t=1$ and $E\left[\Pi_2^u|\Omega_{m2}(z, p_2(z))\right]$ in t=2, the firm 's price strategies are for the first period*

$$p_1^{u*} = \quad arg \quad \max_{p_1^u} \quad \{\lambda\,(\theta_i - p_1^u)\,p_1^u + (1-\lambda)\,(\theta_i - \bar{x} - p_1^u)\,p_1^u\,(1+r)\} \tag{2.19}$$

and the firm's price strategy for the second period is

$$\begin{aligned} p_2^{u*} = \quad arg \quad \max_{p_2^u} \quad & \{\lambda\,(\theta_i - p_2^u)\,p_2^u \\ & + ((1-\lambda)\,(\theta_i - (\bar{x}\gamma_x + \delta_z\,(a + bp_2^u) + z\delta_\alpha\gamma_z) - p_2^u))\,p_2^u(1+r)\}\,. \end{aligned} \tag{2.20}$$

2. *Given prior beliefs of α_{it}, and information sets Ω_{it} in each period $t = 1,2$, consumers maximize their utility and decide how much to purchase once the monopolist's price(s) have been announced in each channel.*

3. *Both the monopolist and the consumers use Bayesian updates to compute the posterior beliefs given their set of information in each period and their beliefs are consistent with the equilibrium strategies.*

Given (2.7) and (2.10), and expected demands in $t = 1,2$, the monopolist maximizes her expected benefits in each period. Namely, given the expected demand perceived by the monopolist in (2.17), its optimal price in period 2 is

$$p_2^{u*} = \frac{\theta_i(1+(1-\lambda)r)-(1-\lambda)(r+1)\bar{x}\gamma_x-(1-\lambda)(r+1)z\delta_\alpha\gamma_z-a(1-\lambda)(r+1)\delta_z}{2\,(1+b(1-\lambda)(r+1)\delta_z+(1-\lambda)r)}. \tag{2.21}$$

We are searching for an equilibrium in which the representative consumer's inference rule is correct. Consumers are correct believing that z observed by the firm equals $z = a + bp_2^u$; then p_2^u must also satisfy $p_2^u = (z-a)/b$. Hence, in a linear equilibrium:

$$a = \frac{\theta_i(1+r(1-\lambda))-\bar{x}\gamma_x(1-\lambda)(r+1)}{(1-\lambda)(r+1)\gamma_z}, \tag{2.22}$$

and

$$b = -\frac{2+2r(1-\lambda)}{(1-\lambda)(r+1)\,(2-\delta_\alpha)\,\gamma_z}. \tag{2.23}$$

Subsituting a and b in (2.21), we get the expected price, and therefore, expected demand and profits in period 2.

Proposition 1 characterizes the noisy signaling equilibrium.

Proposition 1 *Suppose that the consumer proportion between channels is given by $\lambda \in (0,1)$, the firm's mark-up is $r \in (0,1)$ and linear inference rules, then there exists a noisy signaling equilibrium with uniform pricing strategy. In equilibrium,*

1. *The firm sets the price in $t=1$,*

$$p_1^{u*} = \frac{\theta_i + (1-\lambda)\,(r\theta_i - \bar{x}(r+1))}{2+2r(1-\lambda)}$$

and the expected demand in equilibrium is

$$q_1^{u*} = \frac{\theta_i + (1-\lambda)(\theta_i r - \bar{x}(1+r(1-2\lambda)))}{2+2r(1-\lambda)}.$$

2. *In period 2, the second period price is*

$$p_2^{u*} = \frac{(2-\delta_\alpha)\,(\theta_i(1+(1-\lambda)r) - (1-\lambda)(r+1)\,(\bar{x}\gamma_x + z\gamma_z))}{2(1+(1-\lambda)r)}, \tag{2.24}$$

and the expected demand in period 2 is

$$q_2^{u*} = \frac{\delta_\alpha\theta_i + (1-\lambda)\,(\delta_\alpha\,(r\theta_i - (r+1)\,(\bar{x}\gamma_x + z\gamma_z)) + 2\lambda r\,(\bar{x}\gamma_x + z\gamma_z))}{2(1+(1-\lambda)r)}. \tag{2.25}$$

Proof. See the Appendix. ■

Expected second-period profits are therefore

$$\Pi_2^{u*} = \frac{(2-\delta_\alpha)\,\delta_\alpha\,(\theta_i(1+(1-\lambda)r) - (1-\lambda)(1+r)\,(\bar{x}\gamma_x + z\gamma_z))^2}{4\,(1+r\,(1-\lambda))}. \tag{2.26}$$

The second order conditions holds in each period. In period 1, the second order condition is $-2\lambda - 2(1-\lambda)(r+1) < 0$. Furthermore, in period 2, the second order condition equals $2(1-\lambda)(r+1)\,(-b\delta_z - 1)$, and plugging "b" specified in (2.23) in the second order contidion we get $-\frac{2\delta_\alpha(1+r(1-\lambda))}{2-\delta_\alpha} < 0$.

Proposition 2 *If γ_z is fixed and common knowledge, then equilibirum prices will be given by p_1^{u*} and p_2^{u*} as above specified. Furthermore,this is the unique equilibrium where consumers' inferences about z are a differentiable and an invertible function of p_2^{u*}.*

Proof. See the Appendix. ■

The second period price is indeed a linear function of the signal z. Furthermore, signaling might distorts prices upward in comparison to the complete information scenario and, the scenario in which z is common knowledge to both consumers and the monopolist. to study this distortion, let p_2^z be the price in equilibrium in period 2 in which z is common knowledge i.e., both consumers and the monopolist can receive information from the signal z. Therefore, consumers will not infer the value of z from the second period price, and z will not equal $a + bp_2$. In this maximization problem, p_2^z equals,

$$p_2^z = \frac{\theta_i(1+r(1-\lambda)) - (1-\lambda)(r+1)(\bar{x}\gamma_x + z\gamma_z)}{2+2r(1-\lambda)}.$$

Secondly, let p_2^F be the price under complete information scenario. In other words, the case in which the observation of the signal reveals the true population average privacy concerns in absence of any noise and, therefore, the precision of the average privacy concerns is perfect, $\gamma_x = 1$. No observation of z exists. Thus, in the maximization problem,

$$p_2^F = \frac{\theta_i(1+r(1-\lambda)) - \bar{x}(1-\lambda)(r+1)}{2+2r(1-\lambda)}.$$

Simple calculations show that the difference $p_2^u - p_2^F$ is positive, as long as $\bar{x} \geq z$. However, for those values of z higher enough than $\bar{x}$, the case is reverse. Let z' be the observed value of z that equals p_2^u and p_2^F. In particular,

$$z' = \frac{(1-\delta_\alpha)\theta_i(1+r(1-\lambda)) + (1-\lambda)(r+1)\bar{x}(\gamma_z(2-\delta_\alpha)+\delta_\alpha+1)}{\gamma_z(2-\delta_\alpha)(1-\lambda)(r+1)}.$$

We find that for some values of z higher than z', but lower than the willingness to pay, θ_i, i.e., $\theta_i > z > z' > \bar{x}$, signaling does distort prices downward with respect the complete information monopoly prices in period 2, $p_2^u < p_2^F$.

On the other hand, signaling always distorts prices upward comparing to the scenario when z is common knowledge for both consumers and the monopolist. In other words,

$$p_2^u - p_2^z = \frac{(1-\delta_\alpha)(\theta_i - (\lambda-1)(\theta_i r + (r+1)(\bar{x}\gamma_x - \gamma_z z)))}{2+2r(1-\lambda)} > 0.$$

To sum up, the existence of noisy signals and the uncertainty over consumers' privacy, led to a distortion on prices in the market. We find that signaling does distort prices upward with respect to the full information scenario as long as the observed value of z is under the true $\bar{x}$. The monopolist believes that the average privacy concerns is lower than it really is, and this makes her to increase the price in period 2. On the contrary, for these observed values of the signal z higher than z', signaling it does distort prices downward with respect to the full informative setting, and therefore, consumers are better off because of lower prices. In addition, signaling always distorts prices upward with respect to the case of z common knowledge for all players in the market.

2.4.2 Comparative statics

The expected equilibrium price in period 2 depends on two key parameters, δ_α and γ_z. We turn now to analyze these relationships.

Firstly, we analyze the variation of period 2's expected price as the precision γ_z of the signal, z, changes. Taking into account that $\gamma_x = 1-\gamma_z$, the partial derivative has the following form,

$$\frac{\partial p_2^u}{\partial \gamma_z} = \frac{(\bar{x}-z)(1-\lambda)(r+1)(2-\delta_\alpha)}{2(1+(1-\lambda)r)} = (+/-)$$

The terms $(1-\lambda)(r+1)(2-\delta_\alpha)$ and $2(1+(1-\lambda)r)$ are positive. Then, the sign of the partial derivative depends on the relation between the observed z, and the $\bar{x}$, the true value of the average privacy concerns in the market. It turns out that when the true average privacy in the market is higher than the monopolist's private obsertation, i.e., $\bar{x} > z$, an increase of the precision in the private information increases the level of the expected price in period 2 under uniform pricing strategy. However, if $z > \bar{x}$, any effort to improve the precision of the signal means a lower level of expected prices in period 2. Notice that γ_z enters in p_2^u as $\bar{x}\gamma_x + z\gamma_z = \bar{x}(1-\gamma_z) + z\gamma_z$, so that as γ_z increases, the change on p_2^u depends on the variation of the term $\bar{x}$ and that on z.

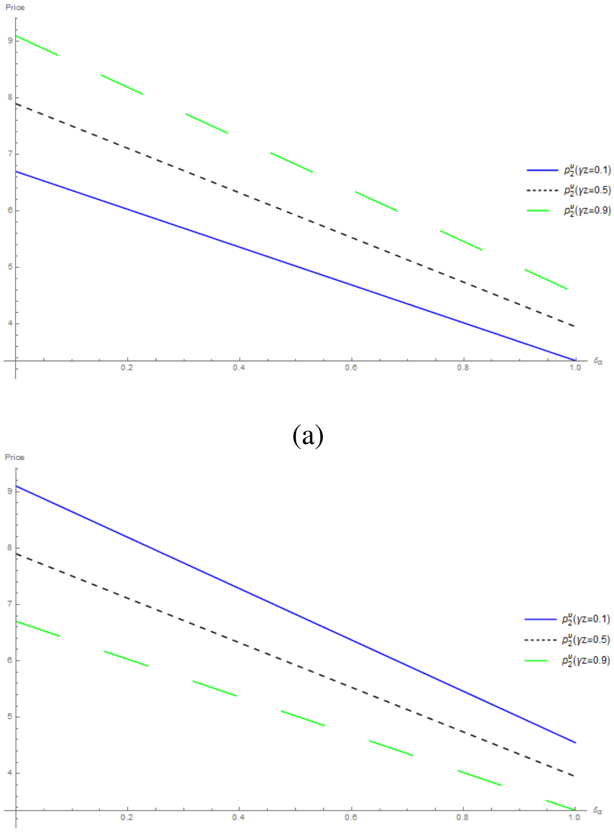
Secondly, we analyze the variations in period 2's expected prices when the importance that consumers give to their previous experiences, δ_α, changes.

The partial derivative of the expected price in period 2 is

$$\frac{\partial p_2^u}{\partial \delta_\alpha} = -\frac{\theta_i(1+r(1-\lambda)) - (1-\lambda)(r+1)\bar{x}\gamma_x - (1-\lambda)(r+1)z\gamma_z}{2-2(\lambda-1)r} < 0,$$

which is negative. The term $2-2(\lambda-1)r$ is positive, and we assumed above that $\theta_i > \bar{x}\gamma_x + z\gamma_z$. Thus, $\theta_i(1+r(1-\lambda)) - (1-\lambda)(r+1)\bar{x}\gamma_x - (1-\lambda)(r+1)z\gamma_z$ is positive, therefore the sign of this partial derivative is negative. That is, as consumers are giving more importance to their experience in the first period, the lower is the period 2's expected price.

In Figure 2.2, we plot different price levels with specific values for the precision of the signal z: $\gamma_z = 0.9$, $\gamma_z = 0.5$ and $\gamma_z = 0.1$. Then, we let free the weight that consumers give to their previous experience, $\delta_\alpha \in (0,1)$. In Figure 2.2(a), the case when $\bar{x} > z$ is plotted and it can be seen that the prices levels are higher when $\gamma_z = 0.9$. Figure 2.2(b) shows the case when $\bar{x} < z$ and it can be also seen that lower levels of prices are achieved when the value of the precision of the information is close to 1. Finally, the higher the importance that consumers give to their previous experience from period 1, the lower the level of the expected price in period 2.



(a)

(b)

Fig. 2.2 Second period price depending on γ_z and δ_α.

2.5 Price discrimination strategy

Our benchmark studies the simplest strategy that the monopolist can decide about her second-period price. However, the firm may choose to practice price discrimination among the two channels in order to extract the maximum willingness to pay.

We assume that a proportion λ of consumers decide to purchase from the traditional shop, meaning that they purchase from this channel in period 1 and 2. Therefore, a proportion $1-\lambda$ purchases from the online channel in period 1 and 2. We do not study the case in which consumers change their channel of purchase at the end of period 1. Although this case is interesting, it needs that λ depends on prices, and this highly complicates the analysis. The analysis that we present focuses on the learning process and the study of price dispersion among channels, highlighting that in the online channel the information sets play a crucial role.

Let the superscript "d" be the actual scenario under price discrimination among channels. Therefore, let p_{1B}^{d} and p_{2B}^{d} be the prices for the brick channel in period 1 and 2, respectively. Furthermore, let p_{1C}^{d} and p_{2C}^{d} be the prices for the online channel in period 1 and 2, respectively. In period 1, like in the uniform pricing strategies, consumers have expected demand given the set of information Ω_1 and the channel chosen for purchasing:

1. Demand through the brick channel: $q_{iB1} = \theta_i - p_{1B}^{d}$.

2. Expected demand through the online channel: $E\left[q_{iC1}|\Omega_{i1}\left(\alpha_{i1}\right)\right] = \theta_i - \bar{x} - p_{1C}^{d}$.

Then, as above, the monopolist expected profits in period 1 are,

$$E\left[\Pi_1^d|\Omega_{m1}\left(\alpha_1\right)\right] = \lambda\left(\theta_i - p_{1B}^{d}\right)p_{1B}^{d} + \left(1-\lambda\right)\left(\theta_i - \bar{x} - p_{1C}^{d}\right)p_{1C}^{d}\left(1+r\right).$$

In period 2, consumers' set of information have changed to Ω_{i2}, and consumers have updated their beliefs about their privacy concerns -as long as they have purchased through the online channel-. Now, the monopolist's decision is to design a price schedule for the two-market channels given her private information.

To begin with, in period 2, expected demands by consumers are,

1. Demand for the brick channel in period two will be $q_{iB2}^{d} = \theta_i - p_{2B}^{d}$.

2. Expected demand by consumer *i* in the online channel conditional on his own information is the given by,

$$E\left[q_{iC2}^{d}|\Omega_{i2}\left(\alpha_{i1}, p_{2C}^{d}\right)\right] = \theta_i - E\left\{E\left\{\alpha_{i2}|\alpha_{i1}, z\right\}|\alpha_{i1}, p_{2C}^{d}\right\} - p_{2C}^{d},$$

where the second term in the right hand specifies to,

$$E\left[q_{iC2}^{d}|\Omega_{i2}\left(\alpha_{i1},p_{2C}^{d}\right)\right]=\theta_{i}-E\left\{\bar{x}\delta_{x}+\alpha_{i1}\delta_{\alpha}+z\delta_{z}|\alpha_{i1},p_{2C}^{d}\right\}-p_{2C}^{d},$$

and, finally to,

$$E\left[q_{iC2}^{d}|\Omega_{i2}\left(\alpha_{i1},p_{2C}^{d}\right)\right]=\theta_{i}-\left\{\bar{x}\delta_{x}+\alpha_{i1}\delta_{\alpha}+\left(a+bp_{2C}^{d}\right)\delta_{z}\right\}-p_{2C}^{d}.$$

The demand curve perceived by the monopolist is the sum of both demands, brick and click. After period 1, the monopolist gets some new information about the average privacy converns, and she uses this information to set prices in both markets.

$$E\left[q_{2}^{d}|\Omega_{m2}\left(z,p_{2}^{d}\left(z\right)\right)\right]=\lambda\left(\theta_{i}-p_{2B}^{d}\right)+\left(1-\lambda\right)\left(\theta_{i}-E\left\{\bar{x}\delta_{x}+\alpha_{i1}\delta_{\alpha}+z\delta_{z}|z\right\}-p_{2C}^{d}\right),$$

and using the expectations already discussed and (2.9), the expected demand curve faced by the firm is

$$E\left[q_{2}^{d}|\Omega_{m2}\left(z,p_{2}^{d}\left(z\right)\right)\right]=\lambda\left(\theta_{i}-p_{2B}^{d}\right)+\left(1-\lambda\right)\left(\theta_{i}-\left(\bar{x}\gamma_{x}+\delta_{z}\left(a+bp_{2C}^{d}\right)+z\delta_{\alpha}\gamma_{z}\right)-p_{2C}^{d}\right). \tag{2.27}$$

Thus, the monopolist's second-period expected profits, taking into account the extra benefits of data sales are,

$$\begin{aligned}E\left[\Pi_{2}^{d}|\Omega_{m2}\left(z,p_{2}^{d}\left(z\right)\right)\right]&=\lambda(\theta_{i}-p_{2B}^{d})p_{2B}^{d}\\&+(1-\lambda)(\theta_{i}-(\bar{x}\gamma_{x}+\delta_{z}\left(a+bp_{2C}^{d}\right)+z\delta_{\alpha}\gamma_{z}))-p_{2C})p_{2C}^{d}(1+r).\end{aligned} \tag{2.28}$$

2.5.1 Equilibrium

Once we have specified the expected demands and the expected benefits in $t = 1,2$ under price discrimination strategy, the equilibrium concept is noisy signaling equilibrium and consists of: the monopolist's price strategy in each period given his set of information Ω_{mt} in $t = 1,2$, the expected demand of the customers as a result of the utility maximization given their set of information Ω_{it} in $t = 1,2$, and beliefs of both consumers and monopolist follow the Bayes Rule to perform their posterior belief respectively. In equilibrium, the posterior beliefs are consistent with Bayes' rule and the equilibrium distribution of prices.

Definition 2 *The tuple $(p_{1B}^{d*}, p_{1C}^{d*})$ for period 1 and $(p_{2B}^{d*}, p_{2C}^{d*})$ for period 2 and the beliefs $(\alpha_{i1}, \alpha_{i2})$ is a Noisy Signaling Equilibrium with pice discrimination strategy if*

1. *Given $E\left[\Pi_1^d|\Omega_{m1}(\alpha_1)\right]$ in $t = 1$ and $E\left[\Pi_2^d|\Omega_{m2}\left(z, p_2^d(z)\right)\right]$ in t=2, the firm 's price strategies are for the first period*

$$p_1^{d*} = arg \max_{p_{1B}^d, p_{1C}^d} \left\{\lambda\left(\theta_i - p_{1B}^d\right) p_{1B}^d + (1-\lambda)\left(\theta_i - \bar{x} - p_{1C}^d\right) p_{1C}^d (1+r)\right\} \quad (2.29)$$

and the firm's price strategy for the second period is

$$p_2^{d*} = \quad arg \max_{p_{2B}^d, p_{2C}^d} \; E\left[\Pi_2^d|\Omega_{m2}\left(z, p_2^d(z)\right)\right] \quad (2.30)$$

2. *Given the prior beliefs of α_{it}, and the sets of the information Ω_{it} in each period $t = 1,2$, consumers maximize their utility and decide how much to purchase once the monopolist's price(s) have been announced in each channel.*

3. *Both monopolist and the firm use Bayesian Rules to compute the posterior beliefs given their set of information in each period and their beliefs are consistent with the equilibrium strategies.*

Given (2.7) and (2.10), and expected demands in $t = 1,2$, the monopolist maximizes her expected benefits in each period. In concrete, given the expected demand perceived by the monopolist in (2.27), its optimal price in period 2 in the click channel is

$$p_{2C}^{d*} = \frac{\theta_i - a\delta_z - \bar{x}\gamma_x - z\delta_\alpha\gamma_z}{2+2b\delta_z}. \tag{2.31}$$

We are searching for an equilibrium in which the representative consumer's inference rule is correct. Under this strategy, only the online channel is affected by the existence of signals in this market. Thus, consumers are correct believing that z observed by the firm equals $z = a + bp_{2C}^{d}$; then p_{2C}^{d} must also satisfy $p_{2C}^{d} = (z-a)/b$. Hence, in a linear equilibrium:

$$a = \frac{\theta_i - \bar{x}\gamma_x}{\gamma_z}, \tag{2.32}$$

and

$$b = \frac{2}{(\delta_a - 2)\gamma_z}. \tag{2.33}$$

Subsituting "*a*" and "*b*" in (2.31), we get the expected price, and therefore, expected demand and profits in period 2 in the online channel.

Proposition 3 characterizes the noisy signaling equilibrium.

Proposition 3 *Suppose that markets proportions are given by $\lambda \in (0,1)$, the firm's mark-up is $r \in (0,1)$, and linear inference rules. Thus, there exists a noisy signaling equilibrium with price discrimination strategy. In equilibrium,*

1. *In period 1, the equilibrium quantities and prices for the brick channel are*

$$p_{1B}^{d*} = \frac{\theta_i}{2}, \qquad q_{1B}^{d*} = \lambda\frac{\theta_i}{2},$$

and for the click channel,

$$p_{1C}^{d*} = \frac{1}{2}(\theta_i - \bar{x}), \qquad q_{1C}^{d*} = (1-\lambda)\frac{1}{2}(\theta_i - \bar{x})$$

2. *In period 2, the equilibrium quantities and prices for the brick channel are*

$$p_{2B}^{d*} = \frac{\theta_i}{2}, \qquad q_{2B}^{d*} = \lambda\frac{\theta_i}{2} \tag{2.34}$$

and in the click channel,

$$p_{2C}^{d*} = \frac{1}{2}(2-\delta_\alpha)(\theta_i - \bar{x}\gamma_x - z\gamma_z), \tag{2.35}$$

and the expected quantity by

$$q_{2C}^{d*} = \frac{1}{2}(1-\lambda)\delta_\alpha(\theta - \bar{x}\gamma_x - z\gamma_z).$$

Proof. See the Appendix. ■

Expected second-period benefits under price discrimination strategy over the two channels are therefore

$$\Pi_2^{d*} = \frac{1}{4}\left((1-\lambda)(r+1)(2-\delta_\alpha)\delta_\alpha(\theta_i - \bar{x}\gamma_x - z\gamma_z)^2 + \theta^2\lambda\right). \tag{2.36}$$

The second order conditions are satisfied. For the brick channel in period 1 and 2, the second order condition is $-2\lambda < 0$. In the online channel, the second order condition is $-2(1-\lambda)(1+r) < 0$ in period 1, and $2(1-\lambda)(1+r)(-1+b\delta_z) < 0$ in period 2. Plugging "b" in (2.33) in the second order for the click channel reveals a negative sign, i.e., $-\frac{2(1-\lambda)(r+1)\delta_\alpha}{2-\delta_\alpha} < 0$ and the second order conditions are satisfied.

Proposition 4 *In the click channel, if γ_z is fixed and common knowledge, then equilibirum prices are given by p_{1C}^{d*} and p_{2C}^{d*} as above specified. Furthermore, this is the unique equilibrium where consumers' inferences about z are a differentiable and invertible function of p_{2C}^{d*}.*

Proof. See the Appendix. ■

Signaling distorts prices upward in the click channel if $\bar{x} > z$. This fact also applies under the uniform price strategy. The second period price in the click channel is a linear function of the signal z and, under the price discrimination strategy, all the learning process only affects the second-period price in the online market. Note also that under a price discrimination policy, the second period prices in both markets do not depend on the mark-up earned by the monopolist, neither on the parameter λ. The price in the brick channel in both period does not change.

2.5.2 Comparative statics

Let us analyze the implications of the key parameters on the equilibrium prices scheme in this scenario. Firstly, we analyze the price as a function of the signal precision. Similar to the case under uniform pricing, the partial derivatives over z and $\bar{x}$ are negative. Furthermore, an increase in the precision of the signal γ_z has different effects on the second-period price in the online market depending on the relation between z and $\bar{x}$, just as we analyzed under uniform price.

Given that $\gamma_x = 1 - \gamma_z$, the partial derivative has the following form

$$\frac{\partial p_{2C}^{d}}{\partial \gamma_z} = \frac{1}{2}\left(2 - \delta_\alpha\right)\left(\bar{x} - z\right) = (+/-).$$

Note that this partial derivative is only affected by parameter δ_α. The partial derivative with respect the private signal's precision, γ_z, shows the same behaviour as the one under the uniform price setting.

Secondly, we analyze what happens in the expected price in period 2 when the importance that consumers give to their previous experiences changes, δ_α. The partial derivative of the price in the click channel in period 2 is,

$$\frac{\partial p_{2c}^{d*}}{\partial \delta_\alpha} = \frac{1}{2}(-\theta_i + \bar{x}\gamma_x + z\gamma_z) < 0,$$

which is negative given that $\theta_i > \bar{x}\gamma_x + z\gamma_z$. Just as with the case of uniform price, the price in the click channel turns out to be reduced if the importance that consumers give to its previous experience increases.

2.6 Comparison of scenarios

2.6.1 Profits

Before comparing profits under the different strategies, it is important to indicate how they move for different values of the parameters and variables in the model. Table 2.1 exhibit partial derivatives of expected profits under both price strategies in period 2:

Table 2.1 Comparative statics on profits in period 2

Π_2^{d*}	Π_2^{u*}
$\frac{\partial \Pi_2^{d*}}{\partial r} > 0$	$\frac{\partial \Pi_2^{u*}}{\partial r} > 0$
$\frac{\partial \Pi_2^{d*}}{\partial \lambda} \gtrless 0$	$\frac{\partial \Pi_2^{u*}}{\partial \lambda} \gtrless 0$
$\frac{\partial \Pi_2^{d*}}{\partial \bar{x}} < 0$	$\frac{\partial \Pi_2^{u*}}{\partial \bar{x}} < 0$
$\frac{\partial \Pi_2^{d*}}{\partial \delta_\alpha} > 0$	$\frac{\partial \Pi_2^{u*}}{\partial \delta_\alpha} > 0$
$\frac{\partial \Pi_2^{d*}}{\partial z} < 0$	$\frac{\partial \Pi_2^{u*}}{\partial z} < 0$
$\frac{\partial \Pi_2^{d*}}{\partial \theta_i} > 0$	$\frac{\partial \Pi_2^{u*}}{\partial \theta_i} > 0$
$\frac{\partial \Pi_2^{d*}}{\partial \gamma_z} \gtrless 0$	$\frac{\partial \Pi_2^{u*}}{\partial \gamma_z} \gtrless 0$

These derivatives point out the following comments,

- Profits under both strategies are decreasing in the value of the average-population privacy concerns in the market, $\bar{x}$, and the observed value of the average-population privacy concerns, z. The existence of privacy concerns disminishes the overall profits attainable for the monopolist.

- Profits are increasing in the value of the mark-ups, r. Monetization of data is profitable for the monopolist. Furthermore, the existence of mark-ups can be interpreted as the privacy-policy available in the market. Indeed, if we let $r \to 0$, the monopolist does not get extra profits for the sale of data, and it can be interpreted as if no data sale is permitted in the market. In Chapter 4 we analyze three policies concerning privacy where consumers can decide wheter to have their data sold (opt-out option).

- Profits are increasing, as expected, in the willingness to pay of consumers, θ_i.

- Profits are increasing in the precision of the monopolist’s private signal, γ_z, as long as $\bar{x} > z$. This indicates that the monopolist has incentives to invest in order to have a full informative signal. This incentive is analyzed in Chapter 3, where the investment in the precision of the information might exhibit negative externalities for consumers in the market. Specifically, the monopolist finds it profitable to manipulate market's information, and it might result in abuse of position.

- Profits are increasing in the importance that consumers give to its previous experience, δ_α. We also study in Chapter 3 the incentives for the monopolist to invest in security to improve consumers' previous experience in period 1.

The main purpose of this model is the monopolist's decision about pricing strategy under privacy concerns in a dual-channel context. In order to answer this question, it is necessary to know if price dicrimination generates higher expected profits than uniform pricing strategy. In other words, the sign of the difference, $E\Pi_2^{d*} - E\Pi_2^{u*} > 0$.

Proposition 5 *Expected profits in period 2 are higher under channel-based price discrimination.*

Proof. See the Appendix. ■

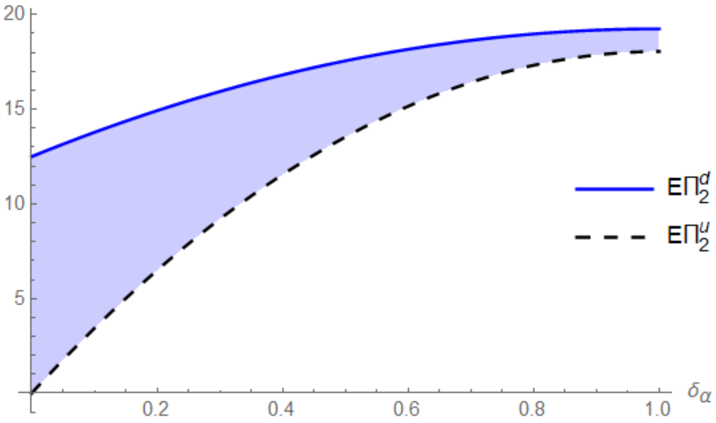
The monopolist will get higher profits if she discriminates over channels, and sets different prices in a market with signals. Note that this fact is consistent with microeconomics theory where price discrimination increase the monopolist's profits.

Consumers' learning process are determined not only by the public signal, z, but for their private signal, δ_α. Thus, the importance that consumers give to their previous experience plays and important role. Indeed, this weight in consumers' previous experience can mark a substancial reduction in the monopolist's expected profits in period 2.

In particular, depending on how much weight consumers put on their previous experience i.e., the value of δ_α, the distance between profits can be significant.

The shaded area in Figure 2.3 shows the cutback in the expected profits in period 2 taking into account both pricing strategies.

Fig. 2.3 Expected second-period benefits over changes in δ_α



If consumers give a huge importance to their experience in period 1 on privacy matters, $\delta_\alpha \to 1$, the difference of the expected profits will decrease. Otherwise, when $\delta_\alpha \to 0$, the difference turns out to be higher and clearly, expected profits from discrimination among channels are enormous.

2.6.2 Are prices similar (or not) over channels?

In the previous section, the results show that engaging in a channel-based price differentiation increase the monopolist's profits, which is consistent with microeconomics theory. In a market with heterotegeneous tastes and different product valuations, companies may increase their profits by segmenting consumers and charging differential prices, which allows for the extraction of additional consumer surplus.

Nevertheless, this finding might contradict existing empirical studies on price dispersion. Cavallo (2017) explains that there is significant heterogeneity in pricing behaviors across retailers: those with nearly identical online and offline prices, those with stable online markups (either positive or negative), and those with different prices that are not consistently higher or lower online. Furthermore, he finds that prices are identical about 72% of the time online and offline, that imply little within-retailer price dispersion. Much in line with the widespread idea of consistent prices across channels in order to maintain a strong brand and channel price integrity (Campbell and Campbell 2010). On the other hand, there are empirical papers that support the existence of price dispersion among channels. Cuellar and Brunamonti (2014) find price dispersion for a single item across retail channels. Also, given the common accepted possibility that online prices are more expensive than offline because of the possibility of tailored offers, Wolk and Ebling (2010) conclude that multi-channel retailers charge on average higher prices through the offline channel.There are several possible explanations that could shed light on this matter: price dispersion based on demographic self-selection and shopping intent (Cuellar and Brunamonti 2014), or the perceived risk in the online channel (Wolk and Ebling 2010). Cavallo (2017) also analyzes price dispersion based on IP addresses or browsing habits (very controversial causes), but surprisingly, they do not find any evidence to support those causes.

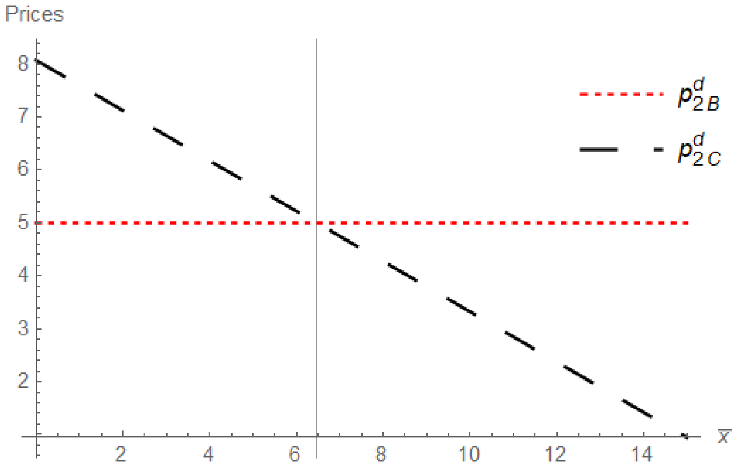
Our model shows that the differences between prices among channels depend on the average-population privacy concerns in the market, suggesting a possible explanation to the dispersion of prices between the sales channels. We find two thresholds that point out changes in the price orderings. Indeed, the fact of setting an identical price in both channels is not always the lowest price that can be achieved compared to discriminatory prices.

Importance of the average-population privacy concerns in the market

Prices are an important element in our model. Although the best strategy for the monopolist is to price discriminate between sales channels, our objective now is to analyze how prices are related. We will first analyze whether the price of the brick channel is always higher than the price of the click channel. That is, $p^d_{2B} - p^d_{2C} > 0$.

In order to make an interpretation, let us plot the prices. It can be easily seen that prices under price discrimination strategy cross for a certain value of average privacy in the market.

Fig. 2.4 p_{2B}^{d} vs. p_{2C}^{d} changes in $\bar{x}$



There is a certain level of average privacy concerns in the market, $\bar{x}_1$, from which the price level orderings in the market change. In other words, for an average privacy in the market lower than $\bar{x}_1$, we find that the price in the click channel is higher than the one charged in the brick. However, for higher levels of the average privacy concerns than $\bar{x}_1$, the result is reverse.

We calculate this threshold equaling (2.23) and (2.27), and leaving $\bar{x}$ alone. This yields,

$$\bar{x}_1 = \frac{\theta_i\,(1-\delta_\alpha) - z\gamma_z\,(2-\delta_\alpha)}{(2-\delta_\alpha)\,\gamma_x}.$$

As already said, price discrimination among channels is the optimal strategy. However, empirical findings in Cavallo (2017) show that in 72% on average prices are identical among channels in the real world. Thus, our interest is to analyze how the uniform price is regarding to discriminatory prices.

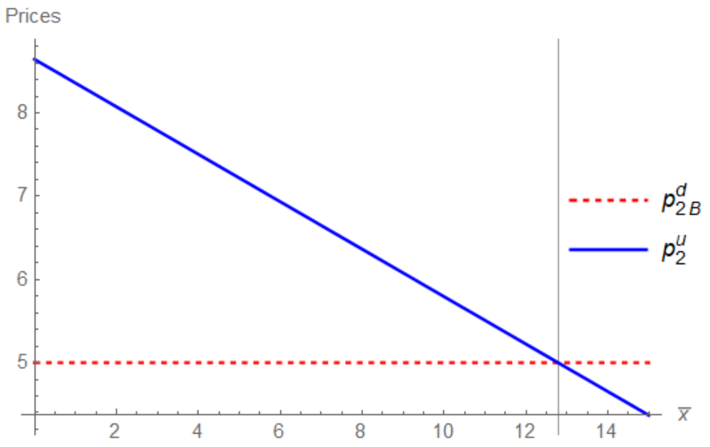
It is easy to check that the uniform price is always higher than the equilibrium price for the click channel i.e., $p_2^u - p_{2C}^d > 0$.

The difference of prices equals

$$p_2^u - p_{2C}^d = \frac{\lambda\,(2-\delta_\alpha)\,(\bar{x}\gamma_x + z\gamma_z)}{2+2(1-\lambda)r} > 0$$

which is positive. Surprisingly, this is not the case when the uniform price is compared with the equilibrium price to the brick channel. Comparing $p_2^u - p_{2B}^d > 0$, we find a new threshold that marks a point of change in the order on prices. See Figure 2.5.

Fig. 2.5 p_2^u vs. p_{2B}^d changes in $\bar{x}$



There is a threshold when we compare uniform pricing with the brick channel price, and it is obtained equaling (2.17) and (2.23) and solving for $\bar{x}$. We get this new threshold $\bar{x}_2$ which is,

$$\bar{x}_2 = \frac{\theta_i(1+(1-\lambda)r)(1-\delta_\alpha) - z\gamma_z(2-\delta_\alpha)(1-\lambda)(1+r)}{\gamma_x(2-\delta_\alpha)(1-\lambda)(1+r)}$$

When we compare $\bar{x}_1$ and $\bar{x}_2$,we get

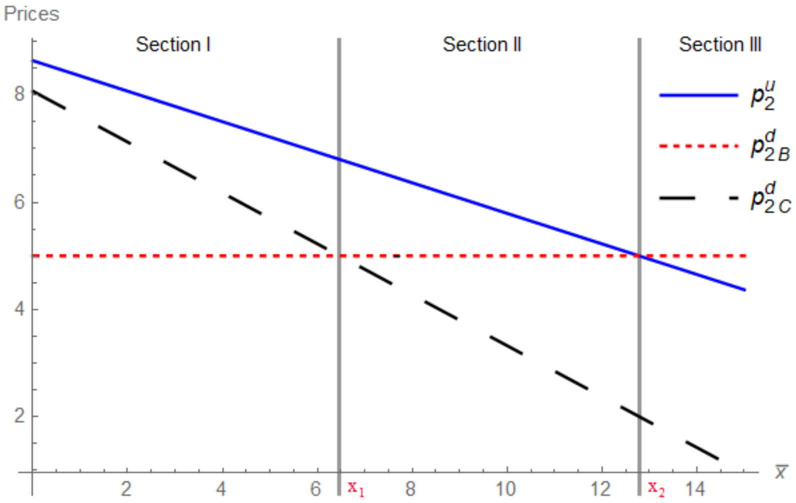
$$\bar{x}_2 - \bar{x}_1 = \frac{\theta_i\lambda(1-\delta_\alpha)}{\gamma_x(2-\delta_\alpha)(1-\lambda)(r+1)} > 0,$$

which is positive. The level of average privacy in the market that makes equal p_2^u and p_{2B}^d is higher than the one which equals the prices under price discrimination strategy.

Figure 2.6 shows how prices orderings change as a function of the average privacy in the market.

To sum up, the above findings are stated in the following proposition:

Fig. 2.6 Prices level when $\overline{x}$ changes



Proposition 6 *1. In Section I of Figure 2.6, for values of the average privacy in the market, $\overline{x} < \overline{x}_1$, the price ordering is $p_2^u > p_{2C}^d > p_{2B}^d$.*

2. In Section II of Figure 2.6, for values of the average privacy in the market, $\overline{x}_1 < \overline{x} < \overline{x}_2$, the price ordering is $p_2^u > p_{2B}^d > p_{2C}^d$.

3. In Section III of Figure 2.6, for values of the average privacy in the market, $\overline{x}_2 < \overline{x}$, the price ordering is $p_{2B}^d > p_2^u > p_{2C}^d$.

We get the thresholds as we specify above, $\overline{x}_1$ and $\overline{x}_2$, and we compare prices inside each interval. Figure 2.7 shows the prices behaviors with the same values of the parameters and variables, which are $\theta_i = 10$, $z = 3$, $\gamma_x = 0.5$, $\gamma_z = 0.5$, $\delta_\alpha = 0.1$, $\lambda = 0.5$ and $r = 0.5$. Once the values are set, we get the values of the thresholds, $\overline{x}_1 = 6.4736$ and $\overline{x}_2 = 12.7894$, represented in Figure 2.6 by the vertical thick lines. This Figure shows an example for these values. However, the orderings remain whatever values we have.

To conclude with, we find that in case of not setting an identical price in the two sales channels, the online prices can be higher or lower than the offline prices depending on the average privacy concerns in the market. In addition, and contrary to what is suggested in the literature, online and offline prices under a price discrimination strategy over channels, can be smaller than those charged under uniform pricing or identical price strategy in a dual-channel context. Consumers' learning procedure matter and affect the monopolist's expected profits, and therefore, their optimal decisions.

2.7 Effect of non-homogeneity in the set of consumers' information: welfare implications

This section studies how the existence of heterogeneity in the set of consumers' information in the online channel affect the equilibrium prices, as well as expected profits in period 2. To study this effect, we take the price discrimination strategy over channels as a benchmark. Thus, an interesting question is whether the distribution of information affects the nature of equilibrium, and how this affect the social welfare in the market.

To model heterogeneity in consumers, we assume that a proportion of them purchases over the two periods and other other proportion, are new in the market. Therefore, we now have different sets of information for consumers that operate in the click channel.

Let $\rho \in (0,1)$ be the proportion of consumers in the online channel who receive a signal about their privacy concerns in the first period because they have purchased the product via online in period 1. In other words, ρ represents the proportion of consumers whose set of information is given by Ω_{i2} in period 2 and, they are "savvies" or inexperienced. On the other hand, let $(1-\rho)$ be the proportion of consumers who have not received any signal about their privacy concerns or they do not purchase the product in period 1, and therefore, their set of information is Ω_{i1}, "non-savvies" or uninformed. This heterogeneity in consumers makes the "non-savvies" ones to have only a simple update of beliefs, and therefore, do not make any inference over the signal z because they have not developed any privacy concerns derived from the monopolist's use of their data.

Grubb (2015) exposes an overview of the Industrial Organization literature with behavioral consumers, and how consumers' heterogeneity is incorporated and its equilibrium effects. Furthermore, Armstrong (2015), examines how "savvies" and "non-savvies" consumers interact in the market, analyzing conditions in which there exist search externalities (when savvy consumers exert a positive externality on the non-savvy), ripoff externalities (when savvy consumers benefit from the presence of the non-savvy), and no interactions between consumers (consumers surplus do not depend on the proportion of savvies in the market). We find that consumer surplus and social surplus depend on the proportion of the more experienced consumers in the online channel. Indeed, the higher the level on information in consumers, the higher the social welfare (SW) and the consumer surplus (CS) attainable in this market.

The fact that the willingness-to-pay for the product is something homogeneous between channels and known makes it a suitable scenario to be able to focus on the study of heterogeneity. We are interested in how the non-homogeneity in the set of consumer information affects the equilibrium in the game. In addition, we seek to study how consumer surplus are under the above decribed heterogeneity, and the final implications in social welfare.

The general consumer surplus is,

$$CS = U - pq = (\theta_i - \alpha_{it})\, q - \frac{q^2}{2} - pq$$

therefore, social welfare is specified as $SW = CS + \Pi$, where Π are the monopolist's profits.

In order to define the inexperienced (uninformed) and experienced (informed) consumer surplus, note that:

- Inexperienced and more experienced consumers face a different sets of information. Then, the expected demand in period 2 will depend on the two types.

- Thus, taking into account that the demands from both types are different, they are specified by the following super-index, q_{2c}^{Ih} with I for those informed (more experienced) consumers and where h refers to heterogeneous consumers. Similarly, let q_{2c}^{NIh} identify the demand by the uninformed (inexperienced) consumers, NI. It is obvious to think that given that the expected demands in period 2 depend on the consumers' sets of information, therefore, the utilities derived for them will be also different. The monopolist sets a price in period 2 which will depend on the proportion of informed consumers.

The consumer surplus in the click channel is,

$$CS = (\theta_i - \alpha_{it})\, q_{2C}^{dh} - \frac{{q_{2C}^{dh}}^2}{2} - p_{2C}^{dh} q_{2C}^{dh}.$$

where p^{dh} identifies the scenario analyzed in this section under consumers' heterogeneity.

For a representative experienced consumer i, the utility maximization problem include the set of information for α_{it} in period 2,

$$CS^I = (\theta_i - E\{\alpha_{i2}|\alpha_{i1}, z\})\, q_{2C}^{Ih} - \frac{{q_{2C}^{Ih}}^2}{2} - p_{2C}^{dh} q_{2C}^{Ih}.$$

For a representative uninformed consumer i, NI,

$$CS^{NI} = (\theta_i - E\{\alpha_{i1}|, z\})\, q_{2C}^{NIh} - \frac{{q_{2C}^{NIh}}^2}{2} - p_{2C}^{dh} q_{2C}^{NIh}.$$

As can be seen, consumer surplus are different in which informed consumers I have more information because they have purchased in both periods, periods 1 and 2. On the contrary, uninformed consumers NI only purchase in one period, in period 2. Therefore, uninformed beliefs' about expected privacy concerned are just a simple expectation.

Namely,

$$q_{2C}^{Ih} = \rho\left(\theta_i - \delta_z(a + bp_{2C}^{dh}) - z\delta_\alpha\gamma_z - \bar{x}\gamma_x - p_{2C}^{dh}\right), \tag{2.37}$$

and,

$$q_{2C}^{NIh} = (1-\rho)\left(\theta_i - \gamma_z(a + bp_{2C}^{dh}) - \bar{x}\gamma_x - p_{2C}^{dh}\right). \tag{2.38}$$

In period $t = 2$, the demand by consumers are,

1. Demand for the brick channel in period two is $q_{iB2} = \theta_i - p_{2B}^{dh}$.

2. Expected demand by consumer i in the online channel conditional on his own information is the given by

$$q_{iC2}^{dh} = (1-\rho)\left(\theta_i - \gamma_z(a + bp_{2C}^{dh}) - \bar{x}\gamma_x\right) + \rho\left(\theta_i - \delta_z(a + bp_{2C}^{dh}) - z\delta_\alpha\gamma_z - \bar{x}\gamma_x\right) - p_{2C}^{dh}.$$

The monopolist's expected demand in period 2 under price discrimination strategy is

$$E\left[q_2^{dh}|\Omega_{m2}\left(z, p_2^{dh}(z)\right)\right] =$$
$$(1-\lambda)\left((1-\rho)\left(\theta_i - \gamma_z(a + bp_{2C}^{dh}) - \bar{x}\gamma_x\right) + \rho\left(\theta_i - \delta_z(a + bp_{2C}^{dh}) - z\delta_\alpha\gamma_z - \bar{x}\gamma_x\right) - p_{2C}^{dh}\right)$$
$$+\lambda(\theta_i - p_{2B}^{dh}). \tag{2.39}$$

Given (2.7) and (2.10), and expected demands in $t = 1,2$, the monopolist maximizes her expected profits in each period. More specifically, given the expected demand perceived by the monopolist in (2.39), its optimal price in period 2 in the click channel is

$$p_{2C}^{dh*} = \frac{\theta_i - \bar{x}\gamma_x - a\rho\delta_z - \gamma_z(\rho z\delta_\alpha - a(1-\rho))}{2(1 + b\rho\delta_z + b\gamma_z(1-\rho))}. \tag{2.40}$$

We are searching for an equilibrium in which the representative consumer's inference rule is correct for experienced (informed) and inexperienced (uninformed) consumers. Under this scenario, only the online channel is affected by the existence of signals and heterogeneity in this market. Thus, consumers are correct believing that z observed by the firm equals $z = a + bp_{2C}^{dh}$; then p_{2C}^{dh} must also satisfy $p_{2C}^{dh} = (z-a)/b$. Hence, in a linear equilibrium:

$$a = \frac{\theta_i - \bar{x}\gamma_x}{\gamma_z}, \tag{2.41}$$

and

$$b = \frac{2}{\gamma_z\left(\rho\delta_\alpha - 2\right)}. \tag{2.42}$$

Subsituting "a" and "b" in (2.40), we get the expected price, and therefore, the expected demand and expected profits in period 2 in the online channel.

Proposition 7 *Suppose that markets proportions are given by $\lambda \in (0,1)$, second-period mark-up $r \in (0,1)$, and the distribution of consumer heterogeneity is ρ, there exists a noisy signaling equilibrium with price discrimination. In equilibrium,*

1. *The firm sets discriminate prices in period $t = 2$*

$$p_{2B}^{dh*} = \frac{\theta_i}{2}, \tag{2.43}$$

and

$$p_{2C}^{dh*} = \frac{1}{2}\left(2-\rho\delta_\alpha\right)\left(\theta_i - \bar{x}\gamma_x - z\gamma_z\right), \tag{2.44}$$

in each channel.

Proof. See the Appendix. ■

Expected period 2 profits with different levels of experienced consuemrs consumers are,

$$\Pi_2^{dh*} = \frac{1}{4}\left(\lambda\theta_i^2 + (1-\lambda)\rho(r+1)\delta_\alpha\left(2-\rho\delta_\alpha\right)\left(\theta_i - \bar{x}\gamma_x - z\gamma_z\right)^2\right). \tag{2.45}$$

2.7.1 Discussion

Once we get the equilibrium, our aim is to explore the implications of the existence of more experienced consumers in privacy mattersin this market. To that purpose, we compute the consumers surplus for a representative experienced consumer *i* and for a representative less experienced consumer *i*. Later on, we explore the effects on welfare due to the existence of this heterogeneity.

To start with, we compute the consumer surplus for both experienced consumers, specified by CS^I, and inexperienced consumers, specified by CS^{NI}. In particular,

$$CS^I = \frac{1}{8}\delta_\alpha^2\rho^3(\theta_i - \bar{x}\gamma_x - z\gamma_z)^2,$$

and

$$CS^{NI} = \frac{1}{8}\delta_\alpha^2(1-\rho)\rho^2(\theta - \bar{x}\gamma_x - z\gamma_z)^2.$$

Furthermore, we compute the consumer surplus for those who purchase in the brick channel,

$$CS_{2B} = \frac{\theta_i^2}{8}.$$

Adding the consumer surplus for informed and uninformed, and those purchasing in the brick channel, we get the total consumer surplus in the market, CS^T, given by

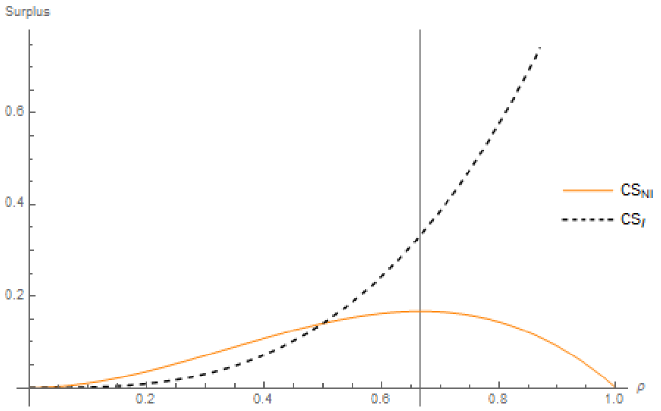
$$CS^T = \frac{1}{8}\left(\theta^2\lambda + \delta_\alpha^2(1-\lambda)\rho^2(\theta_i - \bar{x}\gamma_x - z\gamma_z)^2\right). \tag{2.46}$$

From the expression of CS^T we find that:

- The partial derivative with respect ρ, that represents the presence of uninformed and informed consumers in the online market, is positive. In other words, $\frac{\partial CS}{\partial \rho} > 0$. This fact highlight an interesting interpretation. As the proportion of more experienced consumers increases in the market, consumer surplus will also increase.

- Consumer surplus for informed consumers is positive in the second derivative, being always increasing. However, the uninformed' consumers surplus is concave, as can be seen in Figure 2.7.

Fig. 2.7 CS depending on ρ.



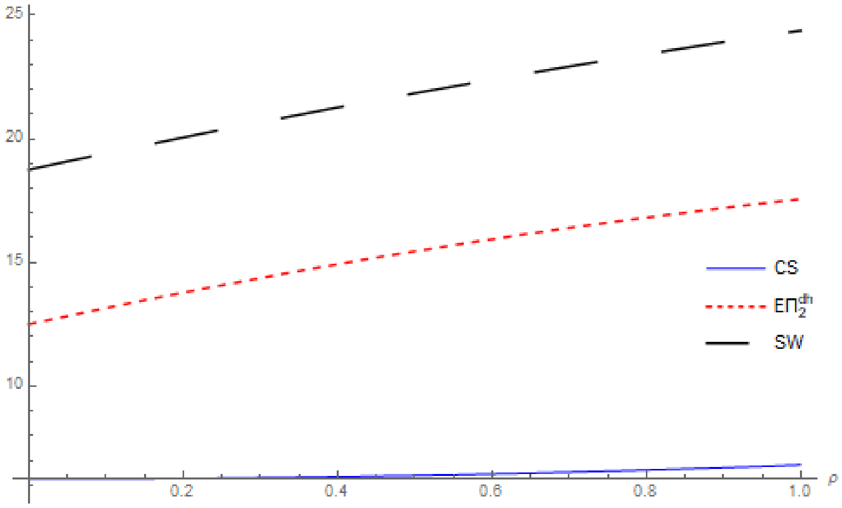
In Figure 2.7, CS^{NI} is increasing until it reaches an exact value of $\rho = \frac{2}{3}$, delimited by a vertical line. From that specific value, the consumer surplus for uniformed consumers starts to decrease. On the other hand, CS^{I} has an exponential form and, it is always increasing. Furthermore, both CS cross when $\rho = \frac{1}{2}$. Thus, for values of $\rho \in (0, \frac{1}{2})$, we get that $CS^{NI} > CS^{I}$; otherwise, for values of $\rho \in (\frac{1}{2}, 1)$, we have $CS^{NI} < CS^{I}$. This result indicates that for lower values of information, being an inexperienced consumer yields higher consumer surplus. However, as long as the proportion of informed consumers grow up in the market, the uninformed consumer surplus starts to decrease, thus they have incentives to become more informed over the average privacy concerns. Information increases consumer surplus.

We next examine the implications for SW when there are inexperienced consumers in the market. As $SW = \Pi + CS^{T}$, then adding the expected profits in period 2 of the monopolist, we get the SW, that is

$$SW = \frac{1}{8}\left(3\theta_i^2\lambda + 2\delta_\alpha(1-\lambda)\rho(r+1)(2-\delta_\alpha\rho)(\theta_i+\bar{x}\gamma_x+z\gamma_z)^2\right) + \frac{1}{8}\left(\delta_\alpha^2(1-\lambda)\rho^2(\theta_i+\bar{x}\gamma_x+z\gamma_z)^2\right).$$

In Figure 2.8, we plot CS^T, expected profits for the monopolist and total SW.

Fig. 2.8 SW, CS^T and expected profits Π_2^{dh} depending on the proportion of experienced consumers



A few remarks can be done: Firstly, the monopolist's profits in period 2 are increasing in the proportion of informed consumers. Secondly, the social surplus SW, similarly to the expected profits for the monopolist, is also increasing in ρ. Finally, the existence of heterogeneity in the consumers' information, and therefore, uniformed consumers, harm the whole market in general. Thus, homogeneous consumers in the level of information guarantee gains in the market, and hence a higher SW.

2.8 Conclusions

In the digital era, firms are aware that operating in different channels and the presence in many of them, need the development of new business models and strategies in order to make profits in a multi-channel context. In this Chapter, motivated by the unprecedented increase of sales on the Internet and the availability of consumer information, we analyze the monopolist's decision to set a uniform price or price discriminate among channels, when consumers who purchase in the online channel have privacy concerns over their personal data.

This Chapter offers a model with signals in the market, where both the monopolist and consumers are learning the privacy concerns of the latter. The monopolist receives a noisy private signal that gives her information about the value of privacy for consumers, and uses it in order to adjust prices in period 2. On the other hand, consumers make an inference from the second period's price over the monopolist's private information. However, consumers' expected demand are derived from not only the public signal (prices) but their private signal (previous experience in privacy matters).

Firstly, we analyze the optimal price policy for the monopolist. We find out that the monopolist's expected profits in period 2 are higher under channel-based price discrimination with the presence of signals and consumers' learning in the market. Furthermore, we get that there is price dispersion among channel. In particular, price dispersion depends on the average level of privacy concerns in the market. Thus, our results do not agree with the literature saying that prices offline are always higher than those online; in our analysis, the existence of privacy concerns can explain the existence of price dispersion between sales channels.

On the other hand, we aim to study how the heterogeneity in consumers' information affect the nature of equilibrium and the social welfare in this market. Our results, interestingly, point out that the presence of more experienced consumers about their privacy concerns increase social welfare in the market. That suggest, in line with regulations about consumers' privacy in digital markets, that the higher control that consumers have about their information, the higher the welfare that can be achieved in the marketplace.

Our results emphasize the importance of privacy concerns in decision-making for both players in the market. Some studies focus on the existence of other factors that may affect the design of prices in channels context, like shipping cost, waiting cost, transportation cost to the shop, etc. and they do not incorporate privacy concerns as an important part of consumers' utility. We address this fact in this chapter, but we leave other relevant questions aside. We assume the proportion of channels exogenous, and the linearity of the functions suppose an important technical limitation that we tried to cover. Having the proportions of channels depending on prices would give rise to interesting questions where prices and privacy concerns will lead the flow of consumers in both channels. How much privacy are you willing to give up in order to get a better price? This can be a fascinating idea for future research.

2.9 Appendix

Proof of Proposition 1

Using Definition 1 under uniform price strategy, the conditional expectations (2.7) and (2.10) in the main text, consumers are correct in believing that z observed by the firm equals $z = a + bp_2^u$.

1. Given (2.7) and (2.10) in the main text, and the expected demand in $t = 1,2$, the monopolist maximizes her expected profits in each period (2.13) and (2.15) in the main text, respectively. Taking the first order conditions with respect p_1^u and p_2^u yields

$$\lambda\,(\theta_i - p_1) + (1-\lambda)(r+1)\,(\theta_i - p_1 - x) - \lambda p_1 + (1-\lambda)\,(-p_1)\,(r+1) = 0, \quad (2.47)$$

and in period 2

$$\begin{aligned}(1-\lambda)(r+1)\,(-\delta_z\,(a+bp_2) - z\delta_\alpha\gamma_z + \theta_i - p_2 - \bar{x}\gamma_x)\\ + (1-\lambda)p_2(r+1)\,(-b\delta_z - 1) + \lambda\,(\theta - p_2) - \lambda p_2 = 0. \quad (2.48)\end{aligned}$$

The second-order conditions holds. In period 2, second order conditions is $2(1-\lambda)(r+1)\,(-b\delta_z - 1) - 2\lambda < 0$ where b as we specified in (2.23) in the main text. Then, solving (2.47) and (2.48) for prices strategies yields

$$p_1^{u*} = \frac{\theta_i + (1-\lambda)\,(r\theta_i - (r+1)\bar{x})}{2(1-\lambda)r + 2},$$

and

$$p_2^{u*} = \frac{\theta_i(1+(1-\lambda)r) - (1-\lambda)(r+1)\bar{x}\gamma_x - (1-\lambda)(r+1)z\delta_\alpha\gamma_z - a(1-\lambda)(r+1)\delta_z}{2\,(1+b(1-\lambda)(r+1)\delta_z + (1-\lambda)r)}.$$

2. Given any observation of p_2^{u*} in the second period, consumers and firm updates their information. Consumers will make an inference over z after observing the second period price, then consumers are correct in believing that the z observed by the firm actually equals $p_2^{u*} = \frac{z-a}{b}$. Then, in a linear equilibrium

$$a = \frac{\theta_i(1+r(1-\lambda)) - \bar{x}\gamma_x(1-\lambda)(r+1)}{(1-\lambda)(r+1)\gamma_z},$$

and

$$b = -\frac{2+2r(1-\lambda)}{(1-\lambda)(r+1)\,(2-\delta_\alpha)\,\gamma_z}.$$

3. Substituting a and b in (2.21) in the main text, using simplifications described in (2.11) and (2.12) in the main text, we get the expected second period price and expected second period profits, specified in (2.24) and (2.26) in the main text.

Proof of Proposition 2

If γ_z is fixed and common knowledge, then the equilibrium prices in period 1 and 2, are specified in the main text. Furthermore, this is the unique equilibrium where comsumers' inferences about z are a differentiable and invertible function of p_2^u.

The calculations show that this a linear equilibrium. The uniqueness property follows from the nature of the signaling differential equation. Assume that consumers infer $z = \hat{z}(p_2^u)$ if second period price is p_2^u, where $\hat{z}$ is C^1. The demand curve faced by the firm in period 2 is

$$\lambda\,(\theta_i - p_2^u) + (1-\lambda)\,(\theta_i - (\bar{x}\gamma_x + \delta_z\hat{z}p_2^u + z\,(p_2^u)\,\delta_\alpha\gamma_z) - p_2^u)\,.$$

The profit maximization price satisfies the first-order condition

$$\begin{aligned}(1-\lambda)(r+1)\left(-z\,(p_2^u)\,\delta_\alpha\gamma_z + \theta_i - p_2^u - x\gamma_x - \delta_z\hat{z}' p_2^u - \hat{z}\,(p_2^u)\,\delta_z\right)&\\ +\lambda(\theta_i - p_2^u) - \lambda p + (1-\lambda)(-p_2^u)(r+1) = 0,&\end{aligned}$$

and implicitly defines the correct rule, $z(p_2^u)$. In a Bayes-Nash equilibrium, consumers use the correct inference rule, that is $\hat{z}\left(p_2^u\right) = z\left(p_2^u\right)$; hence, $z\left(p_2^u\right)$ must solve the ordinary differential equation

$$(2p_2^u - \theta_i)(1-r(1-\lambda)) + \bar{x}\gamma_x(1+r)(1-\lambda) = \\ -(1+r)(1-\lambda)\left(z^{'} p_2^u\delta_z + z(p_2^u)(\delta_z+\delta_\alpha\gamma_z)\right).$$

We proceed ordering and simplifying the terms in the previous differential equation to look for general/particular solutions. To that end,

- Firstly, dividing the ordinary differential equation by $(1+r)(1-\lambda)p_2^u\delta_z$, we get

  $$\frac{2}{\delta_z}\left(\frac{1+r(1-\lambda)}{(1+r)(1-\lambda)}\right) - \frac{\theta_i}{p_2^u\delta_z}\left(\frac{1+r(1-\lambda)}{(1+r)(1-\lambda)}\right) + \frac{\bar{x}\gamma_x}{\delta_z} = \\ -\left(\frac{z^{'}\left(p_2^u\right)\delta_z p_2 + z\left(p_2^u\right)(\delta_z+\delta_\alpha\gamma_z)}{p_2^u\delta_z}\right).$$

  Letting $s = \frac{2}{\delta_z}\left(\frac{1+r(1-\lambda)}{(1+r)(1-\lambda)}\right)$, $m = \frac{\theta_i}{\delta_z}\left(\frac{1+r(1-\lambda)}{(1+r)(1-\lambda)}\right)$, $t = \frac{\bar{x}\gamma_x}{\delta_z}$,and $r = \frac{(\delta_z+\delta_\alpha\gamma_z)}{\delta_z}$, and reordering the terms yields

  $$z^{'}(p_2^u) + z(p_2^u)p_2^{-1}r = p_2 m^{-1} - p_2^{-1}t - s.$$

- Secondly, multiplying the above expression by p^r (the integrating factor) then gives

  $$p^r\left(z^{'}(p_2^u) + z(p_2)p_2^{-1}r\right) = p^r\left(mp_2^{-1} - tp_2^{-1} - s\right),$$

  which may be integrated to

  $$p^r\left(z(p_2)\right) = p^r\left(\frac{m-t}{r} - \frac{p\quad s}{1+r}\right) + C.$$

for some constant C. This is a general solution. To determine C, we need the value of the function $z(p_2)$ at one point. For instance, if $z(0)$ is finite (the initial condition), then, evaluating the differential equation at $p_2 = 0$, gives that $C = 0$. Hence $z(p_2)$ is linear in p_2.

Proof of Proposition 3

Using the Definition 2 under price discrimination strategy, the conditional expectations (2.7) and (2.10) in the main text, consumers are correct in believing that z observed by the firm equals $z = a + bp^d_{2C}$.

1. Given (2.7) and (2.10) in the main text, and the expected demand in period 2 in equation (2.27) in the main text, the monopolist maximizes her expected profits in each period, respectivaley. Taking the first order conditions with respect, p^d_{1B} and p^d_{1C} in period 1

$$\lambda(\theta_i - p_{1B}) - \lambda p_{1B} = 0, \tag{2.49}$$

and

$$(1-\lambda)(r+1)(\theta_i - p_{1C} - \bar{x}) - (1-\lambda)p_{1C}(r+1) = 0. \tag{2.50}$$

Taking the first order conditions with respect p^d_{2B} and p^d_{2c} in period 2, yields

$$\lambda(\theta_i - p_{2B}) - \lambda p_{2B} = 0, \tag{2.51}$$

and

$$(1-\lambda)(r+1)\,(\theta_i - z\delta_\alpha\gamma_z - \delta_z(a+b \quad p_{2C}) - p_{2C} - \bar{x}\gamma_x) \\ + (1-\lambda)p_{2C}(r+1)\,(-b\delta_z - 1) = 0. \tag{2.52}$$

The second conditions holds in period 1, that is $-2\lambda < 0$ and $-2(1-\lambda)(r+1) < 0$. In period 2, the second order conditions also holds, $-2\lambda < 0$ and $2(1-\lambda)(r+1)(-b\delta_z - 1) < 0$ where b is as we specify in (2.33) in the main text. Then, solving (2.49) and (2.50) for period 1, (2.51) and (2.52) for period 2, we get

$$p_{1B}^{d*} = \frac{\theta_i}{2}, \tag{2.53}$$

and

$$p_{1C}^{d*} = \frac{1}{2}(\theta_i - \bar{x}), \tag{2.54}$$

in period 1. For period 2, we get

$$p_{2B}^{d*} = \frac{\theta_i}{2}$$

and, the ex ante price in (2.31) in the main text, which is,

$$p_{2C}^{d*} = \frac{\theta_i - a\delta_z - \bar{x}\gamma_x - z\delta_\alpha\gamma_z}{2(1+b\delta_z)}.$$

2. Given any observation of p_{2C}^{d*} in the second period, consumers and firm updates their information. Consumers will make an inference over z after observing the second period price, then consumers are correct in believing that the z observed by the firm actually equals $p_{2C}^{d*} = \frac{z-a}{b}$. Then, in a linear equilibrium

$$a = \frac{\theta_i - \bar{x}\gamma_x}{\gamma_z},$$

and

$$b = \frac{2}{(\delta_\alpha - 2)\gamma_z}.$$

as we specified in (2.32) and (2.33) in the main text.

3. Substituting a and b in (2.31) in the main text, using simplifications described in (2.11) and (2.12) in the main text, we get the expected second period price and expected second period profits, specified in (2.35) and (2.36) in the main text.

Proof of Proposition 4

In the click channel, If γ_z is fixed and common knowledge, then the equilibrium prices in period 1 and 2, are specified in the main text. Furthermore, this is the unique equilibrium where comsumers' inferences about z are a differentiable and invertible function of p_2^d.

The calculations show that this a linear equilibrium. The uniqueness property follows from the nature of the signaling differential equation. Assume that consumers infer $z = \hat{z}(p_{2C})$ if second period price is p_{2C}, where $\hat{z}$ is C^1.

The demand curve faced by the firm in period 2 is

$$(1-\lambda)p_{2C}(r+1)\,(\theta_i - z\delta_\alpha\gamma_z - \bar{x}\gamma_x - p_{2C} - \hat{z}\,(p_{2C})\delta_z) + \lambda\, p_{2B}(\theta_i - p_{2B}).$$

The profit maximization price satisfies the first-order condition

$$(1-\lambda)(r+1)\,(\theta_i - p_{2C} - \bar{x}\gamma_x - z\delta_\alpha\gamma_z - \hat{z}\delta_z) - (1-\lambda)p_{2C}(r+1)\left(1 + \hat{z'}\,(p_{2C})\,\delta_z\right) = 0,$$

and implicitly defines the correct rule, $z(p_{2C})$. In a Bayes-Nash equilibrium, consumers use the correct inference rule, that is $\hat{z}\,(p_{2C}) = z\,(p_{2C})$; hence, $z\,(p_{2C})$ must solve the ordinary differential equation

$$\begin{aligned}(\theta_i - \bar{x}\gamma_x)\,[(1-\lambda)\,(r+1)] - 2p_{2C}\,[(1-\lambda)\,(r+1)] = \\ [(1-\lambda)\,(r+1)]\left(z\,(\delta_z\gamma_z + \delta_z) + z'p_{2C}\delta_z\right).\end{aligned}$$

We proceed ordering and simplifying the terms in the previous differential equation to look for general/particular solutions. To that end,

- Firstly, dividing the ordinary differential equation by $(1+r)(1-\lambda)p_{2C}\delta_z$, we get

$$\frac{(\theta_i - \bar{x}\gamma_x)}{p_{2C}\delta_z} - \frac{2}{\delta_z} = \frac{z(\delta_z\gamma_z + \delta_z)}{p_{2C}\delta_z} + z'.$$

* Letting $m = \frac{(\theta_i - \bar{x}\gamma_x)}{\delta_z}$, $s = \frac{2}{\delta_z}$, and $r = \frac{(\delta_z\gamma_z + \delta_z)}{\delta_z}$, and reordering terms yields

$$z' + zp_{2C}^{-1}r = mp_{2C}^{-1} - s.$$

- Secondly, multiplying the above expression by p^r (the integrating factor) then gives

$$p^r\left(z^{'}(p_{2C}) + z(p_{2C})p_{2C}^{-1}r\right) = p^r\left(mp_{2C}^{-1} - s\right),$$

which may be intedrated to

$$p^r\left(\frac{m}{r} - \frac{p_{2C}s}{r+1}\right) + C,$$

for some constant C. This is a general solution. To determine C, we need the value of the function $z(p_{2C})$ at one point. For instance, if $z(0)$ is finite (the initial condition), then, evaluating the differential equation at $p_{2C} = 0$, gives that $C = 0$. Hence $z(p_{2C})$ is linear in p_{2C}.

Proof of Proposition 5

We want to know whether channel-based price discrimination generates higher profits or not. In order to make the proof simpler, let us define the following terms:

- $A = (1-\lambda)(1+r)$,
- $B = (1 + r(1-\lambda))$,
- $C = \bar{x}\gamma_x + z\gamma_z$,

- $D = (2-\delta_\alpha)\,\delta_\alpha$,
- $B - A = \lambda$,
- $1 - D = 1 - (2-\delta_\alpha)\,\delta_\alpha$,

which are, furthermore, all non-negative. Then, we rewrite $E\Pi_2^{d*} - E\Pi_2^{u*} > 0$ using the terms defined before:

$$\frac{1}{4}\left(AD(\theta_i - C)^2 + {\theta_i}^2\lambda\right) > \frac{D(\theta_i B - AC)^2}{4B}.$$

Thus, operating and simplifying,

$$AD(\theta_i - C)^2 + \theta_i^2\lambda > \frac{D(\theta_i B - AC)^2}{B};$$

$$ADB(\theta_i - C)^2 + \theta_i^2\lambda B > D(\theta_i B - AC)^2;$$

$$ADB\left({\theta_i}^2 + C^2 - 2\theta_i C\right) + \theta_i^2\lambda B > D\left({\theta_i}^2 B^2 + A^2C^2 - 2\theta_i BAC;\right)$$

$${\theta_i}^2\lambda B > D\left({\theta_i}^2 B\,(B-A) - AC^2\,(B-A)\right);$$

$${\theta_i}^2\lambda B > D\left({\theta_i}^2 B\lambda - AC^2\lambda\right);$$

$${\theta_i}^2\lambda B > D\lambda\left({\theta_i}^2 B - AC^2\right);$$

$${\theta_i}^2 B > D\left({\theta_i}^2 B - AC^2\right);$$

$${\theta_i}^2 B > {\theta_i}^2 BD - AC^2 D;$$

Finally, we get that the inequality is positive, that is,

$${\theta_i}^2 B\,(1-D) + AC^2 D > 0.$$

Then, the expected profits from channel-based price discrimination are higher than profits from an identical pricing policy among channels.

Proof of Proposition 7

In this case, we do not exposure a formal definition, but we have to take into account that the benchamark is price discrimination among channels and we adapt the definition 2 in order to get the equilibrium. Using the definition 2 under price discrimination strategy and given that ρ represents the proportion of consumers in the online arm who receive a signal about their privacy concerns in the first period, the conditional expectations (2.7) and (2.10) in the main text, consumers are correct in believing that z observed by the firm equals $z = a + bp^{d}_{2C}$.

1. Given (2.7) and (2.10) in the main text, and the expected demand in period 2 in equation (2.39) in the main text, the monopolist maximizes her expected profits in each period, respectivaley. Taking the first order conditions with respect, p^{dh}_{1B} and p^{dh}_{1C} in period 1

$$\lambda(\theta_i - p^{dh}_{1B}) - \lambda p^{dh}_{1B} = 0, \tag{2.55}$$

and

$$(1-\lambda)(r+1)(\theta_i - p^{dh}_{1C} - \bar{x}) - (1-\lambda)p^{dh}_{1C}(r+1) = 0. \tag{2.56}$$

Taking the first order conditions with respect p^{dh}_{2B} and p^{dh}_{2c} in period 2, yields

$$\lambda(\theta_i - p^{dh}_{2B}) - \lambda p^{dh}_{2B} = 0, \tag{2.57}$$

and

$$\begin{aligned}(1-\lambda)(1-\rho)&(-\gamma_z(a+bp^{dh}_{2c}) + \theta_i - p^{dh}_{2c} - \gamma_x\bar{x})\\ &+ (1-\lambda)\rho\left(-\delta_z(a+bp^{dh}_{2c}) + \theta_i - p^{dh}_{2c} - \gamma_x\bar{x} - \gamma_z\delta_\alpha z\right)\\ &+ p^{dh}_{2c}((1-\lambda)(1-\rho)(-b\gamma_z - 1) + (1-\lambda)\rho(-b\delta_z - 1)) = 0.\end{aligned} \tag{2.58}$$

The second conditions holds in period 1, that is $-2\lambda < 0$ and $-2(1-\lambda)(r+1) < 0$. In period 2, the second order conditions also holds, $-2\lambda < 0$ and $2(1-\lambda)(1-\rho)(-b\gamma_z - 1) + 2(1-\lambda)\rho\,(-b\delta_z - 1)$ where b is as we specify in (2.42) in the main text. Symplifying the expression, and using (2.11), we get $-\frac{2\delta_\alpha(1-\lambda)\rho}{2-\delta_\alpha\rho} < 0$. Then, solving (2.55) and (2.56) for period 1, (2.57) and (2.58) for period 2, we get

$$p_{1B}^{dh*} = \frac{\theta_i}{2}, \tag{2.59}$$

and

$$p_{1C}^{dh*} = \frac{1}{2}(\theta_i - \bar{x}) \tag{2.60}$$

in period 1. For period 2, we get

$$p_{2B}^{dh*} = \frac{\theta_i}{2}, \tag{2.61}$$

and, the ex ante price in (2.40) in the main text, which is,

$$p_{2C}^{dh*} = \frac{\theta_i - \bar{x}\gamma_x - a\rho\delta_z - \gamma_z(\rho z\delta_\alpha - a(1-\rho))}{2(1 + b\rho\delta_z + b\gamma_z(1-\rho))}.$$

2. Given any observation of p_{2C}^{dh*} in the second period, consumers and firm updates their information. Consumers will make an inference over z after observing the second period price, then consumers are correct in believing that the z observed by the firm actually equals $p_{2C}^{dh*} = \frac{z-a}{b}$. Then, in a linear equilibrium,

$$a = \frac{\theta_i - \bar{x}\gamma_x}{\gamma_z},$$

and

$$b = \frac{2}{\gamma_z(\rho\delta_\alpha - 2)}.$$

as we specified in (2.41) and (2.42) in the main text.

3. Substituting a and b in (2.40) in the main text, using simplifications described in (2.11) and (2.12) in the main text, we get the expected second period price and expected second period profits, specified in (2.44) and (2.45) in the main text.

Chapter 3

Security in digital markets

3.1 Introduction

In the digital age, we live in an always-on world. Our commercial and private lives are migrating to online platforms at a frenetic pace thanks to technological advances and a vast array of apps. To speak of the intersection between technology and privacy is inevitable. Consequently, privacy has long been a moving target. For example, in October 2017, Amazon unveiled *Amazon key*, which lets deliverers into consumers' homes.[1] It has thus become a reality that corporations not only access our digital data but also gain a window into our very lives. To use this service, consumers must buy a camera and a digital key to enable delivery and guarantee security. Although this idea is original within the industry, it has become the target of hackers.[2] As a result, questions over security and trust in digital markets abound.

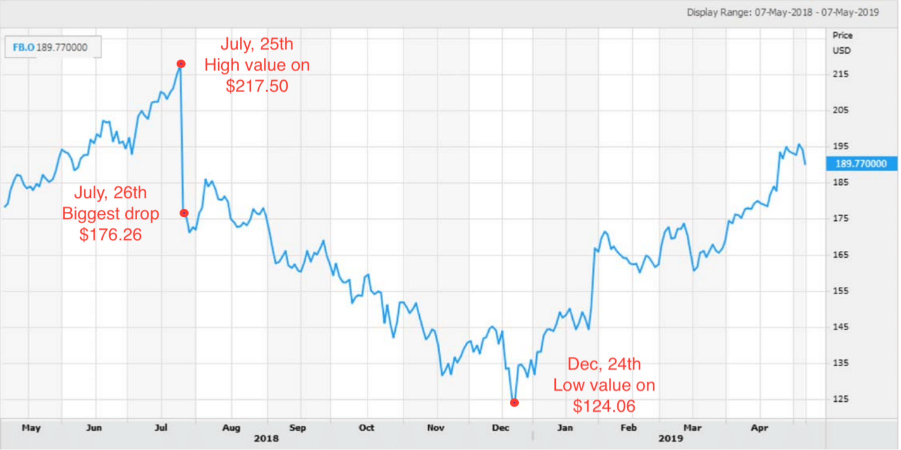
Security in digital markets is therefore a fundamental consideration when consumers are concerned with privacy. Additionally, these concerns have their impact on businesses, and in

[1] https://www.youtube.com/watch?v=wn7DBdaUNLA

[2] https://www.forbes.com/sites/kevinmurnane/2017/12/12/what-could-possibly-go-wrong-amazon-key/#187c99974119

consumers' perception over security in a digital environment as well.

Fig. 3.1 Facebook's stock market decline is the largest one-day drop in US

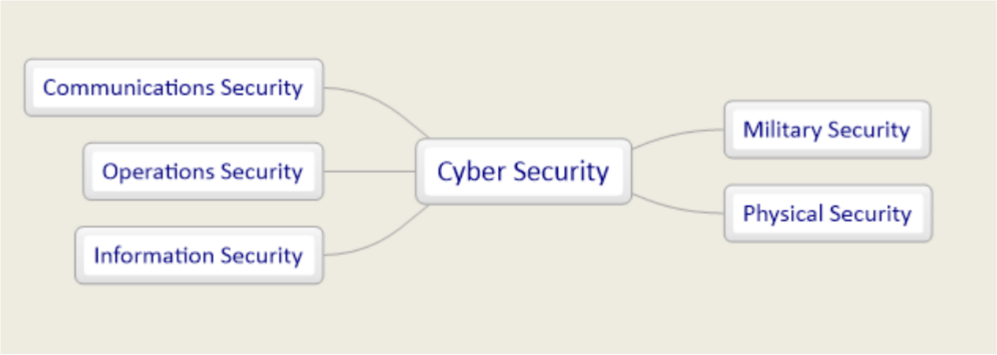


Source:Thomson Reuters Eikon.

Figure 3.1 shows the stock market prices for Facebook in 2018-2019. As can be seen, Facebook's stock experimented a huge drop, roughly 20%, on July 26th 2018. This fact, represented loses of $120 billion in market capitalization. Among the main reasons for this: i) Cambridge Analytica scandal on March 2018. The company did not prevent the filtering of 50 million user data to Cambridge Analytica and, what is even worse, there are suspicions of influencing in electoral processes. ii) Europe's new privacy laws: the General Data Protection Regulation (GDPR) (introduced in Chapter 1) cost the company 1 million users after it rolled out. And iii) The emergence of "fake news" problems through informational dominance. Mark Zuckerberg, CEO of Facebook, announced after users disenchantment: "(...) We will continue **to invest heavily in security and privacy** because we have a responsibility to keep people safe". Security has become a must.

The crux of the matter is: what is *security* in digital markets? In general, the term used to refer to this concept is Cybersecurity and contrary to what one might think, there is an added difficulty when it comes to finding a definition due to the large number of issues that cybersecurity covers. According to ENISA (2015), the European Union Agency for Network and Information Security, “Cybersecurity shall refer to security of cyberspace, where cyberspace itself refers to the set of links and relationships between objects that are accessible through to generalized telecommunications networks, and to the set of objects themselves where they present interfaces allowing their remote control, remote access to data, or their participation in control actions within that Cyberspace”.[3] Figure 3.2 illustrates the different domains within the term Cybersecurity according to the ENISA report.

Fig. 3.2 Different domains within the term “Cybersecurity”



Source: ENISA. December 2015.

Communications Security is referred to the protection against a threat to the technical infraestructure of a cyber system; Operations security is the protection against the intended corruption of procedures or workflows; Information Security is the protection against the threat of theft, deletion or alteration of stored data. The last two domains, which may seem the strangest ones are related to the protection against physical threats (Physical Security) and the protection against a threat whose origin is from within cyberspace which will have a political, military or strategic gain for the attacker (Public/National Security). We do not

[3] ENISA (2015) Definition of Cyber Security | Gaps and overlaps in standardisation. European Union Agency For Network And Information Security, Vol. v1.0.

differentiate in our work among any specific type of security investment but such investments can cover a wide range of aspects.

Finding a common understanding of cybersecurity is a major challenge and it might not be possible to harmonize the definition and usage of the term. Above all, it is a challenge because there is an overlapping of areas that is even more relevant when it is intended to regulate in an international context and for each type of industry. In this sense, and as ENISA empathizes, "Industry regulations do not cover Cybersecurity directly, but through rules on technical and ethical compliance and code of conduct of business." In fact, a way of indirect regulation of cybersecurity is through measures that ensure consumer privacy.

Privacy is one of the core European basic rights, and so is Cybersecurity.

Cybersecurity is a fundamental aspect to guarantee the future in digital environments and, studies estimate that the Internet economy annually generates between 2 trillion and 3 trillion, a share of the global economy that is expected to grow rapidly, according to the report of Inter Security (2014).[4] Proof of this is that the European Union addresses cybersecurity failures in systems and organizations as a key topic in the Horizon 2020 Project and it plays an important role in the construction of the Digital Single Market.[5] Moreover, privacy is one of the core European basic rights and it is evident that this aspect seems to have been left-out in the technical standards. In this direction the ISO (International Organization for Standardization) has conveyed a committee of privacy experts to develop the first set of international guidelines to ensure consumer privacy is embedded in the design of consumer products and services. The new committee (ISO/PC 317, Consumer protection: privacy by design for consumer goods and services) will develop guidelines that are intended to both enforce compliance with regulations and generate consumer trust.[6] The ISO Copolco's

[4] Intel Security. (2014). Net Losses: Estimating the Global Cost of Cybercrime. McAfee

[5] Find out more about key topics in https://ec.europa.eu/programmes/horizon2020/

[6] To keep updated with the project, visit https://www.iso.org/committee/6935430.html

report (ISO's Committee on Consumer Policy) has identified 70 consumer privacy needs (where), among them: network and system security, consumer digital security, consumer security information and the right to be forgotten or privacy by default.[7] Thus, this gives us as a conclusion, that these fields are interconnected by way of overlapping areas; i.e., there are areas of security standards with relevance to privacy and vice versa. Greater security in digital markets generates greater confidence and less privacy concerns of consumers.

We contribute to the literature on security in such markets by analyzing the investment decisions of a two-period monopoly market in which consumers have privacy concerns. The value of privacy is unknown by all market participants in the first period and may affect their willingness to pay for the product. The monopolist receives a noise signal about consumers' average privacy. This signal enables the monopolist to adjust the price in the second period. The monopolist's price in this second period acts as a signal to consumers about their privacy. This signal, together with consumers' purchase experiences from the first period, determines demand. Our setting is novel in that it considers the implications of firms' investment in security. As far as we know, no study has considered security investment as a way for firms to increase profits when consumers have privacy concerns. We fill this gap in the literature. We address two scenarios: direct investment in security to improve consumers' experiences and investment in market signal precision.

Through direct investment, the firm shows that it cares about each consumer's individual experiences and thereby seeks to maximize consumers' maximum willingness to pay. The incentives to invest are huge; in words of McAfee's report "the most important cost of cybercrime comes from its damage to company performance and to national economies. Cybercrime damages trade, competitiveness, innovation, and global economic growth."

[7] More information in https://www.iso.org/copolco.html

We analyze also the possibility of investment in market signal precision through, e.g., Big data analisys. Today, no investment in Big Data represents a huge opportunity cost for companies,since the collection of large amounts of data and the search for trends within the data allow companies to move much more quickly, smoothly and efficiently. Furthermore, bis data includes packages, as for example, big data security of Sisense, which include all the measures and tools used to guard both the data and analytics processes from attacks, theft or, other malicious activities that could harm them.[8] Through investment in market signal precision, the firm tries to manipulate consumers' information and increase market demand. This is important because of the power that goes with it. In this line, it is striking how it is possible to achieve objectives such as Cambridge Analytica's to change the opinion of people about Trump and influence it not through persuasion but through informational dominance.[9] From a general point of view and in words of Danah Boyd, president and founder of Data & Society, "[...] Media manipulators have figured out how to trick you into telling their story. Accept this and outsmart them."[10]

3.2 Literature review

Issues with privacy and economics are nothing new. For a complete review of this field, see Acquisti et al. (2016). Theoretical research has analyzed price competition (Taylor and Wagman 2014; Montes et al. 2018), price for information (Villas-Boas 2004; Chen and Zhang 2009), and exchange of consumer information (Taylor 2004b; Calzolari and Pavan 2006).

Chellappa and Pavlou (2002) empirically linked trust to perceived information security as an intuitive perception for assessing consumer's risk. In fact, consumers' attitudes toward

[8] More info in https://www.sisense.com/

[9] https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

[10] https://points.datasociety.net/media-manipulation-strategic-amplification-and-responsible-journalism-95f4d611f462

online purchasing seem to depend heavily on privacy and security concerns, and consumers' trust decreases when these concerns increase (McCole et al. 2010). Cases et al. (2010) described the indirect process whereby privacy concerns influence attitudes toward email campaigns. Our model captures the idea of consumers' trust via market signals (prices) and consumers' experiences to analytically quantify perceived privacy concerns.

Studies have investigated privacy concerns and regulation as potentially costly factors that depend on consumers. Acquisti and Varian (2005) and Conitzer et al. (2012) studied models in which consumers accessed anonymizing technologies, showing that welfare can be non-monotonic in degree of privacy. Investment in information security has become a significant organizational asset for companies in recent years. Some research on investment in security has focused primarily on cost savings associated with preventing cybersecurity breaches (Anderson 2001; Gordon and Loeb 2006; Angst et al. 2017). In this scenario, organizations must decide which information technology (IT) security measures to invest in (e.g.,Fenz et al. 2011) and how to evaluate those investment decisions (Anderson et al. 2008). Gordon and Loeb (2002) present a model that determines the optimal amount to invest to protect a given information set. In this study, we determine the optimal level of investment, but we also consider the effects of this investment on consumers' beliefs and demand.

From a point of view of game theory, Cavusoglu et al. (2008) compare decision-theoretic and game-theoretic approaches to IT security investment, focusing on a firm and a hacker. One of the results they find exposes that if the firm learn from prior observations of hacker effort and uses these to estimate the furute hacker effort, then the gap between results when decision theory is used and those when they play a simultaneous game approach disminishes over time. Kunreuther and Heal (2003) consider game theory for interdependent security in order to study how the expectation that others will not adopt protective measures reduces the incentive that a particular agent has to incur those costs. They also assume that all the decision-makers are identical and have the same security's costs. Varian (2004) also utilized game theory to study interdependence among security firms' risks. For a survey of game theory, as applied to network security and privacy, we refer the reader to Manshaei et al. (2013).Nagurney and Nagurney (2015) apply game theory with incomplete and imperfect information in the emerging field in network security and privacy, where prices depend on the quantities provided by the sellers of the product as well as the average security level for the marketplace. Few studies have provided empirical insight into how organizations make decisions regarding IT security investment. Recent studies have identified the main components of the information security investment decision-making process (e.g., Dor and Elovici 2016; or Weishäupl et al. 2018).

As far as we know, no study has considered security investment as a way for firms to increase profits when consumers have privacy concerns. We fill this gap in the literature.

The Chapter is organized as follows. The model is presented in Section 3.3. Section 3.3.1 specifies the uptading of beliefs. The price equilibrium and the general model is analyzed in section 3.3.2 Section 3.3.3 describes the firm's investment in security in our model. Section 3.4 and 3.4.1 analyze the firm's investment in the market precision of the signal. Section 3.5 provides some policy remarks and conclusions.

3.3 Theoretical framework: The baseline model

Our model is a two-period signaling game in which a monopolist and a continuum of consumers, who buy in an on-line market, use market signals to learn about consumers' privacy concerns. We apply the classical signaling game framework to analyze the information content of prices and the market performance under imperfect information and privacy concerns. Although the main features of the model have been set in Chapter 1, we include them here in order to produce a self-contained Chapter.

All the consumers know their willingness to pay for the product represented by θ_i. It is a way of expressing that the product is not new and that consumers are familiar with its quality and/or characteristics. We assume that individual i purchasing for the first time has some privacy concern but does not know the precise value of these concerns, represented by α_{it}, at the time of the purchase. Consumer $i's$ demand is given by

$$E\left\{\theta_i - \alpha_{it} - p_t | \Omega_{it}\right\}, \tag{3.1}$$

where Ω_{it} is consumer i's information for period t. The privacy concerns of individual i who decides to purchase a product in period $(t = 1, 2)$ is represented by an index α_{it}, which is equal to

$$\alpha_{it} = \tilde{x} + \widetilde{\omega}_i + \widetilde{v_{it}}. \tag{3.2}$$

Random variables $\tilde{x}$, $\widetilde{\omega}_i$ and $\widetilde{v_{it}}$ represent the population-average privacy in that specific product market, the individual i's persistent deviation from that population-average privacy, and individual $i's$ specific time deviation, respectively. The random variables have the following distributions $\tilde{x} \sim N\left(\bar{x}, \sigma_x^2\right)$, $\widetilde{\omega}_i \sim N\left(0, \sigma_\omega^2\right)$ and $\widetilde{v_{it}} \sim N\left(0, \sigma_v^2\right)$. Therefore, $E\left\{\tilde{\omega}\right\} = E\left\{\tilde{v_{it}}\right\} = 0$. Thus, we also assume that all of them are normally and independently distributed. Normality has the inconvenient feature of an unbounded support, which allows for negative demand and prices. However, normality also has the highly desirable feature of implying the use of linear Bayesian updating rules by consumers, which simplifies our analysis considerably.

Variable $\tilde{x}$ refers to average privacy concerns in that specific market. With the vast amount of news about the sale of personal data collected on the Internet, what are society's general concerns regarding personal information? With this random variable, we capture the idea that privacy has long been a moving target and that it continues to be so.

Variable $\tilde{\omega}_i$ captures differences between consumers. Some consumers do not care about privacy, whereas others consider privacy vital. If such a consumer realizes that some private information has been used in a harmful way, this will increase the value of α_{it}, in turn reducing consumer's utility. Variable $\tilde{v_{it}}$ is an external shock, which avoids complete learning by any market agent.

The firm receives a private signal about consumers' privacy concerns after period 1 given the amount of data disclosed and/or the cookies that have been eliminated. Specifically,

$$z = \tilde{x} + \tilde{\varphi}, \tag{3.3}$$

where $\tilde{x}$ represents the same random variable showing, as above, the average privacy in the market and where $\tilde{\varphi}$ is an external shock that is distributed normally $\tilde{\varphi} \sim N\left(0, \sigma_{\varphi}^2\right)$.

Signal z represents important information for the monopolist's second period choice. This signal is observed after first-period sales. With this particular definition of z, we can now give a more complete interpretation of $\tilde{x}$ and the random variable $\tilde{\varphi}$. Here, $\tilde{x}$ is the portion of the mean effect on the population that is detectable through z. Therefore, if $\tilde{x}$ is independent and not correlated with $\tilde{\varphi}$, then z will signal the actual population-average privacy concerns. If $\tilde{\varphi}$ were correlated, then $\tilde{x}$ would be the ex-ante expectation rather than the average privacy concerns about using this specific channel. We also assume that the unit production cost in each period is common knowledge and is normalized to zero.

The timing of the game is as follows. The market for the product opens in period one. The monopolist decides on a price strategy and announces the first-period price. In this first period, no information is generated by any player. The monopolist has no private information, and consumers do not learn either. Therefore, the information set Ω_{i1} consists of simple expectations: the monopolist has an expected demand and the consumers have an expected privacy concern. Consumer *i* observes the market price and decides how much of the product to purchase given her or his privacy concern expectations. Note that at the beginning of the first period, consumers are uncertain about their privacy concerns, and they need some experience to update their information. Because it is common knowledge that the monopolist will receive a private signal about the mean privacy at the end of period 1, the consumers and the monopolist receive some new information at the beginning of period 2.

In period 2, the information set is Ω_{i2}. The firm learns both $z = \tilde{x} + \tilde{\varphi}$ (i.e., the private signal about the average privacy concerns) and the first-period purchases. Both constitute the monopolist's information set in period $t = 2$. The monopolist then sets and announces its period 2 price. Consumers learn about their real privacy concerns from their purchases in the first period and from the second-period price. They are able to make an inference on z from the market price. Finally, they make a decision. The consumers' information set consist of consumers' purchase experiences, α_{i1}, and the inference made on z once the second-period price has been announced.

The above two-period game with imperfect information is a dynamic bayesian game. In addition, given that consumers signal their (probabilistic) knowledge about their privacy concerns through their demands, and the monopolist signals her information on consumers' privacy concerns through the second period price, the imperfect information dynamic game is a noisy signaling game. Therefore, the corresponding equilibrium concept (Perfect Bayesian

Equilibrium) specifies to that of a Noisy Signaling Equilibrium (NSE). The Noisy Signaling Equilibrium prescribes equilibrium strategies for the firm and the consumers which are sequentially rational to the other players' equilibrium strategies at each of their information sets (their beliefs about the consumers' privacy concerns), and beliefs wich are consistent with the equilibrium strategies, that is, they come from Bayesian updating.

3.3.1 Updating of beliefs

Given the above information, we first calculate several Bayesian updaties for future references. Because all random variables are normally distributed, the Bayesian updates are just regression equations. First, we have the consumer's updated random variable α_{i1} once z has been observed. By normality and the parameters of the corresponding distributions (see Chapter 1),

$$E\{\alpha_{i1}|z\} = \gamma_z z + \gamma_x \bar{x}, \tag{3.4}$$

where

$$\gamma_z = \frac{\sigma_x^2}{\sigma_z^2}, \gamma_x = 1 - \gamma_z = \frac{\sigma_z^2 - \sigma_x}{\sigma_z^2}. \tag{3.5}$$

Here, γ_z is the relative precision of signal z, and γ_x is the relative precision of the prior distribution of α_{i1}. The Bayesian updating of privacy concerns in period 2, conditional on z and α_{i1}, is given by

$$E\{\alpha_{i2}|\alpha_{i1}, z\} = \bar{x}\delta_x + \alpha_{i1}\delta_\alpha + z\delta_z, \tag{3.6}$$

where

$$\delta_\alpha = \frac{\sigma_x^2\sigma_\varphi^2 + \sigma_\omega^2\sigma_z^2}{\sigma_\alpha^2\sigma_z^2 - \sigma_x^4},$$

$$\delta_z = \frac{\sigma_x^2\sigma_v^2}{\sigma_\alpha^2\sigma_z^2 - \sigma_x^4},$$

and

$$\delta_x = 1 - \delta_\alpha - \delta_z.$$

In these equations, $\sigma_{\alpha}^{2}=\sigma_{x}^{2}+\sigma_{\omega}^{2}+\sigma_{\vartheta}^{2}$ and $\sigma_{z}^{2}=\sigma_{x}^{2}+\sigma_{\varphi}^{2}$. Therefore, we can rewrite as

$$\delta_{z}=\gamma_{z}\left(1-\delta_{\alpha}\right), \tag{3.7}$$

$$\delta_{x}=\left(1-\gamma_{z}\right)\left(1-\delta_{\alpha}\right). \tag{3.8}$$

Note that in period 2, the consumers' posterior distribution of α_{i2} comes from the information obtained through the purchase in period 1 and the updating of α_{i1}. In other words, it comes from consumers' experiences in period 1 and the inference made on z from the second-period price. Here, δ_{α} is the relative precision of the experience in period 1, γ_{z} is the relative precision of the signal in period 2, and γ_{x} is the relative precision of the prior distribution of α_{i2}. Equations (3.7) and (3.8) show that beliefs depend on two key parameters: δ_{α} and γ_{z}. Parameter δ_{α} measures how much weight consumers place on their privacy concerns regarding their purchase experiences. Parameter γ_{z} is the precision of the monopolist's private information (i.e., the signal precision of z).

3.3.2 Equilibrium analysis under privacy concerns

In this section, we analyze how the monopolist sets prices in periods $t=1,2$ given the information Ω_{t} that is available in each period. Thus, the monopolist's information set is specified by Ω_{mt} where m indicates the set of information for the monopolist available in each perios t. On the other hand, representative consumer i has an expected privacy concern in each period t, and his set of information is given by Ω_{it}.

In period 1, consumers have expected demands given their set of information in period $t=1$. As specified above, no information has yet been given to either monopolist or the consumers. Thus, consumers' expected demands and the monopolist's expected profits are, respectively:

$$E\left[q_{i1}|\Omega_{i1}\left(\alpha_{i1}\right)\right]=\theta_i-\bar{x}-p_1,$$

$$E\left[\Pi_1|\Omega_{m1}\left(\alpha_1\right)\right]=\left(\theta_i-\bar{x}-p_1\right)p_1. \tag{3.9}$$

Now consider the equilibrium in period 2. In this equilibrium, the monopolist's second-period price is a linear function of the monopolist's private information. The first step when computing the perfect Bayesian equilibrium is to specify exactly what consumer i believes when he or she decides to purchase the product for any possible information set, Ω_{i2}. A consumer's information set at the beginning of period 2 consists of the consumer's own experience regarding α_{it} plus the commonly observed p_2, which might indicate the monopolist's observation of z. Suppose consumers make inferences on z from p_2 following Bayes according to the linear rule $z=a+bp_2$.

The expected demand in period 2 of consumer i is,

$$E\left[q_{i2}|\Omega_{i2}\left(\alpha_{i1},p_2\right)\right]=\theta_i-E\left\{E\left\{\alpha_{i2}|\alpha_{i1},z\right\}|\alpha_{i1},p_2\right\}-p_{2,}$$

which specifies to,

$$E\left[q_{i2}|\Omega_{i2}\left(\alpha_{i1},p_2\right)\right]=\theta_i-E\left\{\bar{x}\delta_x+\alpha_{i1}\delta_\alpha+z\delta_z|\alpha_{i1},p_2\right\}-p_2,$$

and therefore,

$$E\left[q_{i2}|\Omega_{i2}\left(\alpha_{i1},p_2\right)\right]=\theta_i-\left\{\bar{x}\delta_x+\alpha_{i1}\delta_\alpha+\left(a+bp_2\right)\delta_z\right\}-p_2.$$

After period 1, the monopolist gets some information about average privacy. The monopolist uses this information to set the second-period price. Therefore, the monopolist's second-period expected demand is

$$E\left[q_2|\Omega_{m2}\left(\alpha_{i2},z\right)\right]=\left(\theta_i-E\left\{\bar{x}\delta_x+\alpha_{i1}\delta_\alpha+z\delta_z|z\right\}-p_2\right),$$

Using the expectations already discussed and (8), the expected demand curve faced by the monopolist is

$$E\left[q_2|\Omega_{m2}\left(\alpha_{i2},z\right)\right]=\left(\theta_i-\left(\bar{x}\gamma_x+\delta_z\left(a+bp_2\right)+z\delta_\alpha\gamma_z\right)-p_2\right).$$

Thus, the monopolist's second-period expected profits are,

$$E\left[\Pi_2|\Omega_{m2}\left(\alpha_{i2},z\right)\right]=\left(\left(\theta_i-\left(\bar{x}\gamma_x+\delta_z\left(a+bp_2\right)+z\delta_\alpha\gamma_z\right)-p_2\right)\right)p_2. \tag{3.10}$$

As already mentioned, the equilibrium concept is a perfect Bayesian equilibrium, which specifies here as a *noisy signaling equilibrium*, and consists of the monopolist's price in each period given the information set Ω_t in periods $t=1,2$, the consumers' expected demand from the consumers' utility maximization given the information set Ω_{it} in periods $t=1,2$, and the posterior beliefs of both the consumers and the monopolist. In equilibrium, the posterior beliefs are consistent with Bayes' rule and equilibrium prices. In particular, we wish to study Noisy Signaling Equilibria with linear optimal rules. Given that all of our random variables are normally distributed, all the Bayesian updates are linear inference rules (linear regressions). Therefore, at the equilibrium, the firm's second-period price is a linear function of its private information. This specification is necessary in order the consumers of the on-line channel may update their beliefs and appropriately maximise their utility.

The following proposition characterizes the noisy signaling equilibrium.

Proposition 8 *There exists a noisy signaling equilibrium. In equilibrium,*

1. *The firm sets the price in period $t = 1$*

$$p_1^* = \frac{\theta_i - \bar{x}}{2}.$$

2. *Since the ex-ante expected price in the second period is*

$$p_2^* = \frac{\theta_i - z\delta_\alpha\gamma_z - a\delta_z - \bar{x}\gamma_x}{2\,(1 + b\delta_z)}, \tag{3.11}$$

and in a linear equilibrium

$$a = \frac{\theta_i - \bar{x}\gamma_x}{\gamma_z}, \tag{3.12}$$

and

$$b = \frac{2}{(\delta_\alpha - 2)\,\gamma_z}, \tag{3.13}$$

then, the second period expected price is,

$$p_2^* = \frac{1}{2}\,(2 - \delta_\alpha)\,(\theta_i - \bar{x}\gamma_x - z\gamma_z)\,, \tag{3.14}$$

Proof. *See the Appendix.* ■

The second period monopoly profits are,

$$\Pi_2 = \frac{1}{4}\,(2 - \delta_\alpha)\,\delta_\alpha(\theta_i - \bar{x}\gamma_x - z\gamma_z)^2. \tag{3.15}$$

Proposition 9 *If γ_z is fixed and common knowledge, then equilibirum prices will be given by p_1^* and p_2^* as specified above. Furthermore, this is the unique equilibrium where consumers' inferences about z are a differentiable and invertible function of p_2^*.*

Proof. See the Appendix. ■

Note that the second period price is indeed a linear function of signal z. As indicated above, the key parameters of the model are δ_α and γ_z. Some remarks should be made here. First, signaling distorts price upward on average. Second, the price in period 2 increases as long as the precision of the signal increases too. Thus, the derivative with respect the precision of the signal z is positive: $\frac{\partial P_2^*}{\partial \gamma_z} > 0$. However, the opposite occurs when consumers' privacy experiences, δ_α, are considered. When consumers attach greater importance to their experiences, the price in period 2 is lower: $\frac{\partial P_2^*}{\partial \delta_\alpha} < 0$.

These remarks highlight two lines of action for the monopolist to increase profits. One option is for the monopolist to try to manipulate consumers' experiences in period 1. We address this option in the next section through investment in security in period 1. Alternatively, the monopolist could use market signal precision to manipulate consumers' beliefs. We address this possibility in Section 3.4.

3.4 Privacy and security

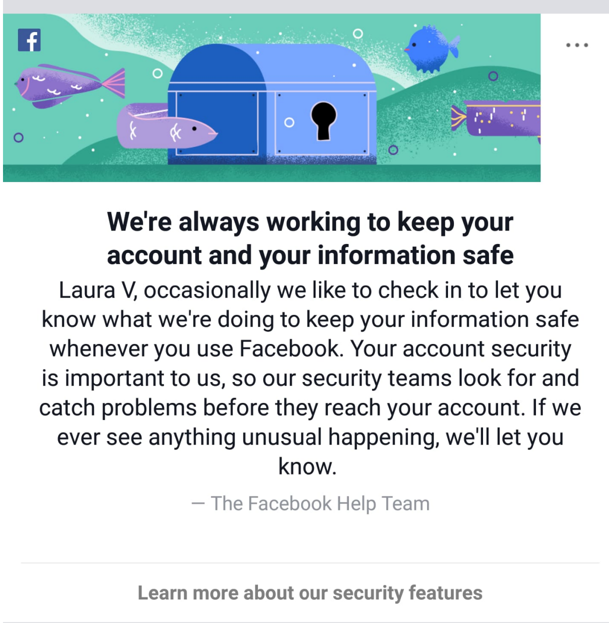
Many real-world examples show that security and privacy in the digital market are unresolved issues. Until recently, consumers paid for online security in the form of software and antivirus packages. These packages guaranteed them protection against viruses and other digital intrusions. Nowadays, privacy has become the responsibility of firms, which seek security in digital markets. Newspapers have reported the vulnerability, data hacking, and data theft of consumer information. The onus in terms of who must pay for security investment has shifted noticeably from consumers to firms in recent years.

Companies are aware that guaranteeing security, privacy, and trust is the key to success in digital markets. Firms like Apple and Facebook constantly publicize their efforts and commitment in this area.[11],[12] Signaling this commitment has become a basic requirement.

[11] https://www.apple.com/apples-commitment-to-customer-privacy/

[12] This is an example of how Facebook reminds users of (i.e., sends signals) of its commitment to security. See Figure 3.3

Fig. 3.3 Facebook's notification in a profile signaling the company's effort in security



We're always working to keep your account and your information safe

Laura V, occasionally we like to check in to let you know what we're doing to keep your information safe whenever you use Facebook. Your account security is important to us, so our security teams look for and catch problems before they reach your account. If we ever see anything unusual happening, we'll let you know.

— The Facebook Help Team

Learn more about our security features

3.4.1 Private investment

The following set-up presents a simple model of security investment by a monopolist. The monopolist may invest in privacy measures in the first period. The effect of this investment is reflected by consumer $i's$ computation of expected privacy concerns in period 1 (α_{i1}), represented by the parameter s_1. This parameter affects the first-period utility of consumers' expectated privacy concerns. However, while it does not directly affect consumer $i's$ utility in the second period, it does affect second-period demand due to the inference by consumers. As in the baseline model, α_{it} is given by

$$\alpha_{i1} = \tilde{x} + \omega_i + v_{1t} - s_1,$$

where s_1 diminishes consumers' overall privacy concerns because of investment in security to protect consumers' personal data. The cost of that investment is $c\frac{s_1^2}{2}$, where $c > 0$. In this section, we assume that γ_z is fixed and is common knowledge. In other words, market signal precision is known by all the participants in the market.

The next step in our analysis is to adjust the period 2 expectations formulae to reflect the consumers' beliefs about privacy once the security investment s_1^e has been made. They become

$$E\left\{\alpha_{i1}|z\right\} = \gamma_z z + \gamma_x \bar{x} - s_1^e,$$

and

$$E\left\{\alpha_{i2}|\alpha_{i1},z\right\} = \bar{x}\delta_x + \left(\alpha_{i1} + s_1^e\right)\delta_\alpha + z\delta_z. \tag{3.16}$$

Therefore, the new expected demand faced by the monopolist in period 2 is

$$E\left[q_2^s|\Omega_{m2}\left(\alpha_{i2},z\right)\right] = \theta_i - \left(\delta_\alpha\left(s_1^e - s_1\right) + z\delta_a\gamma_z + \delta_z(a+bp_2) + \bar{x}\gamma_x\right) - p_2,$$

and the monopolist's expected profits in period 2 are

$$E\left[\Pi_2^s|\Omega_{m2}\left(\alpha_{i2},z\right)\right] = \left(\theta_i - \left(\delta_\alpha\left(s_1^e - s_1\right) + z\delta_a\gamma_z + \delta_z(a+bp_2) + \bar{x}\gamma_x\right) - p_2\right)p_2. \tag{3.17}$$

Equilibrium

With the new expectation formulae, the equilibrium when there is investment in security consists of the monopolist's price strategies in period $t = 1,2$, $p_1^{s*}\left(E\left\{\alpha_{i1}\right\}\right)$ and $p_2^{s*}\left(E\left\{\alpha_{i2}|\alpha_{i1},p_2^s\right\},E\left\{\alpha_{i2}|\alpha_{i1},z\right\}\right)$, the optimal level of investment s_1, and the Bayesian beliefs, which take the following linear form $z = a + bp_2^s$.

Proposition 10 *There exists a noisy signaling equilibrium. In equilibrium,*

1. *The firm sets the price in period $t = 1$*

$$p_1^{s*} = \frac{1}{2}\left(\theta_i - \left(\bar{x} - s_1\right)\right).$$

2. *Since the second period ex-ante expected price is*

$$p_2^{s*} = \frac{\theta_i - z\delta_\alpha\gamma_z - a\delta_z - \bar{x}\gamma_x}{2\left(1 + b\delta_z\right)}, \tag{3.18}$$

and in a linear equilibrium

$$a = \frac{\theta_i - \bar{x}\gamma_x}{\gamma_z}, \tag{3.19}$$

and

$$b = \frac{2}{\left(\delta_\alpha - 2\right)\gamma_z}, \tag{3.20}$$

then the second period expected price and expected profits are, respectively,

$$p_2^{s*} = \frac{1}{2}\left(2 - \delta_a\right)\left(\theta_i - \bar{x}\gamma_x - z\gamma_z\right), \tag{3.21}$$

$$\Pi_2^{s*} = \frac{1}{4}\left(2 - \delta_\alpha\right)\delta_\alpha\left(\theta_i - \bar{x}\gamma_x - z\gamma_z\right)^2. \tag{3.22}$$

3. *Using the expressions for a and b, the effect of the investment on consumers' beliefs about the general security in period 2 (δ_α), and the cost of privacy to the monopolist yields the following first-order condition for s_1, taking expectations over z:*

$$s_1^* = \frac{\left(2 - \delta_\alpha\right)\delta_\alpha\left(\theta_i - \bar{x}\right)}{2c}. \tag{3.23}$$

Proof. See Appendix. ■

At the equilibrium, beliefs are correct (i.e., $s_1 = s_1^e$), so it is optimal for the monopolist to invest the amount s_1^*, specified in (3.25), for a cost c. The optimal level of investment in period 1, s_1^*, is a decreasing function of cost.

The main findings of the model are the following:

1. The optimal level of investment increases with the consumers' experience, δ_α.

2. The expected price in period 1 is the only price affected by the firm's investment in period 1. It does not affect the expected price in period 2. Moreover, the expected price in the first period with investment in security is higher than the expected price without investment (see Section 4). Thus, $p_1^s > p_1$. The firm transfers the cost of security investment to consumers through price.

The interesting feature of this solution is that even though the security investment does not affect the consumer's second-period utility, the firm still makes the investment. This is because the marginal first-period investment affects each consumer's inference about the individual specific valuation, δ_α, which increases confidence and therefore second-period demand.

To illustrate our results, we provide a numerical example. It is not feasible to find real budgetary data on IT security investment, so we make some assumptions. We assume that the willingness to pay for a product is known to be 5 monetary units. We take the average privacy concern in the market $\bar{x} = 0.84$, from the estimated privacy parameter in Eastlick et al. (2006). Similarly, the realization of the firm's signal observation, z, is taken to be 0.60. Finally, we assign different values to the key parameters of the model δ_α (consumers' experiences) and γ_z (relative precision of signal z).

Table 3.1 A numerical example

	$\delta_\alpha = \gamma_z = 0.5$	$\delta_\alpha = 0.9; \gamma_z = 0.1$	$\delta_\alpha = 0.1; \gamma_z = 0.9$	$\delta_\alpha = 0.9; \gamma_z = 0.9$	$\delta_\alpha = 0.1; \gamma_z = 0.1$
Period 1					
p_1	2.08	2.08	2.08	2.08	2.08
CS_1	2.08	2.08	2.08	2.08	2.08
Π_1	4.33	4.33	4.33	4.33	4.33
Period 2					
p_2	3.21	2.30	4.16	2.41	3.97
CS_2	1.07	1.88	0.22	1.97	0.21
Π_2	3.43	4.33	0.91	4.74	0.83
Period 1(Security investment)					
p_1^s	3.44	3.55	2.75	3.56	2.75
CS_1^s	0.72	0.60	1.41	0.60	1.41
s_1^*	2.71	2.96	1.34	2.96	1.34
Π_1^s	9.97	10.49	7.11	10.49	7.11
$CS_T^{NI} = CS_1 + CS_2$	3.15	3.96	2.30	4.05	2.29
$CS_T^I = CS_1^s + CS_2$	1.79	2.48	1.63	2.57	1.62
$\Pi_T = \Pi_1 + \Pi_2$	7.76	8.66	5.24	9.07	5.16
$\Pi_T^s = \Pi_1^s + \Pi_2$	13.40	14.82	8.02	15.23	7.94
SW^{NI}	10.91	12.62	7.53	13.12	7.45
SW^I	15.20	17.30	9.65	17.80	9.56
$\%\triangle SW$	39.3%	37.1%	28.1%	35.7%	28.4%
$\%\frac{s_1}{\Pi_T^s}$	20.2%	20.0%	16.7%	19.5%	16.9%

$\theta_i = 5; \bar{x} = 0.84; z = 0.60$

Table 1 first presents the scenario in which there is no investment in security, where CS_1 and CS_2, and Π_1 and Π_2, are the consumer surplus and the firm's profits in periods 1 and 2, respectively. Second, Table 1 presents the scenario in which there is investment in security in period 1. Finally, CS_T^{NI}, CS_T^{I}, SW_T^{NI} and SW_T^{I} show the sum of period 1 and period 2 consumer's surplus and social welfare with no investment in security (identified by superscript NI) and with investment in security (identified by the superscript I), respectively.

The following remarks derived from the data in Table 1 reinforce the model results:

1. The greater consumers' experience, δ_α, is, the higher the optimal investment in security s_1^* will be.

2. Prices in period 1 are higher with security investment than without investment. This results in higher profits for the firm in period 1 and lower consumer surplus. Nevertheless, social welfare is still higher than without security investment.

3. Interestingly, the percentage of security investment is 16%-20% of the sum of period 1 and period 2 profits. This may seem a sizeable investment, but it is by no means unrealistic. Indeed, according to Karpersky,[13] an international company that specializes in IT security, almost a quarter (23%) of IT budgets in large companies is spent on IT security, and this amount is expected to grow. Businesses are starting to view this investment as strategic. Our model shows the benefits of doing so.

3.4.2 Endogenous precision: information manipulation

In the previous section, we analyzed the level of investment that the monopolist must make to increase its expected profits. By achieving the optimal level of investment, the monopolist seeks to improve consumers' experiences in the first period by increasing consumers'

[13] Full text available on https://www.kaspersky.com/about/press-releases

confidence. Here, the approach is different. In this section, the monopolist sets a specific level of market signal precision, γ_z. The choice of signal precision allows the monopolist to manipulate the information received by consumers.

We now assume that the monopolist chooses the precision of its information (i.e., γ_z is endogenous). More specifically, we hold σ_x^2 constant and assume that the monopolist determines γ_z by an implicit choice of σ_φ^2, as equation (5) shows. The monopolist receives its private signal without any kind of noise. This could be the case if the firm conducted a prior market study or big data analysis. We determine the equilibrium level of γ_z under various specifications of the informational and regulatory environment. To focus on the optimal choice of γ_z, we assume that there is no period-one investment. For expositional clarity, we assume that γ_z is chosen at some initial time prior to the introduction of any specific good.

The cost of achieving precision γ_z is $c(\gamma_z)$. We assume that $c(\cdot)$ is increasing and convex such that $c(1) = c'(1) = \infty$ and $c(0) = c'(0) = 0$. Because $\gamma_z = 1$ corresponds to the situation in which the monopolist has perfect information about $\bar{x}$, it is natural to assume that the total and marginal cost of eliminating the last bit of uncertainty is infinite. Becuase $\gamma_z = 0$ corresponds to no information, it is reasonable to assume that the marginal cost of the first bit of information is zero. These assumptions yield interior solutions to the monopolist's choice of γ_z.

The monopolist's choice of precision is not observable by consumers. Therefore, consumers form some point expectation of γ_z, whose value will determine their point beliefs about the regression coefficients δ_α and δ_z. These coefficients generate consumers' predictions about the information quality of z. We denote consumers' (common) beliefs about the monopolist's information quality by γ_z^e. These beliefs translate into beliefs about the values of δ_α and δ_z, which we denote by δ_α^e and δ_z^e. They, in turn, determine the period-two coefficients, a and b, of the consumers' period 2 inference rule, $z = a + bp_2$.

Equilibrium

The firm's expectation of α_{it} is conditional on z and depends on the true value of γ_z. Given consumer beliefs about γ_z and the resulting inference parameters, the expected demand function perceived by the monopolist in period 2 is

$$E\left[q_2^e|\Omega_{m2}\left(\alpha_{i2},z\right)\right] = \theta_i - \left(\delta_\alpha^e\gamma_z z + \delta_z^e(a+bp_2^e) + \bar{x}\left(1-\delta_\alpha^e\gamma_z - \delta_z^e\right)\right) - p_2^e, \tag{3.24}$$

and given that the firm knows γ_z, then $E\left[\alpha_{i1}|z\right] = \gamma_z z + (1-\gamma_z)\bar{x}$.

Solving for the profit-maximizing price and substituting into the profit function, period 2 expected profit conditional on z is given by

$$\Pi_2^e = \frac{\left(\theta_i + \bar{x}\left(\gamma_z\delta_\alpha^e + \delta_z^e - 1\right) - a\delta_z^e - z\gamma_z\delta_\alpha^e\right)^2}{4\left(1+b\delta_\alpha^e\right)}. \tag{3.25}$$

Hence the firm chooses γ_z to maximize $E\left\{\Pi_2^e\right\} - c(\gamma_z)$, where the expectation is taken over z because γ_z is chosen ex ante.[14]

The first-order condition of the monopolist's problem is

$$c'\left(\gamma_z^e\right) = \frac{\gamma_z^e\sigma_z^2\left(\delta_\alpha^e\right)^2}{2\left(1+b\delta_z^e\right)}. \tag{3.26}$$

Note that $c'\left(\gamma_z^e\right)$ is positive and is indeed the marginal profit of the information precision. It is simple to show that the second-order condition is satisfied. The optimal level of γ_z is

$$\gamma_z^* = \frac{2c\left(\gamma_z\right)}{(2-\delta_\alpha^e)\delta_\alpha^e\sigma_z^2}. \tag{3.27}$$

[14] Note that z is squared in (3.25), so $E\left\{z^2\right\} = \bar{x}^2 + \sigma_z^2$.

The optimal value of the information precision is a negative function of consumers' experiences. In Bayes Nash equilibrium, consumers' beliefs are correct. This implies that $\gamma_z^e = \gamma_z$, $\delta_\alpha^e = \delta_\alpha$, and $\delta_z^e = \delta_z$, where γ_z^e denotes the equilibrium value of γ_z when the monopolist's choice of γ_z is unobservable. Thus,

Proposition 11 *At equilibrium, the optimal precision choice is*

$$\gamma_z^* = \frac{2c\left(\gamma_z\right)}{(2-\delta_\alpha)\delta_\alpha\sigma_z^2}. \tag{3.28}$$

Proof. See Appendix. ■

To interpret our results, we should note that (3.29) can be written as marginal revenues by equating marginal costs:

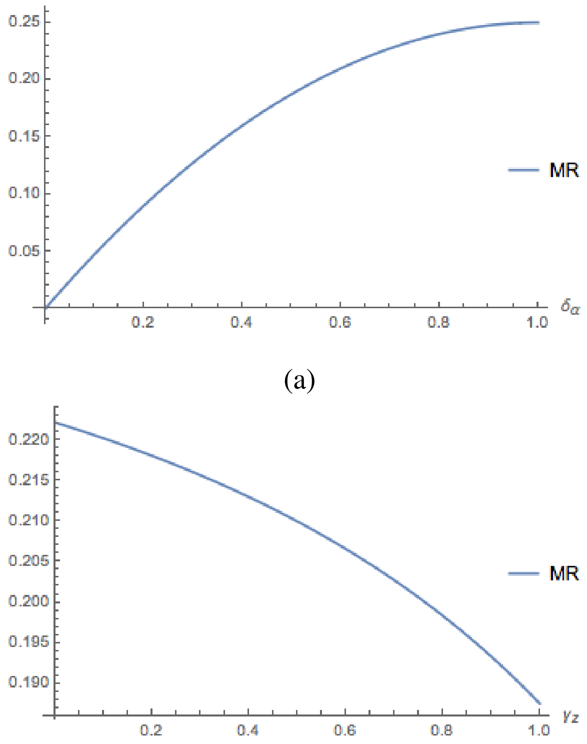
$$c'\left(\gamma_z\right) = \frac{1}{2}(2-\delta_\alpha)\delta_\alpha\sigma_x^2. \tag{3.29}$$

Figure 3.4 plots the monopolist's marginal revenues as a function of consumers' experiences (a) and as a function of the value of the signal's precision (b).

The monopolist finds it profitable to choose to invest in market signal precision because the monopolist's marginal revenue of doing so, given cost $c(\gamma_z)$, is positive.

To interpret our results, in equation (3.29), we let marginal costs equaling marginal revenues, clearing for c. Given the negative relationship between δ_α and γ_z, (see the proof of proposition 11 in the Appendix), the monopolist find it optimal to manipulate the consumers' belief about the monopolist's private signal. There are incentives to create in this market more confidence in the private signal (consumers' experience in the previous period) than in the public signal, (precision of the monopolist's signal), and therefore, the inference made from the market's price.

Given the potential marginal revenue of investing in the signal's precision, an incentive to manipulate arises. In particular, the monopolist wants to signal a specific value of precision to



(a)

(b)

Fig. 3.4 Marginal revenues depending on γ_z and δ_α

make consumers believe that precision is worse than it really is. By doing so, the monopolist increases consumers' trust in the online market, thereby increasing consumers' market demand.

As Figure 3.4 (a) shows, the monopolist's marginal revenue, and therefore her expected profits, increases with consumers' experience, δ_α. Moreover, as Figure 3.4 (b) shows, marginal revenue, and therefore her expected profits, decreases with the signal precision, γ_z.

These results also show an interesting trade-off between the level of expected price and expected demand in period 2. This trade-off is due to the negative relationship between the market signal, γ_z, and the parameter that measures the weight of experience, δ_α. Whereas expected price increases with the market signal, the effect is the opposite with respect to the expected demand. If the monopolist manipulates the market signal precision, consumers will pay more attention to their own experience and less to the market signal. This shift in attention increases expected demand, q_2^e, for the monopolist and results in a lower expected price, p_2^e, than when there is an absence of manipulation. The optimal choice is the one that increases the monopolist's expected profits, so the demand effect dominates the price effect. According to our results, the monopolist has an incentive to create less confidence in the market signal (the public signal) and more in the consumers' individual experiences (the private signal).

Manipulative behavior for specific cost functions

We assumed so far that the cost of achieving precision γ_z is $c(\gamma_z)$. And this cost function is increasing and convex such that $c(1) = c'(1) = \infty$ and $c(0) = c'(0) = 0$. The intuition for that specific costs function is that achieving perfect information about $\bar{x}$ and eliminate the last bit of uncertainty translates to an infinitine marginal costs. Because $\gamma_z = 0$ corresponds to the no information scenario, it is reasonable to assume that marginal cost of the first bit of information is zero. Thus, the signal's precision ranges from 0 to 1, $\gamma_z \in (0,1)$.

Our aim in this section is to consider specific cost function to give further intuitions. Specifically, we want to compare convex costs functions with linear costs functions, and their implications for the precision signal's investment.

Firstly, we adapt the convex costs of cybersecurity investments in Nagurney and Nagurney (2015).[15] To this end, define c^c as the convex cost of investment in the signal's precision. Particularly,

$$c^c = c\left(\frac{1}{\sqrt{(1-\gamma_z)}} - 1\right). \tag{3.30}$$

Moreover, let c^l be the case with linear cost of the signal's precision investment, so

$$c^l = c\gamma_z. \tag{3.31}$$

In both cost functions, $c > 0$, and have the same cost for the first bit of information and it is equal to zero, i.e. $c(\gamma_z = 0) = c^c = c^l = 0$. However, with linear cost the cost to have perfect information is finite and equals c.

Given these cost functions, the monopolist maximizes her expected profits in period 2, looking for the optimal level of precision investment. Let γ_z^{c*} be the optimal precision that solves the maximization problem of $E(\Pi_2^c) - c(\gamma_z^c)$,

$$\gamma_z^{c*} = \quad arg \quad \max_{\gamma_z^c} \frac{(\theta_i + a\delta_z^e - \delta_z^e\overline{x} + \overline{x})^2 + \delta_\alpha^e \gamma_z^2 \sigma_z^2}{4\left(1 + \delta_z^e b\right)} - c\left(\frac{1}{\sqrt{(1-\gamma_z)}} - 1\right). \tag{3.32}$$

Solving the maximization problem in (3.34), gives the following optimal precision

$$\gamma_z^{c*} = 1 - \frac{1}{\left(\frac{(2-\delta_\alpha)\delta_\alpha \sigma_x^2}{c}\right)^{2/3}}, \tag{3.33}$$

[15] Nagurney and Nagurney (2015) consider m competitive sellers of a homogeneous product and, n buyers. All participants in this online market are connected via a network security interchangeably with cybersecurity. They specified a cost function for each seller that depends on the probability of a succesful cyberattack on seller $i \in m$, and we adapt this setting where the cost function depend on the precision of the information.

which requires $c \leq (2-\delta_\alpha)\delta_\alpha\sigma_x^2$ in order that γ_z^{c*} is non-negative. Let us recall this threshold in the cost c_1. Note that the second order condition is satisfied. In the same way, let γ_z^{l*} the optimal precision for the maximization problem faced by the monopolist with linear costs,

$$\gamma_z^{l*} = \quad arg \quad \max_{\gamma_z^l} \frac{(\theta_i + a\delta_z^e - \delta_z^e\overline{x} + \overline{x})^2 + \delta_\alpha^e\gamma_z^2\sigma_z^2}{4\left(1+\delta_z^e b\right)} - c\gamma_z. \tag{3.34}$$

The maximization problem yields the following optimal precision investment, that is,

$$\gamma_z^{l*} = \frac{2c}{(2-\delta_\alpha)\delta_\alpha\sigma_z^2}, \tag{3.35}$$

which requires $c \leq \frac{1}{2}(2-\delta_\alpha)\delta_\alpha\sigma_z$. Let c_2 be this specific threshold. Here, again, the second order condition is also satisfied.

Different cost functions lead to distinct manipulative behaviour. The key fact of investment in the signal's precision is that we hold σ_x^2 constant and, we assume that the monopolist determines γ_z by an implicit choice of σ_φ^2. Recall that $\gamma_z = \frac{\sigma_x^2}{\sigma_z^2}$, where $\sigma_z^2 = \sigma_x^2 + \sigma_\varphi^2$. The choice of σ_φ^2 changes dramatically under different cost functions, and hence, the manipulative ability of the monopolist may be affected, and more restricted in some cases.

To clarify the key aspects, we wish to analyze the equilibrium choice of the optimal signal's precision. Particularly, our aim is to answer how the choice of σ_φ^2 is under different cost functions, and ultimately, analyze the effects on the manipulative capacity for the monopolist.

Cost of the signal's precision investment

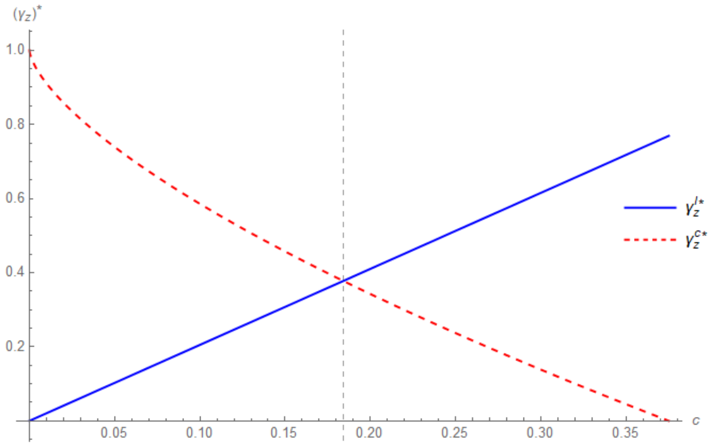
To answer the above query we study first the behaviour of the optimal precision investment as c changes. As noted before, we require that $c \leq c_1$ in order to have a non-negative optimal precision under a convex cost function, i.e., $\gamma_z \geq 0$. Furthermore, we also require that $c \leq c_2$ in order to have an optimal precision under linear cost smaller than/or equal to 1 i.e., $\gamma_z \leq 1$.

Thus, we study these optimal precisions as a function of c inside the interval, $c \in (0,(c_1,c_2))$. Comparing c_1 to c_2, we find out that the superior limit (c_1 or c_2) in the interval will depend on the choice of σ_φ^2. In particular, if $\sigma_\varphi^2 = 0$, then, $\sigma_z^2 = \sigma_x^2$. This fact implies that $c_2 < c_1$ and the requirement for γ_z^{c*} is met. On the other hand, if $\sigma_\varphi^2 > 0$, then $\sigma_z^2 > \sigma_x^2$, and $c_1 < c_2$, therefore, the resquirement is verified under linear cost functions, $\gamma_z^{l*} \leq 1$.

In this interval, the partial derivative of γ_z^{c*} with respect c is negative, i.e., $\frac{\partial \gamma_z^{c*}}{\partial c} < 0$. This means that an increase in the cost of acquiring increasingly more precision in the information about $\bar{x}$ leads to a lower levels of the optimal precision. However, the case is the reverse when the monopolist faces linear cost of investments. In fact, the bigger the cost of investments, the higher the level of the optimal precision that maximizes her profits, i.e., $\frac{\partial \gamma_z^{l*}}{\partial c} > 0$.

Figure 3.5 shows this behaviour for $c \in (0,c_1)$:

Fig. 3.5 Optimal signal's precision depending on c.



$\sigma_x^2 = 0.5$, $\sigma_\varphi^2 = 0.8$, $\delta_\alpha = 0.5$

Thus, there is a specific level of c, let call it c', that makes that the optimal signal's precision under both investment cost functions coincides. For values of c lower than c', we find that the optimal signal's precision is higher under convex cost function. On the contrary, there exist some c above c', for which the optimal signal's precision is higher than under linear costs.

Therefore, the manipulative capacity of the monopolist is affected by the type of cost function the monopolist has, and in particular, by the values of c. As noted above, the monopolist has incentives to signal lower levels of signal's precision in the market. It is easily seen that linear costs allows the monopolist to signal lower levels of precision with c small, which is not too much costly for her. However, signaling a lower signal's precision is more expensive under convex costs (it requires an amount of c), and hence, the monopolist could have limited her ability for manipulation.

3.5 Conclusions

Comparing the two investment approaches reveals several implications for consumers. First, the direct investment in security in period 1 results in a transfer of the cost directly to consumers through price. Second, investment in signal precision transfers the control of information in the market to the monopolist. This transfer influences both demand and expected prices. In this scenario, the monopolist obtains higher profits by increasing expected demand, which implies a lower price in period 2 (i.e., prices are lower than in the absence of investment in period $t = 2$). We therefore conclude that it would be preferable to grant the monopolist a certain power of information because doing so would result in lower prices. On the other hand, there are significant implications depending on which cost functions the monopolist faces. In particular, under linear cost function, the monopolist has greater incentives to manipulate the signal's precision, and it is possible to do so with c small (cheaper). However, if the monopolist faces convex cost functions, signaling lower signal's precision is more expensive, and therefore, manipulation is more costlier.

The European Union addresses cybersecurity failures in systems and organizations as a key topic in the Horizon 2020 Project. The construction of the Digital Single Market requires the necessary tools to fight cybercrime and consistently guarantee cybersecurity. Recently, the General Affairs Council (GAC) announced its commitment to tightening cybersecurity.

Incentivizing investment in cybersecurity is a precondition for the construction of the Digital Single Market.[16]

Subsidizing security costs to benefit from their economic effect on the market and consumers is still economically controversial. For example, in our model, the firm can take two directions in its investment efforts. Subsidizing the cost of security suggests the need for a clear economic policy on firms' behavior.

1. Investment in cybersecurity tools only makes sense if it is done continuously under strict regulation. If it lasts for only short periods and there is little control, traditional monopolies or oligopolies with significant market power will return and will transfer security costs back to consumers. The data in Table 1 indicate that a security investment of around 20% of profits resulted in an increase of almost 40% in prices in period 1.
2. If the subsidy helps firms maintain control of consumers' information, strategic advantages for the firm, such as big data analysis, may emerge. Security measures may lead to market manipulation and the abuse of position by firms.

This Chapter presents open questions that are interesting to analyze. We study the monopolist's decision to invest in security. However, a competitive scenario (duopoly) can offer very different conclusions. In concrete, the study of investments' decision of a firm that could depend on the security investments of the other one. Some interesting queries: i) To know the implications of a competitive setting in social welfare and, to compare the resulting optimal precisions in equilibrium with the one in absence of competition. ii) To investigate the implications of a competitive setting in consumers' expectations over privacy concerns.

On the other hand, a convenient study is to consider investment in security depending on the probability of suffering a cyberattack. This may complicate the analysis but it is an actual

[16] http://www.consilium.europa.eu/es/press/press-releases/2017/11/20/eu-to-beef-up-cybersecurity/pdf

factor taking into consideration in the companies' security investments.

3.6 Appendix

Proof of Proposition 8

There exists a noisy signaling equilibrium:

1. Given (3.4) and (3.6), and the expected demand in period 1 and 2, the monopolist maximizes her expected profits in each period, given by (3.9) and (3.10) in the main text, respectivaley. Taking the first order conditions with respect p_1 in period 1

   $$\theta_i - \bar{x} - 2p_1 = 0 \tag{3.36}$$

   Taking the first order conditions with respect p_2 in period 2, yields

   $$\theta_i - \bar{x}\gamma_x - \bar{x}\delta_\alpha\gamma_z - \delta_z(a + bp_2) - p_2(1 + b\delta_z) - p_2 = 0. \tag{3.37}$$

   The second conditions holds in period 1, that is $-2 < 0$. In period 2, second order condition also holds, $-2 - 2b\delta_z < 0$ where b is as we specified in (3.13) in the main text. Then, solving (3.36) for the period 1, and (3.37) for period 2, we get the equilibrium price

   $$p_1^* = \frac{\theta_i - \bar{x}}{2} \tag{3.38}$$

   in period 1. For period 2, we get (3.11) in the main text, which is

   $$p_2^* = \frac{\theta_i - a\delta_z - \bar{x}\gamma_x - z\delta_a\gamma_z}{2(1 + b\delta_z)}.$$

2. Given any observation of p_2^* in the second period, consumers and firm updates their information. Consumers will make an inference over z after observing the second period price, then consumers are correct in believing that the z observed by the firm

actually equals $p_2^* = \frac{z-a}{b}$. Then, in a linear separating equilibrium

$$a = \frac{\theta_i - \bar{x}\gamma_x}{\gamma_z}$$

and

$$b = \frac{2}{(\delta_\alpha - 2)\,\gamma_z}$$

as it is specified in the main text.

3. Substituing a and b in (3.11), using simplifications described in (3.7) and (3.8) in the main text, we get the expected second period price and expected second period profits, specified in (3.14) and (3.15) in the main text.

Proof of Proposition 9

If γ_z is fixed and common knowledge, then the equilibrium prices in period 1 and 2, are specified in the main text. Furthermore, this is the unique equilibrium where comsumers' inferences about z are a differentiable and invertible function of p_2.

The calculations above showed that this a linear equilibrium. The uniqueness property follows from the nature of the signaling differential equation. Assume that consumers infer $z = \hat{z}(p)$ if second period price is p_2, where $\hat{z}$ is C^1. The demand curve faced by the firm in period 2 is

$$\theta_i - \bar{x}\gamma_x - \delta_z\hat{z}(p_2) - z(p_2)\delta_\alpha\gamma_z - p_2$$

The profit maximization price satisfies the first-order condition

$$\theta_i - \bar{x}\gamma_x - \delta_z z' p_2 - \delta_z\hat{z}(p_2) - z\,(p_2)\,\delta_\alpha\gamma_z - 2p_2 = 0,$$

and implicitly defines the correct rule, $z(p)$. In a Bayes-Nash equilibrium, consumers use the correct inference rule, that is $\hat{z}\,(p_2) = z\,(p_2)$; hence, $z\,(p_2)$ must solve the ordinary differential equation

$$2p_2 - \theta_i + \bar{x}\gamma_x = -\left(z^{'} p_2 \delta_z + z(p_2)(\delta_z + \delta_\alpha \gamma_z)\right).$$

We proceed ordering and simplifying the terms in the previous differential equation to look for general/particular solutions. To that end,

- Firstly, dividing the ordinary differential equation by $p_2\delta_z$, we get

$$\frac{2}{\delta_z} - \frac{\theta_i - \bar{x}\gamma_x}{p_2\delta_z} = -\left(\frac{z^{'}(p_2)\,\delta_z p_2 + z(p_2)(\delta_z + \delta_\alpha \gamma_z)}{p_2\delta_z}\right).$$

  Letting $s = \frac{2}{\delta_z}$, $t = \frac{\theta_i - \bar{x}\gamma_x}{\delta_z}$, and $r = \frac{(\delta_z + \delta_\alpha \gamma_z)}{\delta_z}$, and reordering the terms yields

$$z^{'}(p_2) + z(p_2) p_2^{-1} r = p_2^{-1} t - s.$$

- Secondly, multiplying the expression above by p^r (the integrating factor) then gives

$$p^r\left(z^{'}(p_2) + z(p_2) p_2^{-1} r\right) = p^r\left(p_2^{-1} t - s\right),$$

  which may be integrated to

$$p^r(z(p_2)) = p^r\left(\frac{t}{r} - \frac{p\ \ s}{1+r}\right) + C = p^r t r^{-1} - p^{r+1} s(1+r)^{-1} + C.$$

  for some constant C. This is a general solution. To determine C, we need the value of the function $z(p_2)$ at one point. For instance, if $z(0)$ is finite (the initial condition), then, evaluating the differential equation at $p_2 = 0$, gives that $C = 0$. Hence $z(p_2)$ is linear in p_2.

Proof of Proposition 10

Security investments in period 1 translates to period 2 through the possible changes in consumers' previous experience, δ_α. Roughly speaking, the optimal level is obtained by equating marginal revenues with the marginal cost of security investment in period 2.

1. Firstly, we compute the partial derivative $\frac{\Pi_2^{s*}}{s_1^*}$, which it is indeed the marginal revenues of the security investment, $\frac{\partial \Pi_2^*}{\partial s_1^*} = \delta_\alpha p_2^s$.

2. Secondly, taking into consideration the simplifications in (3.7) in the main text, and that the marginal cost of security investment, cs_1, we can rewrite the maximization problem as the problem of marginal revenues equaling marginal costs, $MR - MC = 0$, in period 2,

$$\frac{\delta_\alpha \left(\theta_i + s_1 \delta_\alpha - s_1^e \delta_\alpha - z\delta_\alpha \gamma_z - a\delta_z - \bar{x}\gamma_x\right)}{2\left(1 + b\delta_z\right)} - cs_1 = 0. \tag{3.39}$$

3. Substituing the expectation over z, that is, $E\{z\} = \bar{x}$ and clearing for s_1, we get

$$s_1 = \frac{\delta_\alpha \left(\delta_\alpha \left(s_1^e + \bar{x}\gamma_z\right) + b\delta_z - \theta_i + \bar{x}\gamma_x\right)}{\delta_\alpha^2 - 2(c+1)\left(b\delta_z + 1\right)}. \tag{3.40}$$

4. In equlibrium, beliefs are correct (i.e., $s_1 = s_1^e$) and inserting in (3.40) a and b from (3.19) and (3.20) in the main text respectively, the previous expression translates to

$$s_1^* = \frac{\left(2 - \delta_\alpha\right)\delta_\alpha \left(\theta_i - \bar{x}\right)}{2c},$$

the optimal amount of investment in equlibrium for the monopolist.

It is important to note that the firm's second order condition requires that $c > \frac{2\delta_\alpha - \delta_\alpha^2}{2}$; c must sufficiently large so that profit is bounded. Under this condition, we conclude that $0 < s_1 < \bar{x}$.

5. The profit maximizing p_1 is the full information price corresponding to the expected quality, s_1^*. Therefore,

$$p_1^{s*} = \frac{1}{2}(\theta_i - (\bar{x} - s_1)).$$

Proof of Proposition 11

In order to obtain the optimal for the signal precision, we work with the expected demand perceived by the consumers exposed in (3.24) in the main text. Note that it depends on the consumers' beliefs about the values of δ_α and δ_z. Given that the monopolist can choose a specific level in signal precision, we express the update of beliefs in period 1 in terms of γ_z, i.e., $E[\alpha_{i1}|z] = \gamma_z z + (1-\gamma_z)\bar{x}$. Plugging inside on the expected demand, we get

$$E[q_2^e|\Omega_2(\alpha_{i2}, z)] = \theta_i - (\delta_\alpha(\gamma_z z + (1-\gamma_z)\bar{x}) + \delta_z(a + bp_2) + \bar{x}\delta_x) - p_2.$$

Using simplifications in (3.8) in the main text, we get (3.25). Once we get the expected profit conditional on z given by (3.26), the firm solves the maximization problem,

$$\gamma_z^* = \quad arg\max_{\gamma_z} \quad E\{\Pi_2^e\} - c(\gamma_z).$$

We express the first order condition as marginal costs equating marginal revenues in (3.26) in the main text. Next, plugging b in (3.20) in the main text for a linear equlibrium, using (3.7) and clearing for γ_z, we get the expression in (3.27). Assuming that in Bayes Nash equilibrium, consumers' beliefs are correct, we get finally (3.28) in the main text. Furthermore, the second order condition also holds. To show why our assumption on c(·) assure a unique interior value of γ_z, let us write δ_α in as

$$\delta_\alpha = \frac{(1-\gamma_z)\sigma_x^2 + \sigma_\omega^2}{(1-\gamma_z)\sigma_x^2 + \sigma_\omega^2 + \sigma_v^2}. \tag{3.41}$$

i) Let us recall the equation in (3.29), which is the first order condition of the profits, as $\Upsilon(\gamma_z)$. We want to show that $\Upsilon'(\gamma_z) < 0$.

ii) As can be seen from the expression in (3.41), the partial derivative of δ_α respect to γ_z turns out to be

$$\frac{\partial \delta_\alpha}{\partial \gamma_z} = -\frac{\sigma_v^2 \sigma_x^2}{(\sigma_v^2 + \sigma_x^2 (1-\gamma_z) + \sigma_\omega^2)^2}.$$

Since all the variances are non-negative, the sign of the partial derivative above is negative. Thus, there is an inverse relationship between the weight of the previous experience for consumers and the precision of the monopolist's private signal.

iii) Thus, the second order condition, which is $\Upsilon'(\gamma_z) = -\frac{2\left(\sigma_v^2\sigma_x^6\left(\sigma_v^2+(1-\gamma_z)\sigma_x^2+\sigma_\omega^2\right)^2+\sigma_v{}^4\sigma_x^8\right)}{\left(\sigma_v^2+(1-\gamma_z)\sigma_x^2+\sigma_\omega^2\right)^5} < 0$.

Chapter 4

Privacy and successive monopolies

4.1 Introduction

Selling data, some of a personal nature, has led to the creation of the data market in the 21st century. In Chapter 1, it was mentioned that the sale of databases of personal data is not something new and, it existed in the twentieth century. However, the information technology and the accessibility to the Internet have increased the scope and reach of these bases. This fact has made the data market a lucrative business for the economic agents that are dedicated to the collection, analysis and sale of them.

Nevertheless, the indiscriminate use of personal information and the existence of clear harm to consumers of online content (privacy breaches, sale of data without consent, price discrimination, etc.) has urged policy makers for a regulation in order to protect consumers and make them aware of their value for privacy. The overall lack of transparency and disclosure in this market have made it impossible for users to know what they are giving up. As a result, regulators wrestle with consumer privacy protection in the Internet age.

Chapter 1 briefly introduces the current regulation of privacy, and the limits between the private and the public. Specifically, there are some touches on regulation in the US and, the General Data Protection Regulation (GDPR) in Europe. Both policies present different approaches: in the GDPR, European regulators favor an opt-in policy where firms must first obtain consumer consent; on the other hand, American regulators have favored an opt-out policy where concerned consumers can choose to avoid behavioral advertising in order to balance consumer privacy protection. From the users' point of view, opting in is the process by which a user takes an affirmative action to offer their consent. By contrast, opting out is the process by which a user takes action to withdraw their consent. Although they can be seen as a different approaches, in reality it is important to keep in mind that wherever there is an opt-in, there needs to be an opt-out, so that users can withdraw their consent at any time. Thus, all in all, the recent laws and user demand for greater transparency and control when it comes to personal data, stress the importance of implementing opt-in and opt-out mechanisms.

Our contribution is to endogenenize the data sale process and to study three main privacy-policy protection for consumers in a context of two successive monopolies where there exists information sales from one monopoly to the other. The first baseline scenario, autarky, refers to the case in which selling data is not permitted (maximum privacy). Secondly, we explore a scenario of data-sharing policy, the case in which selling data is permitted. And finally, we examine the possibility to opt-out and, therefore, consumers' endogenous decision of not having their personal data sold.

Johnson et al. (2017), estimate the economic loss from opting out by obtaining a proprietary dataset of ad transactions from an ad exchange operating in the United States and internationally. They find that opt-out consumers represent a small share of the marketplace: only 0.23% of American ad impressions arise from opt-out consumers. They show that opt-out rates are similarly low in other countries that implemented the AdChoices program: 0.16% in Canada and 0.26% in the European Union (prior to GDPR). Our main result highlights that giving consumers an opt-out option might be, in principle, social welfare improving under uniformly distributed consumers' valuations. However, and as a possible explanation for the scarce use of the opt-out option policy in the data above, data sharing renders higher consumer surplus than that under out-opt. Thus, the consumer, who is the ultimate recipient of all privacy policies, does not seem to improve his surplus with the opt-out option.

We study the exchange of information between two monopolies, selling sequentially to a pool of buyers. The monopoly in the upstream market gathers information to sell it to the firm in the downstream market, to use it to discriminate in the downstream one. These facts deliver endogenous demand for ”hiding” (privacy) and model consequences in terms of economic primitives.

Some previous literature addresses consumer hiding by assuming there is an exogenous cost to hiding information. We render this cost endogenous. In particular, we render endogenous the cost of collecting information, which we do by assuming that consumer information is collected in one market, and sold on to firms in another market. We stress that the possibility of selling information causes the firm in the information-gathering market to lower its price in order to bring in more consumers and so sell information about them. This is a two-edged sword: consumers benefit from lower prices in that market, but they may suffer in the other market through being discriminated against. Moreover, there are externalities imposed on other consumers in the second market insofar as market prices they face there may rise for some, while falling for others. Some consumers may therefore choose not to buy in the first market in order to hide their valuations and so avoid being discriminated against. This may imply that the firm in the first (information-gathering) market may actually be better off by allowing consumers an opt-out option whereby they elect not to disclose their information, or they may take up offers by the firm in the first market to not have their information revealed to third parties. Allowing such an option enables the first firm to make more profits by eliminating hiding by non-purchase.

We proceed to detailing our model. The model considers an upstream firm with a single downstream one, to which it can sell information gathered in its market. This model delivers already the result that the presence of consumer hiding induces the firm to reduce its price and to sell information. However, because some consumers hide, the market price is higher in the downstream market (than in the absence of consumer hiding). Moreover, because of the hiding and its lower price, the upstream firm's profits from its own sales fall. This is whence comes the impetus for profitably allowing opt-out. And, the opt-out option raises consumer surplus and total welfare. In this context, of a single firm upstream and downstream, the upstream firm can extract the full value of the incremental profit to the downstream one, and so the problem is equivalent to that of a two-product monopoly that gathers information in the first market to use in the second one. However, notice that this is not a simple two-product monopoly for two reasons: first, the consumer hiding, and second, the two-stage structure and impact of rational expectations by consumers: those who hide in the first market rationally expect the price in the second one, and this expected price must be consistent with what the downstream firm actually wants to do, facing a set of consumers who are hiding their values (as well as those who do not, and are discriminated against). The equivalence of the problem to that of a single firm breaks down when there are several firms downstream. In particular, selling information to one firm downstream has negative externalities on other firms there, so that the equilibrium price of information is higher because those suffering firms bid up the value of the information in an attempt to preclude rivals from getting it. The firm selling the information can therefore get more from the information than when it also is one of several sellers downstream: it can internalize part of the externality because it gets value from rival sellers too.

4.2 Literature review

Our model links with market structures both upstream and downstream to analyze the context of selling information from one company to another. The first stream of literature we are related to examines the sale of information to other parties. In particular, Sarvary and Parker (1997) model information-sharing among competing consulting companies; Xiang and Sarvary (2013) study the interaction among providers of information to competing clients; Iyer and Soberman (2000) analyze the sale of heterogeneous signals, corresponding to valuable product modifications, to firms competing in a differentiated-products duopoly; Taylor (2004b) studies the sale of consumer lists that facilitate price discrimination based on purchase history. Other research inside this stream, focus in the strategic role of an intermediary selling this information, as Data Brokers or Platforms e.g., Braulin and Valletti (2016); Montes et al. (2018); Bounie et al. (2018). The presence of an intermediary in these papers renders the acquisition of information to be exogenously given. In this Chapter, there is no intermediary of the information; we endogenize the decision regarding to the acquisition and sale of information through the sale of products in the market. Furthermore, we analyze the setting of take-it or leave-it offer about all information of consumers. We do not study the case of "bit-pricing" of information or sale of segments of information as in Bergemann and Bonatti (2015) and Bounie et al. (2018).[1] Considering the case of succesive sale from one firm to another firm, our work is close to Calzolari and Pavan (2006). They consider an agent who contracts sequentially with two principals, and allow the former to sell information to the latter about her relationship (contract offered, decision taken) with the agent. Their findings point out that the disclosure of information may increase agent's surplus in the two relationships with principals. In our case, we also find that this disclosure increases total consumers' surplus in the market. However, they find ambiguous the effect of disclosure on

[1] Bergemann and Bonatti (2015) focus on "bit-pricing" of information and, propose a model of data provision and data pricing, a setting that captures the key economic features of the market for third-party data.

welfare. On the contrary, in our analysis with consumers' valuations uniformly distributed, the disclosure of information is social welfare improving.

A second stream of literature examines the implications of consumer privacy on pricing and privacy regulation, as well as their consequences on welfare (see Acquisti et al. 2016 for a comprehensive review of this literature). The majority of works here assumes that consumers' privacy decisions are exogenously determined (see, e.g., Acquisti and Varian 2005, Taylor and Wagman 2014, Shy and Stenbacka 2016). In other words, consumers either have no option to remain anonymous, which is the same as that in the literature on behavior-based price discrimination, or they can erase their data costlessly.[2] We differ from the literature on BBPD in two ways: i) in they are dynamic models and our setting is sequential; ii) firms use consumers' information from past purchases to practise third-degree price discrimination (e.g., Fudenberg and Tirole 2000) or personalized pricing (e.g., Choe et al. 2017). The upstream firm in our model does not use the information to price discriminate, but how the dowsntream firm designs her price affects the upstream's price and thus, we focus on the prices dependency when information is sold, that is, prices are endogeneous. Furthermore, we analyze the distortion on prices from letting data sharing with respect to the general monopoly equilibrium.

More recently, a growing number of research papers have considered the implications of consumers' endogenous decisions regarding how much information to be revealed to the firm. Casadesus-Masanell and Hervas-Drane (2015) consider a duopoly setting where consumers can choose the amount of information being provided to the firms, much in line with a opt-out policy. Montes et al. (2018) consider a data-broker selling to downstream Hotelling duopolists with endogenous consumers' privacy choices, where it exists privacy costs to be anonymous in the market. That is, privacy is costly. On the other hand, Braulin and Valletti (2016) investigate the question of the extent to which the data broker that has collected

[2] For a related literature on behavior-based price discrimination see, e.g., Esteves (2010); Fudenberg and Villas-Boas (2012); Villas-Boas (2014).

a unique data set will want to sel the data to all competing dowstream firms. However, consumers' do not have options to access to a privacy policy. Valletti and Wu (2016) analyze a model where a monopolist can profile consumers in order to price discriminate among them, and consumers can take costly actions to protect their identities and make the profiling technologies less affective. We also explore the scenario for consumer' endogenous decisions regarding to avoid being profiling letting them the opportunity to opt-out.

Belleflamme and Vergote (2016) and Chen et al. (2018) are closest to our opt-out analysis because they permit customers to hide from profiling. The former show (for monopoly) that tracking technology lowers consumer surplus because firms are able to price discriminate, but hiding technology worsens consumer surplus further because the firm raises regular prices to discourage hiding. Belleflamme et al. (2017), extend the setting of Belleflamme and Vergote (2016), to a duopoly market for a homogeneous product. If both firms have the same profiling technology of the exact same precision, then the Bertrand paradox continues to prevail. When both firms have imperfect and asymmetric profiling technologies, then both price discrimination and price dispersion arise in equilibrium. In particular, equilibrium personalized prices always exhibit price dispersion. This dispersion may lead firms to randomize equilibrium uniform prices as well to avoid the Bertrand paradox. In Chen et al. (2018), each firm in a Hotelling model can personalize prices for consumers in its target segment and offer a uniform poaching price for non-targeted customers. Hiding consumers make it harder to poach, softening competition through higher prices for non-targeted consumers. Both papers suggest, counterintuitively, that privacy regulation empowering consumers may make them worse off. Our results with consumers' valuations uniformly distributed point out that giving consumers an opt-out option for not taking personal information sold worsens their consumers surplus. Furthermore, and in line with the main result in Belleflamme and Vergote (2016), consumer surplus is larger when this hiding or opt-out option is not available. Indeed, having their personal information sold increases their consumer surplus as long as the maximum willingness to pay in the upstream market gets bigger, big upstream market. Moreover, this fact gives more incentives to the downstream market to buy personal information.

The Chapter is organized as follows. The general model is presented in Section 4.3. Section 4.4 specifies the effects of upstream prices on downstream ones. The case of consumers' valuations uniformly distributed is analized in Section 4.5. Section 4.6 offers the demand for privacy. Finally, a more simple model is analyzed in Section 4.7.

4.3 Upstream & downstream markets

Consider two firms, Firms 0 and 1, which are monopolists in separate markets, but share a common pool of consumers. Therefore, there are 2 independent goods, each sold by a separate monopoly firm. Consumer valuations are independently distributed with valuation distribution functions $F(k)$ for good 0 and $G(v)$ for good 1, where a consumer drawn at random has valuations k and v. We assume that the $1-F(.)$ and $1-G(.)$ are both strictly log-concave. Costs of production are suppressed for simplicity.

We want to study the exchange of information between two monopolies, selling sequentially to a pool of buyers. Consumers visit Firm 0 first and decide whether to purchase its product at price p_0. If they purchase, Firm 0 learns their type, and if they do not purchase, Firm 0 learns nothing. Depending on the information-policy regime, Firm 0 may sell its customers' data that is, reveal their valuations to Firm 1. Then, the consumer visits Firm 1 where, if her data has not been sold, she is offered a uniform price p_1 . Alternatively, if they bought at Firm 0 and it sold their data to Firm 1, then they are charged a personalized price that extracts their full valuation v. Because of the order in which a consumer faces the two firms, we refer to Firm 0's market as upstream and Firm 1's market as downstream. This is just shorthand for the timing of consumer choices; it does not mean that Firm 0 is a supplier to Firm 1.

We start with the case of no information revelation about types. Then the equilibrium prices are simply the monopoly ones that solve,

$$\begin{aligned} p_0^n &= \frac{1-F\left(p_0^n\right)}{f\left(p_0^n\right)}, \\ p_1^n &= \frac{1-G\left(p_1^n\right)}{g\left(p_1^n\right)}. \end{aligned}$$

To set the stage for the information analysis, suppose that Firm 0 were to sell information to Firm 1, and the information fully revealed the consumer's v value. Then Firm 1 offers a perfectly discriminating full-surplus-extraction price to each consumer for whom it has information.

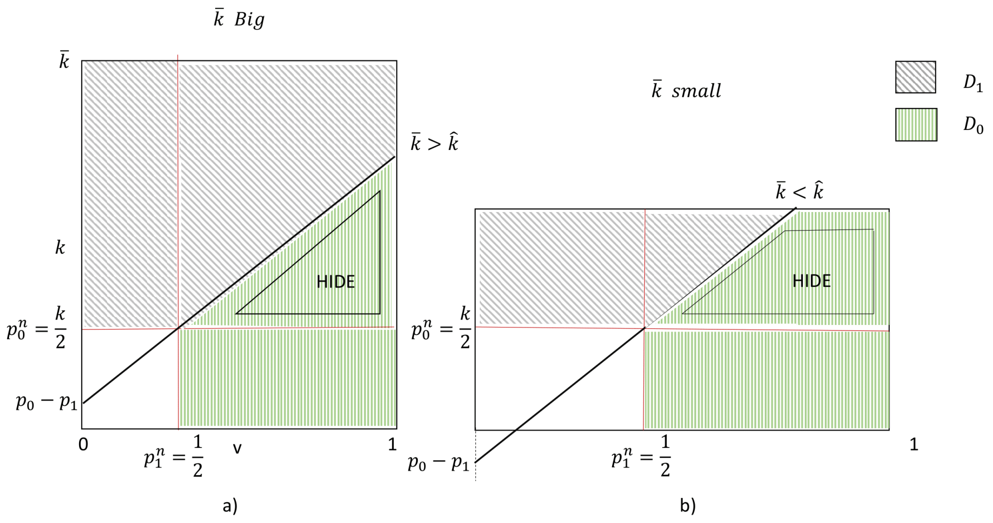
However, suppose for now that the price pair $\left\{p_0^n, p_1^n\right\}$ were fixed as above. Any consumer type $\{k, v\}$ will now face the choice of hiding her v information by not buying good 0, in the knowledge she would get no surplus from Good 1 should she buy Good 0. Then, her value for Good 0 purchase is $k - p_0^n - \left(v - p_1^n\right)$ where the second term is her lost surplus on Good 1. The locus of indifferent consumers is given as

$$k = v + p_0^n - p_1^n.$$

Any consumer for whom $k < p_0^n$ will not buy Good 0, and any consumer for whom $v < p_1^n$ will not buy Good 1 unless she has bought Good 0 and pays v. The attribution of consumers to purchases is shown in Figure 4.1 for values of $v \in (0,1)$, where Figure 4.1 a) shows the case for $\bar{k}$ big or Market 0's huge size and, Figure 4.1 b) shows the case for $\bar{k}$ small or Market 0's small size.

In particular, those left of the locus $k = v + p_0^n - p_1^n$ and with $k > p_0^n$ are those buying Good 0, and they are also discriminated against and getting no extra surplus from Good 1. Those for whom $k < p_0^n$ and $v < p_1^n$ will buy neither good, and those for whom $v > p_1^n$ and below the locus $k = v + p_0^n - p_1^n$ will buy only Good 1, at price p_1^n.

Fig. 4.1 Upstream & downstream markets



With respect to the original allocation, the consumers right of the locus $k = v + p_0^n - p_1^n$ (represented in both figures by the thick black line) and with $k > p_0^n$ are hiding their types from being sold to Firm 1. There is a corresponding loss of consumer surplus on their account, as well as a lost demand (and hence profit) to Firm 0. However, surplus is enhanced by the extra sales made now to consumers in the upper right rectangle in figure 1 a), and this accrues as extra gross profit to Firm 1. There is also a transfer from consumer surplus to Firm 1's gross profit on the consumers with $v > p_1^n$ left of the locus $k = v + p_0^n - p_1^n$. They used to buy Good 1 at p_1^n but now find their surplus fully extracted.

If this were the end of the story, then we could simply add up the various gains and losses to determine whether the information transmission enabled from buying good 0 is socially desirable. Note that consumers are necessarily worse off, and this is a strong driver of the consumer surplus results below. The social surplus calculation simply revolves around whether the lost consumer surplus from Good 0 on those hiding their types by no longer buying it is made up for by the extra surplus on Good 1 generated from those previously not purchasing it.

Note also that giving consumers an opt-out option on having their information forwarded is surplus enhancing: no one needs to hide, all those who bought both goods originally opt out, and the benefits of price discrimination accrue on the types with $k > p_0^n$ and $v < p_1^n$, who do not care whether their information is revealed because they got no surplus from Good 1 since they were not buying it.

We can already see the tensions involved in now rendering the prices endogenous. First, notice that the "hiding" consumers tend to be predominantly high valuation types for Good 1, and thus they render its demand more inelastic, and are a force towards a higher p_1. This is the *selection effect.* However, notice that the lower is p_0 the greater the incentive for 0 to set a higher price because its base of marginal consumers who are not locked in to buying it is larger. Moreover, Firm 0's pricing incentives are driven by 3 factors. A lower price gives it more customers to sell information upon to Firm 1. But more consumers are induced to hide from it. Lastly, it has to internalize the effect that the lower the price it sets then, the higher is 1's equilibrium price.

The first part of the Chapter addresses the upshot of these effects. Thus, at the first stage, Firm 0 sets its price p_0. We study the subgame perfect (Bayesian) Nash equilibria of the model. For any subgame following a choice p_0, this implies that Firm 1's hidden price p_1 maximizes its profits given correct beliefs about which consumers are hidden, and each consumer's decision at Firm 0 maximizes her total surplus, given correct beliefs about Firm 1's downstream pricing. At equilibrium, consumers' beliefs and firm 1's beliefs are correct.

4.4 Effects of upstream price on dowstream one

This section determines how a higher upstream price affects the downstream one. We seek a subgame perfect bayesian equilibrium at which consumers rationally anticipate the price that Firm 1 will set. To do this, we find the price expected by consumers, p_e, that coincides with the actual one that Firm 1 wants to set given the set of consumers who hide their information. We denote Firm 1's actual demand by p_a, so that the equilibrium price satisfies $p_1 = p_e = p_a$.

The downstream demand is

$$D_1 (p_a, p_e) = \int_{p_a}^{\infty} F (v + p_0 - p_e) g (v) dv,$$

with derivative

$$\frac{dD_1 (p_a, p_e)}{dp_a} = -F (p_a + p_0 - p_e) g (p_a).$$

Hence the equilibrium price solves $\max_{p_a} R_1 = p_a D_1 (p_a, p_e)$ (representing 1's revenue from non-discriminatory sales: note that 1's choice of p_a does not affect its profit from discriminatory sales) with $p_1 = p_e = p_a$. This gives the implicit expression

$$\int_{p_1}^{\infty} F (v + p_0 - p_1) g (v) dv = p_1 F (p_0) g (p_1). \tag{4.1}$$

The implicit function theorem yields the derivative expression

$$\frac{dp_1}{dp_0} = \frac{\int_{p_1}^{\infty} f (v + p_0 - p_1) g (v) dv - p_1 f (p_0) g (p_1)}{2F (p_0) g (p_1) + p_1 F (p_0) g' (p_1) + \int_{p_1}^{\infty} f (v + p_0 - p_1) g (v) dv}$$

where the denominator is positive from the second-order condition. $-2F (p_0) g (p_1) - p_1 F (p_0) g' (p_1) < 0$. The expression therefore takes the sign of the numerator. Inserting the expression (4.1) for p_1 gives the numerator as

$$\int_{p_1}^{\infty} f (v + p_0 - p_1) g (v) dv - \frac{f (p_0)}{F (p_0)} \int_{p_1}^{\infty} F (v + p_0 - p_1) g (v) dv.$$

Because F is log-concave, then f/F is decreasing and so $\frac{f(v+p_0-p_1)}{F(v+p_0-p_1)}$ is highest at $v = p_1$, where it takes the value $\frac{f(p_0)}{F(p_0)}$. Thus, looking at the first term above, $\int_{p_1}^{\infty} f (v + p_0 - p_1) g (v) dv = \int_{p_1}^{\infty} \frac{f(v+p_0-p_1)}{F(v+p_0-p_1)} F (v + p_0 - p_1) g (v) dv < \frac{f(p_0)}{F(p_0)} \int_{p_1}^{\infty} f (v + p_0 - p_1) g (v) dv$ and hence we have proved that $\frac{dp_1}{dp_0} < 0$. The intuition is that higher p_0 means fewer hiding consumers, less source of demand inelasticity from this source.

We can now try the general solution for p_0. Write Firm 0's profit as its direct revenue from subscriptions plus the value of its information in improving Firm 1's profit:

$$\pi_0 = p_0 D_0 + \pi_1 - \bar{\pi}_1$$

where $\bar{\pi}_1$ is 1's default profit (i.e., in the absence of information, i.e., $\bar{\pi}_1 = \frac{(1-G(p_1^n))^2}{g(p_1^n)}$) and write D_0 as $\int_{p_0}^{\infty} G(k-p_0+p_1) f(k)\, dk$ (all those above p_0 left of the locus $k = v + p_0 - p_1$).

$\pi_1 = p_1 \int_{p_1}^{\infty} F(v+p_0-p_1) g(v)\, dv + \int_{p_0}^{\infty} f(k) \int_0^{k-p_0+p_1} v g(v)\, dv dk$

These are areas described in Figure 4.1 where it can be seen the regions for Firm 1's demand, D_1, and for Firm 0's demand, D_0. Furthermore, Figure 4.1 shows both cases, with big and small values for $\bar{k}$. The first term is revenue from consumers whose types have not been specifically determined, while the second is discriminatory pricing revenue. The profit derivative is then composed of the parts, which might all be interpreted, and confer with the above Figure 4.1,

$$\begin{aligned}\frac{d\pi_0}{dp_0} &= D_0 - p_0 \left(\int_{p_0}^{\infty} g(k-p_0+p_1) f(k)\, dk + G(p_0) f(p_0) \right) \\ &\quad + p_1 \int_{p_1}^{\infty} f(v+p_0-p_1) g(v)\, dv - \int_{p_0}^{\infty} (k-p_0+p_1) f(k) g(k-p_0+p_1)\, dk \\ &\quad - \int_{p_0}^{\infty} f(k) \int_0^{p_1} v g(v)\, dv dk + \frac{d\pi_1}{dp_1}\frac{dp_1}{dp_0}\end{aligned}$$

Note that $\frac{d\pi_1}{dp_1}$ is not zero by the envelope theorem because of the role of the expected price. We might use the envelope theorem to rewrite it. The derivative is, prior to substitution from the fist order condition:

$$\begin{aligned}\frac{d\pi_1}{dp_1} &= \int_{p_1}^{\infty} F\left(v+p_0-p_1\right)g\left(v\right)dv - p_1\left(\int_{p_1}^{\infty} f\left(v+p_0-p_1\right)g\left(v\right)dv + F\left(p_0\right)g\left(p_1\right)\right)\\ &\qquad + \int_{p_0}^{\infty} f\left(k\right)\left(k-p_0+p_1\right)g\left(k-p_0+p_1\right)dvdk\\ &= -p_1\int_{p_1}^{\infty} f\left(v+p_0-p_1\right)g\left(v\right)dv + \int_{p_0}^{\infty} f\left(k\right)\left(k-p_0+p_1\right)g\left(k-p_0+p_1\right)dvdk\end{aligned}$$

where in the second line we did substitute Firm 1's choice condition (4.1).

Note then the two terms have cross-overs from the earlier part of 0's profit derivative, representing transferring demands between segments of different values. Therefore, we can write

$$\begin{aligned}\frac{d\pi_0}{dp_0} &= D_0 - p_0\left(\int_{p_0}^{\infty} g\left(k-p_0+p_1\right)f\left(k\right)dk + G\left(p_0\right)f\left(p_0\right)\right)\\ &+ \left(p_1\int_{p_1}^{\infty} f\left(v+p_0-p_1\right)g\left(v\right)dv - \int_{p_0}^{\infty}\left(k-p_0+p_1\right)f\left(k\right)g\left(k-p_0+p_1\right)dk\right)\\ &\qquad \left(1-\frac{dp_1}{dp_0}\right) - \int_{p_0}^{\infty} f\left(k\right)\int_{0}^{p_1} vg\left(v\right)dvdk\end{aligned}$$

where $1-\frac{dp_1}{dp_0} = \frac{2F(p_0)g(p_1)+p_1F(p_0)g'(p_1)+p_1f(p_0)g(p_1)}{2F(p_0)g(p_1)+p_1F(p_0)g'(p_1)+\int_{p_1}^{\infty} f(v+p_0-p_1)g(v)dv}$

Given that the above equations are quite cumbersome, and in order to obtain sharper conclusions, we apply the above general findings for the case in which consumers' valuations follow uniform distributions.

4.5 Consumers' valuations uniformly distributed

Take v, which is the maximum willingness to pay for the product in the dowstream market, to be uniformly distributed on $[0,1]$, and k, the maximum willingness to pay in the upstream market, to be uniformly distributed on $\left[0,\bar{k}\right]$. In the uniform setting, we set k to be equal to or higher than v (big market 0). Then, the benchmark prices are $\left\{p_0^n, p_1^n\right\} = \left\{\frac{\bar{k}}{2}, \frac{1}{2}\right\}$, where the subindex 0 represents the upstream market and subindex 1 represents the dowstream market. Profits are given by $\bar{\pi}_1 = \frac{1}{4}$ and $\bar{\pi}_0 = \frac{\bar{k}}{4}$, respectively.

The locus of indifferente consumers, which it has been explained above, is obtained from the expected demand in the usptream market, that is $\bar{k} - p_0$, and, the expected demand in the downstream market, $v - p_1$. Equating $\bar{k} - p_0 = v - p_1$ and reordering the terms, we get the intercept $\bar{k} = v + p_0 - p_1$. Depending on the values of v and k, there are three possible regimes. Namely, each regime will depend on where the dividing line (locus), $k = v + p_0 - p_1$, intersects. The interpretation of this intercept is crucial, because it represents the elasticity of the demand and, moreover, shows that the slope depends on both prices, p_1 and p_0.

4.5.1 Regimes depending on the intercept

We first look at a regime where the purported equilibrium prices satisfied $\tilde{v} + p_0 - p_1 > \bar{k}$, as can be seen in Figure 4.2; this is the case of a small market 0 and does not satisfy the information-gathering requirements. To see that, let us denote this regime as Regime (a) and let p_e be consumers' expectation over Firm 1's price, and p_a Firm 1's actual inverse demand.

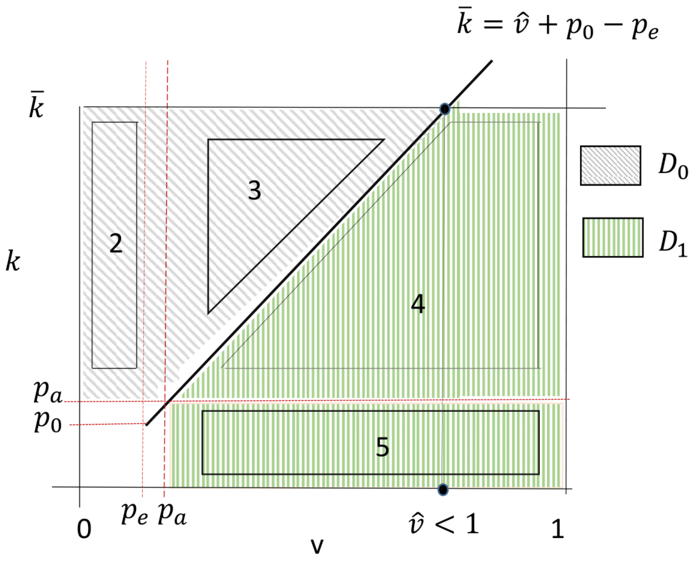


Fig. 4.2 Regime (a): $\bar{k} = \tilde{v} + p_0 - p_1$

Under this regime, and as can be seen in Figure 4.2 a), we calculate the expected demand in the dowstream market (Firm 1) when the consumers willingness to pay in this market is higher than the price, $v \geq p_1$, which corresponds to areas 4 and 5. Alternatively, it can be computed as the full area where $v \geq p_a$ minus area 3, a triangle. Thus,

$$D_1\left(p_a, p_e\right) = (1 - p_a)\bar{k} - \frac{\left(\bar{k} - p_a\right)\left(\hat{v} - p_a\right)}{2},$$

where $\hat{v} = k - p_0 + p_e$, and Firm 1's expected profits are therefore given by

$$\Pi_1\left(p_a, p_e\right) = p_a D_1\left(p_e, p_a\right). \tag{4.2}$$

In equlibrium, expectations are correct, that is, the demand derivative is evaluated at $p_e = p_a = p_1$ and, the second order condition holds $-k - p_0 < 0$. The first order condition gives the following expression,

$$\frac{1}{2}k(p_0 - k + 2) - p_1(k + p_0),$$

which indicates that p_1 as a function of p_0 is,

$$p_1\left(p_0\right) = \frac{2k - k^2 + kp_0}{2(k + p_0)}. \tag{4.3}$$

Firm 1's price specified above is positive when $p_0 = 0$, as long as $\bar{k} < 2$. Hence Firm 1's maximized profit as a function of p_0 is given by 4.3 where $p_1 = p_e = p_1(p_0)$. We now turn to Firm 0's problem. The expected demand for Firm 0 are the areas 2 and 3 in Figure 4.2,

$$D_0\left(p_0, p_a\right) = \left(\bar{k} - p_0\right)p_a + \frac{1}{2}(k - p_0)^2. \tag{4.4}$$

Firm 0's profits are coming from two sources,

$$\Pi_0 = p_0 D_0 + IP,$$

where D_0 is Firm 0's demand specified in equation (4.4) and IP are the informational profits. Specifically, Firm 0's informational profits are the profits for Firm 1 (full extration) specified in equation (4.2) minus Firm 1's default profits in the absence of information i.e., $\overline{\Pi_1} = \frac{1}{4}$ and, those as a result of the price discrimination from all the consumers identifies, from whom Firm 1 is able to charge their v.

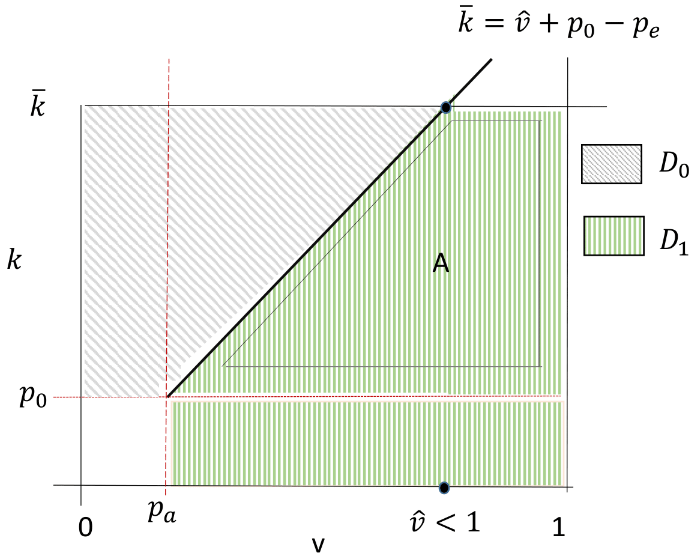


Fig. 4.3 Data-sharing policy a)

If we look carefully to Figure 4.3, we can derive the area that represents the profits coming from those consumers identified. Indeed, price discrimination is practised in area A and therefore, profits in this area are given by

$$A = \int_{p_0}^{k}\int_{0}^{k-p_0+p_e} v \quad dvdk = \frac{1}{6}\left((k-p_0+p_1)^3 - {p_1}^3\right).$$

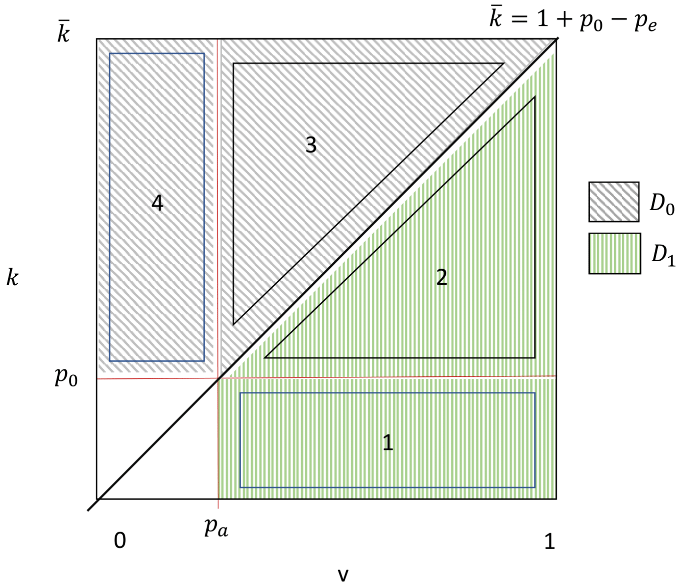
Therefore, Firm 0's profits are

$$\Pi_0 = D_0(p_0, p_1) + \Pi_1 - \frac{1}{4} + A.$$

Firm 0's interest of selling information will be determined for the difference between the profits coming from it and those obtained in the standard monopoly, i.e., $\pi_0^n = \frac{k}{4}$. Once we maximize the profits for Firm 0, the first order condition gives four possibles roots for Firm 0's price. Three roots out of four, are positive. However, none of them jointly with the equilibrium price for Firm 1 meets the restriction of the intersect under this regime, that is, $\tilde{v} \nless 1$. Thus, the equilibrium prices under this regime are not sustainable and, the region specified in A may not exist. Prices have to be lower in order to capture consumers. However, this is not possible because the restriction of the locus requires that $p_1 < p_0$, and the equilibrium prices do not meet it.

Secondly, we analyze regime (b) as can be seen in figure (3). In this case, $\bar{k} = 1 + p_0 - p_1$. In regime (b), the value for $\tilde{v} = 1$. Setting $k = 1$, implies that $p_0 = p_1$, which is clearly not consistent: the price in the upstream market has to be lower than firm 1's price in order to attract consumers to buy in the dowstream market. Furthermore, this setting does not give incentives to the dowstream firm to buy data, because the profits for obtaining info from consumers are lower that the ones coming from no data i.e., $\overline{\pi_1} = \frac{1}{4}$. Thus, this regime does not reflect the strategic interaction between both firms prices, and does not give incentives to share data.

Fig. 4.4 Regime (b): $\bar{k} = 1 + p_0 - p_1$



Finally, we look at the case $1 + p_0 - p_1 < \bar{k}$ (see Figure 4.5), regime (c), where we might say market 0 is dominant, or a big market relative to market 1. Then, the dividing line, $k = v + p_0 - p_1$ intersects $v = 1$ below $\bar{k}$.

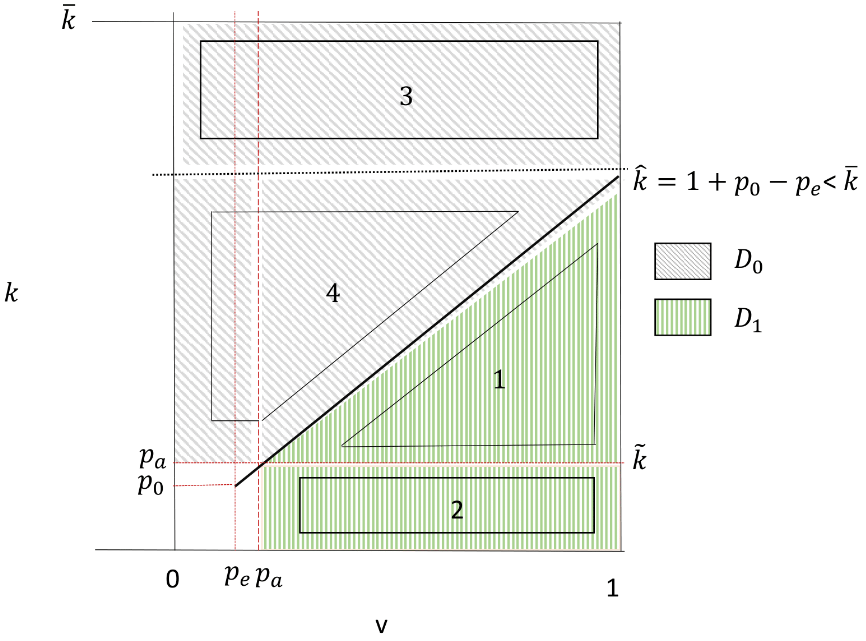
Then, we have (see figure 4.5) that the expected Firm 1's demand, is composed by areas 1 (a triangle) and 2 (a rectangle) in the graph. Therefore,

$$D_1\left(p_a, p_e\right) = \left(1 - p_a\right)\left(p_a + p_0 - p_e\right) + \frac{1}{2}\left(1 - p_a\right)\left(\hat{k} - p_0\right)$$

where $\tilde{k} = \tilde{v} + p_0 - p_e$ and $\tilde{v} = p_a$, the maximun willingness to pay in this area, and hence, $\tilde{k} = p_a + p_0 - p_e$. Furthermore, $\hat{k} = 1 + p_0 - p_e$, and thus, $\hat{k} - p_0 = 1 + p_0 - p_e - p_0 = 1 - p_e$. Finally,

$$D_1\left(p_a, p_e\right) = \left(1 - p_a\right)\left(p_a + p_0 - p_e\right) + \frac{1}{2}\left(1 - p_a\right)\left(1 - p_e\right).$$

Fig. 4.5 Regime (c): $\bar{k} > 1 + p_0 - p_1$



Therefore, Firm 1's profit is

$$\Pi_1\left(p_a, p_e\right) = p_a\left(\left(1-p_a\right)\left(p_a+p_0-p_e\right)+\frac{1}{2}\left(1-p_a\right)\left(1-p_e\right)\right). \tag{4.5}$$

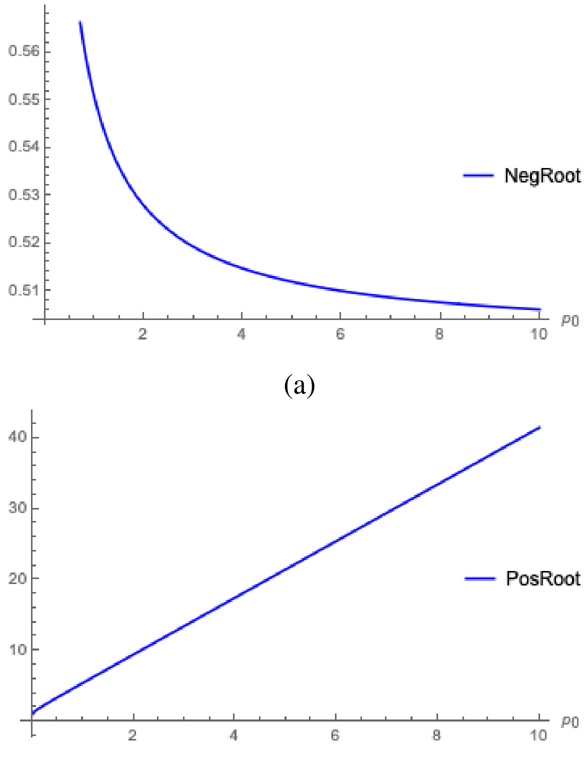
The demand derivative, evaluated at $p_a = p_e = p_1$, and the second order condition are satisfied $(-3p_a - p_0 + p_e < 0)$, that translates to $-2p_1 - p_0 < 0$.

The first order condition gives a quadratic function,

$$\left(1-p_1\right)p_0+\frac{1}{2}\left(1-p_1\right)^2-p_0p_1=0.$$

or

$$p_1^2+p_1\left(-2-4p_0\right)+2p_0+1=0$$



(a)

(b)

Fig. 4.6 Positive roots and tendencies

which is convex, slopes down and it is positive at $p_0 = 0$, and therefore, it has two positive roots. That is,

$$p_1(p_0) = 1 + 2p_0 \pm \sqrt{2}\sqrt{p_0 + 2p_0^2}. \tag{4.6}$$

The second order condition indicates that the solution is

$$p_1(p_0) = 1 + 2p_0 - \sqrt{2}\sqrt{p_0 + 2p_0^2}. \tag{4.7}$$

To see this, we plot in Figure 4.6 both positive results in equation (4.6), but we differentiate between the positive root, that is $+\sqrt{2}\sqrt{p_0 + 2p_0^2}$ and the negative root, $-\sqrt{2}\sqrt{p_0 + 2p_0^2}$. As can be seen, and in order to be consistent with the second order condition, the solution is the one with the negative root in equation 4 because it indicates that the Firm 1's price has a negative tendency as long as the Firm 0's price is increasing, highlighting the prices dependence between both firms prices.

Hence Firm 1's maximized profit as a function of p_0 is given by (4.6) where $p_1 = p_e = p_1(p_0)$.

We now turn to Firm 0's problem. The demand for Firm 0 are areas 3 and 4 in Figure 4.5,

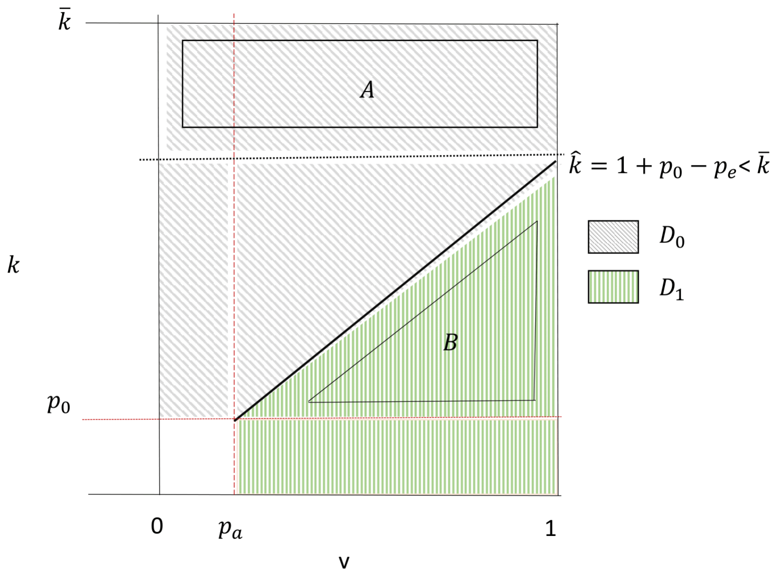
$$D_0(p_0, p_a) = (\bar{k} - p_0) - \frac{1}{2}(1 - p_a)^2. \tag{4.8}$$

Note that now Firm 0's profits are given from two sources similar to the previous case,

$$\Pi_0 = p_0 D_0 + IP,$$

where D_0 is Firm 0's demand specified in (4.8) and IP which are the informational profits. Specificaly, Firm 0's informational profits are the profits for Firm 1 (full extraction) specified in (4.5) minus the Firm 1's default profits in the absence of information (Firm 1's incentives to paticipate) and those as a result of the price discrimination from all the consumers identified.

Fig. 4.7 Data-sharing policy c)



If we look carefully to Figure 4.7, we can derive the area that represents the profits coming from those consumers identified. Indeed, price discrimination is practiced in A and B. A are the profits coming from the consumers with values of $k \in \left[1+p_0-p_1,\bar{k}\right]$ that are charged a price of $\frac{1}{2}$. Therefore, profits in A are given by

$$A=\left(\bar{k}-(1+p_0-p_1)\right)\frac{1}{2}$$

B represents the consumers with values of $k \in [p_0, 1+p_0-p_1]$ where the demand is

$$\int_{p_0}^{1+p_0-p_1} S(k)\, f(k)\, dk.$$

where $S(k)$ is

$$\int_0^{k+p_0-p_1} vg(v)\, dv$$

Solving for the integral, it is

$$B=\int_0^{1+p_0-p_1}\frac{(k-p_0+p_1)^2}{2}dk=\frac{1}{6}\left(1-p_1{}^3\right).$$

Finally, discrimination profits are just $A+B$, that turns out to be

$$A+B=\frac{1}{2}\left(\bar{k}-(1+p_0-p_1)\right)+\frac{1}{6}\left(1-p_1{}^3\right)$$

Therefore, Firm 0's profits are

$$\Pi_0=\bar{k}\left(p_0+\frac{1}{4}\right)-p_0{}^2+p_0\left(-\frac{3p_1{}^2}{2}+2p_1-1\right)+\frac{1}{3}(p_1-1)^3.$$

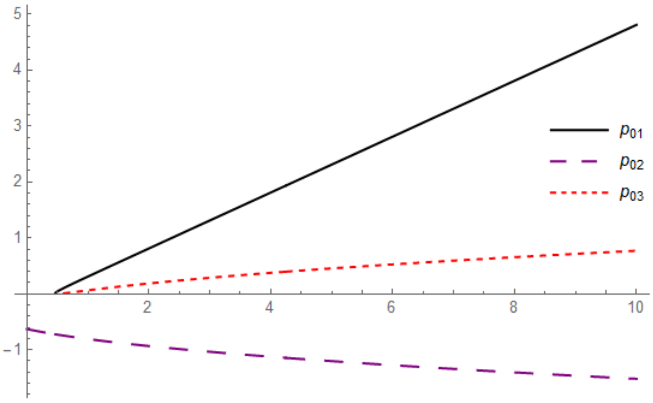
Firm 0's interest of selling information will be determined for the difference between the profits coming from it and those obtained in the standard monopoly i.e., $\pi_0^n=\bar{k}/4$.

Taking into consideration the $p_1\,(p_0)$ above specified, Firm 0's profits from the information selling scenario are

$$\Pi_0 = \frac{1}{12}\left(6\bar{k}(2p_0+1) - 2p_0\left(-2\psi + 4p_0\left(2p_0 - \psi + 3\right) + 3\right) - 3\right),$$

where $\psi = -\sqrt{2}\sqrt{p_0(2p_0+1)}$. If we draw the profits formula, we see that there exists a maximum point. The first order condition gives three possibles roots for Firm 0's price. Figure 7 draws the intuition behind them

Fig. 4.8 FOC Firm 0's price.



Two roots are positive. However, one of them is negative. As the maximum price, we consider the higher price between those that are positive. To see that, we can just take, for example, a fixed value for $\bar{k} = 1$. Then, as a result, we get that

$$\begin{cases} p_{01} = \frac{1}{4}\left(\sqrt{5}-1\right) \approx 0,3090 \\ p_{02} = \frac{1}{4}\left(-\sqrt{5}-1\right) \approx -0,8090 \\ p_{03} = \frac{1}{16} \approx 0,0625 \end{cases}$$

Therefore, p_{01} is the optimal price in equilibrium for the Firm 0 depending on the value of $\bar{k}$ and is given by

$$p_0^* = \frac{1}{48}\left(\phi + 8\bar{k} + \frac{16k(4\bar{k}+9)+57}{\phi} - 15\right). \tag{4.9}$$

and Firm 1's equilibrium price is,

$$p_1^* = \frac{1}{24}\left(\phi + 8\bar{k} + \alpha\right) - \rho \tag{4.10}$$

where,

$$\rho = \sqrt{\frac{1}{576}\left(\phi + 8\bar{k} + \alpha\right)^2 + \frac{1}{24}\left(\phi + 8\bar{k} + \alpha\right)},$$

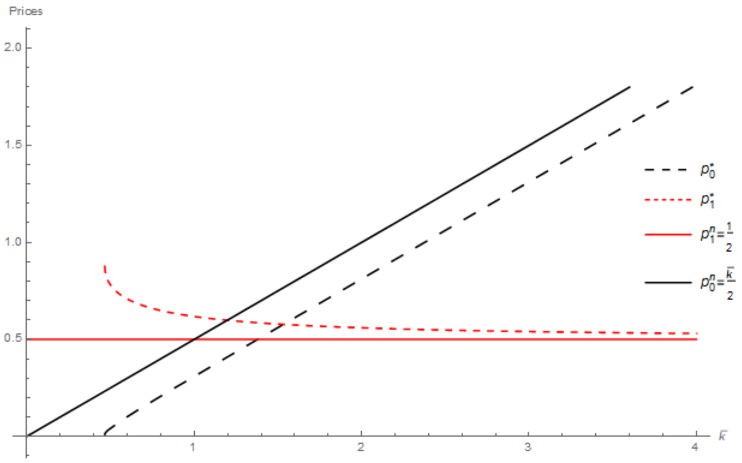
$$\alpha = \frac{16\bar{k}(4\bar{k}+9)+57}{\sqrt[3]{8\bar{k}(8\bar{k}(8\bar{k}-27)-225)+12\sqrt{3}\sqrt{-(4\bar{k}+1)^2(8\bar{k}(32\bar{k}(2\bar{k}+1)-13)-59)}-459}} - 15,$$

and

$$\phi = \sqrt[3]{8\bar{k}(8\bar{k}(8\bar{k}-27)-225)+12\sqrt{3}\sqrt{-(4\bar{k}+1)^2(8\bar{k}(32\bar{k}(2\bar{k}+1)-13)-59)}-459}.$$

We want to check whether: $p_1^* > 1/2$ and $p_0^* < \bar{k}/2$, and what is the distortion on prices with respect to the benchmark prices $\left\{p_0^n, p_1^n\right\} = \left\{\frac{\bar{k}}{2}, \frac{1}{2}\right\}$. Figure 4.9 shows the behaviour of prices depending on $\bar{k}$.

Fig. 4.9 Distortion on prices



Firm 0's price in equilibrium, p_0^*, is represented by the dashed black line in Figure 8. This price turns out to be lower than the benchmark's price $p_0^n = \frac{\bar{k}}{2}$. Therefore, the scenario where Firm 0 decides to sell its information about consumers, results in a lower level of its price. The idea is to fish as many consumers as possible in order to sell their information to Firm 1. As a consequence, Firm 1's price in equilibrium is higher than the benchmark price $p_1^n = \frac{1}{2}$, as can be seen in Figure 4.9. The dashed short line represents the equilibrium price for Firm 1 that gets closer to the price in the benchmark case (asymptotic behaviour) but it is always higher than p_1^n.

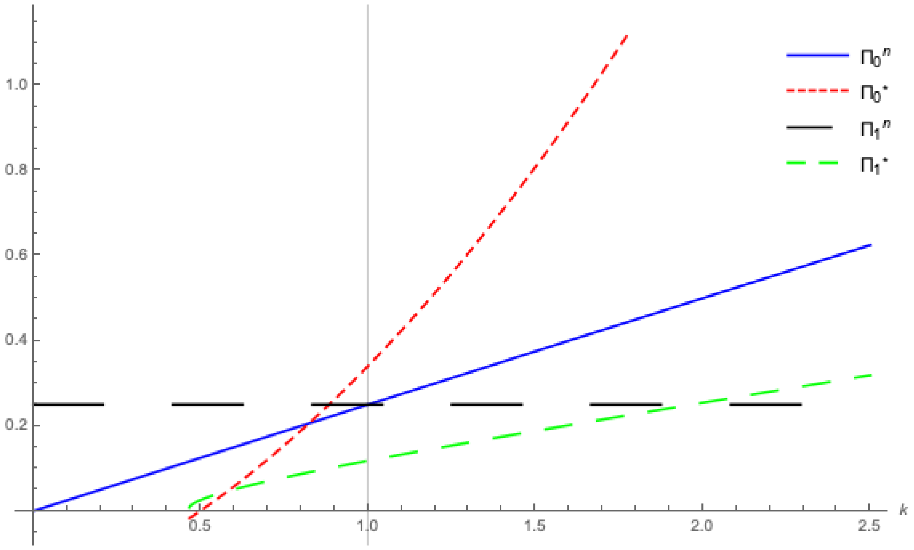
The following Proposition summarizes our findings:

Proposition 12 *Suppose that the consumers' valuations are distributed uniformly on* $[0,1]x\left[0,\bar{k}\right]$. *Then, Firm's 0 equilibrium price is lower than the scenario when there is not sale of information i.e,* $p_0^* < p_0^n$. *Firm's 1 equilibrium price is now higher than the benchmark's price, therefore, the sale of information results in* $p_1^* > p_1^n$.

Now we turn to analyze profits, and to check if there are incentives to sale information and, therefore, incentives to purchase them. Recall that Π_0^n and Π_1^n are profits for Firm 0 and Firm 1 under no sale of information, respectively. Fruthermore, let Π_0^* and Π_1^* be the profits under the sale of information for Firm 0 and Firm 1, respectively.

Firm 0's profits from the sale of information and no sale of information cross for a specific value of $\bar{k}$. Let $k' \approx 0.8$ be the value of the willingness to pay in the upstream market from which Firm 0's profits are higher than the benchmark's profits, $\Pi_0^n = \frac{\bar{k}}{4}$. In other words, $\Pi_0^* > \Pi_0^n$ for values big values for $\bar{k}$ (big market 0). In the same way, profits for Firm 1 shows a similar behaviour. Namely, profits coming from both scenarios also cross each other in a specific lever of k. Specifically, when $k > 1.9$ the profits from purchasing information are higher than those without information. Acquiring information makes sense if and only if the consumers' willingness to pay in market 0 , k, is big enough. A big market 0 means that information sharing would expands the downstream market 1 and, in this case, purchasing information is profitable for Firm 1. If, however, market 0 is small (low k), market 1's expansion does not take place and pricing low and selling as many consumers as possible can be better for the downstream Firm.

Fig. 4.10 Firms' profits under sale of info vs. no sale of info



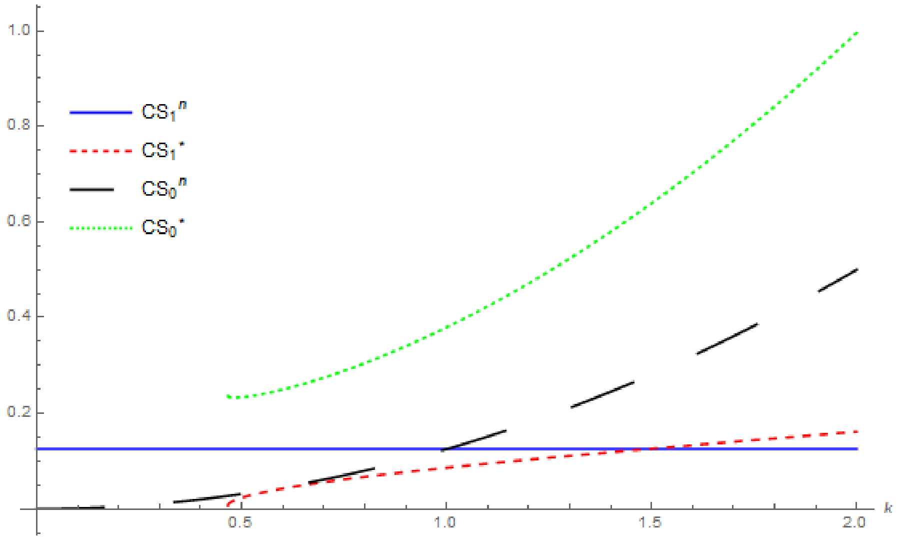
$\overline{k} \in (0, 2.5)$

Figure 4.10 represents plot both firms scenarios as a function of $\overline{k}$, the willingness to pay for the product in market 0, the upstream Firm. The vertical line isolates the case in which $\overline{k} = 1$, where Firm 0's profits are higher under the sale of information; however, for this precise value of k, Firm 1's profits are lower. Indeed, for values of $\overline{k} > 1.9$ both firms find it profitable the sale of information, given that profits are higher than under no sale of information at all.

We care now about the consumers'surplus and social surplus. The social surplus calculation simply revolves around whether the lost consumer's surplus from those consumers hiding their types by no longer buying at Firm 0, is made up by the extra surplus on those buying at Firm 1 and previously not purchasing it. For example, when the distribution of consumer valuations is uniform on the unit square, the discriminatory surplus on the mass of consumers (of mass 1/4) previously not buying is 1/8 per unit mass of total consumers, but the lost surplus on the mass of consumers (of mass 1/8) who hide is at most 1/8 per unit mass of total consumers.

In Figure 4.11, we plot the consumer surplus without sale of information from those who purchase from Firm 0 and Firm 1, CS_0^n and CS_1^n, respectively. Moreover, we plot the consumer surplus under the scenario of sale of information, CS_0^* and CS_1^*.

Fig. 4.11 Consumer's Surplus under sales of info vs. no sale of info

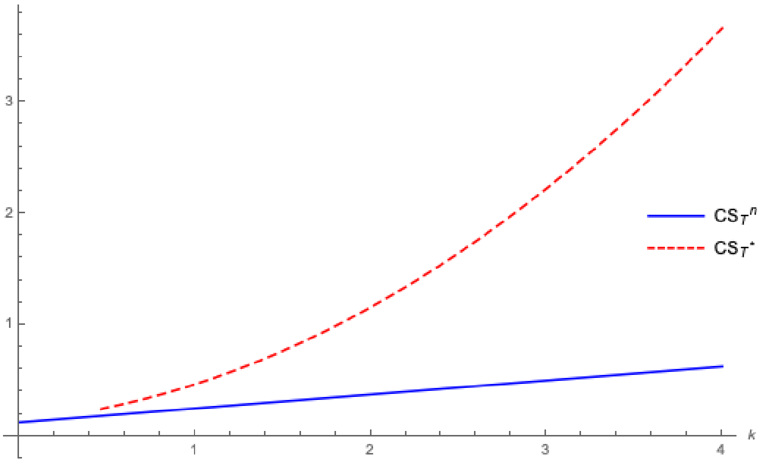


$\bar{k} \in (0,2)$

The following observations are nice to remark: i) Consumers purchasing from Firm 0, get higher consumer surplus under the sale of their information by Firm 0. This fact highlights, against what one might think, that they are better off when Firm 0 sells their information to Firm 1. This is due, to the reduction of Firm 0's price to induce consumers to buy. ii) Consumer who purchase from Firm 1, are better of when the upstream market is big anough (for high values of k), since in this case, there is a downstream market expansion and more consumers can buy from Firm 1.

If we analyze total consumer surplus, as Figure 4.11 shows, it can be seen that the sale of information generates higher consumer surplus i.e., $CS_T^* > CS_T^n$.

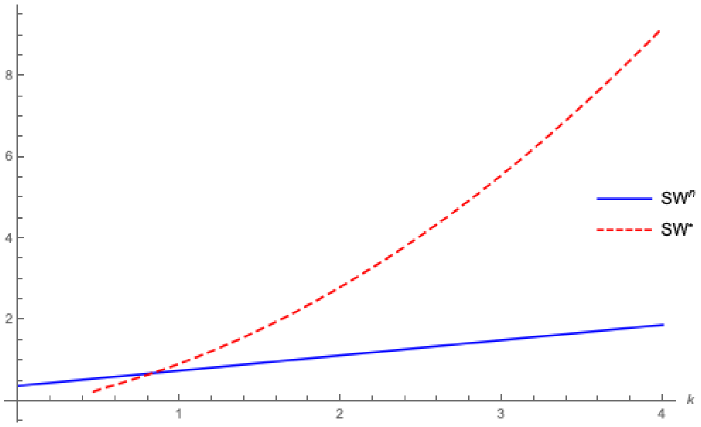
Fig. 4.12 Total Consumer' Surplus under sale of info vs. no sale of info



$\bar{k} \in (0,4)$

Finally, the analysis of social welfare, SW, reveals that allowing information selling translates into higher levels of SW, as can be seen on Figure 4.13.

Fig. 4.13 Social Welfare under sales of info vs. no sale of info



$\bar{k} \in (0,4)$

The above results are summarized in the following proposition:

Proposition 13 *Suppose that the consumers' valuations are distributed uniformly on* $[0,1]x\left[0,\bar{k}\right]$. *Then, information selling is good for everyone when it expands the downstream market, i.e., when it permits price discrimination that brings new consumers into the downstream market.*

By, itself this is good for welfare. And the incentive to profit on this information reduces to the upstream Firm to cut its price, expanding the upstream market, which is also good for welfare.

Note that giving consumers an opt-out option on having their information forwarded is surplus enhancing: no-one needs to hide, all those who bought both goods originally opt out, and the benefits of price discrimination accrue on the types with $k > p_0^n$ and $v < p_1^n$, who do not care whether their information is revealed because they got no surplus from Good 1 before since they were not buying it. We determine in Section 4.6.1 below how this conclusion is tempered when prices are endogenous.

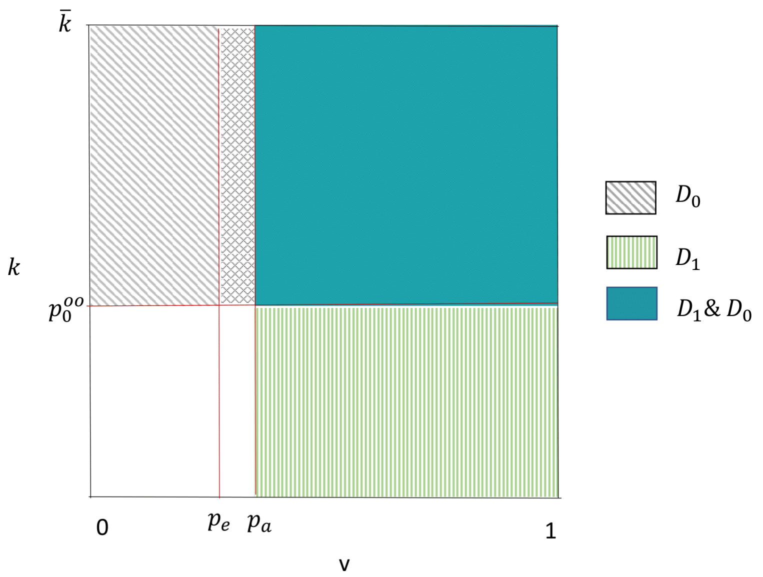
4.6 The demand for privacy-the demand for information

4.6.1 Consumers' Opt-Out

Suppose now that consumers when they buy good 0 from Firm 0 can choose whether they would like their information to be concealed or not.Those who would not buy otherwise will not opt out, and will be charged their valuation, v. But now those who would have hidden their types by not buying from Firm 0 will instead hide by opting out. This takes off the ability for Firm 0 to sell their information, but also restores their demand for Firm 0's primary product.

Figure 4.14 illustrates consumer behavior (the partition of the valuation space) when consumers anticipate the price of Good 1 to be p_e, and they have observed p_0. Recall the order of moves is: Firm 0 sets p_0; consumers choose whether or not to buy Good 0, and if so whether to opt-out of having their information shared; Firm 0 sells information to Firm 1 (notice here that it will transpire that Firm 1's profit in the absence of buying from Firm 0 is independent of Firm 0's actions, so we do not have to worry about default profits depending on Firm 1's actions); Firm 1 sets p_a for those for whom it does not have information;

Fig. 4.14 Opt-out option



consumers choose whether to buy good 1 from Firm 1, paying v if their information has been sold, and p_a otherwise. In equilibrium, $p_e = p_a = p_1$. We assume that consumers opt-out only if they are strictly better off doing so. This ensures that discrimination harvests all those with valuations $v < p_e$ and $k > p_0$.

Consumers in the south-west quadrant do not buy. In the north-west, they buy good 0 from Firm 0, and do not opt out, and so can be sold for discrimination. In the north-east they buy both goods, and opt out of sharing information about their (high) values for good 1. In the south-east they buy good 1 from Firm 1 only. Notice that for $p_a > p_e$ (as illustrated in Figure 4.14) consumers are lost along the full boundary $k = p_e$, in contrast to the case when there is no opt-out. We can now determine the equilibrium prices in the general model, and draw some welfare conclusions.

Proposition 14 *Suppose that the general model assumptions are satisfied. Then, the equilibrium prices with opt-out are $p_1^{oo} = p_1^n$, while $p_0^{oo} < p_0^n$. Total surplus is greater than without information selling, as so Firm 0's profits are.*

Proof. Firm 1's gross profits from sales of good 1 to consumers about whom it has no information are $p_a\left(1-G\left(p_a\right)\right)$. Note that this profit, and the maximizing price, is independent of p_0. The solution is therefore $p_1^{oo} = p_1^n$. Firm 0's profit is

$$\pi_0 = p_0\left(1-F\left(p_0\right)\right) + \left(1-F\left(p_0\right)\right)\int_0^{p_1} vdG$$

where the first term is profit from direct sales, and the second is its profit from selling information about the $\left(1-F\left(p_0\right)\right)G\left(p_1\right)$ consumers it has information on and have not opted out. Notice that the second term is an additional benefit per consumer served, and so is akin to a negative marginal cost. Thus $p_0^{oo} < p_0^n$. Total surplus is higher for 2 reasons: lower price for good 0 raises consumer surplus, and now there is too a surplus on the consumers with $v < p_1^n$. ∎

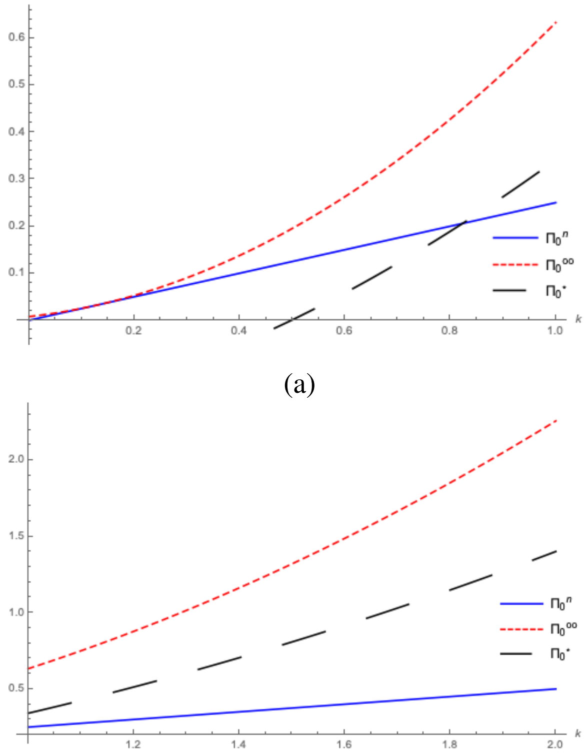
The calculus for Firm 1 is the same as without information selling because its marginal revenue from sales to the segment is the same. Firm 0 has the incentive to drop its price, because profits are increased by the extra profit on those consumers being discriminatingly priced. This leaves open the question whether Firm 0's profits are higher than without offering opt-out. To offer sharper conclusions we analyze the above question under uniuformly distributes consumers' valuations.

4.6.2 Uniform consumers' valuations

For the uniform case we have $p_1 = 1/2$. The condition for finding p_0 is from the maximization of $\pi_0 = \left(p_0 + \int_0^{p_1} vdG\right)\left(k-p_0\right) = \left(p_0 + \frac{p_1^2}{2}\right)\left(k-p_0\right)$; and hence $p_0 = \frac{1}{2}\left(k-\frac{1}{8}\right)$, so 0's equilibrium profit is $\pi_0^{oo} = \frac{1}{2}\left(k+\frac{1}{8}\right)^2$.

Furthermore, calculations yield $CS_0^{oo} = \int_{\frac{1}{2}\left(k-\frac{1}{8}\right)}^{k} \frac{1}{2}\left(k-\frac{1}{8}\right)\ dk = \frac{3k^2}{16} - \frac{k}{64} - \frac{5}{1024}$ and $CS_1^{oo} = \frac{1}{8}$.

We now turn to analyze Firm 0' profits under opt-out option. Firm 0's profits are higher when consumers decide to opt-out comparing with the case when the other cases, as can be seen in Figure 4.15. Selling consumer information may make the upstream firm worse-off, due to the price reduction to fish new consumers, and the loss of that consumers, who prefer not to buy in order to conceal their values in market 1. The upstream Firm may wish it could commit to not selling consumer information. When this is true, the upstream Firm benefits from free opt-out (since this amounts to a type of commitment device.)



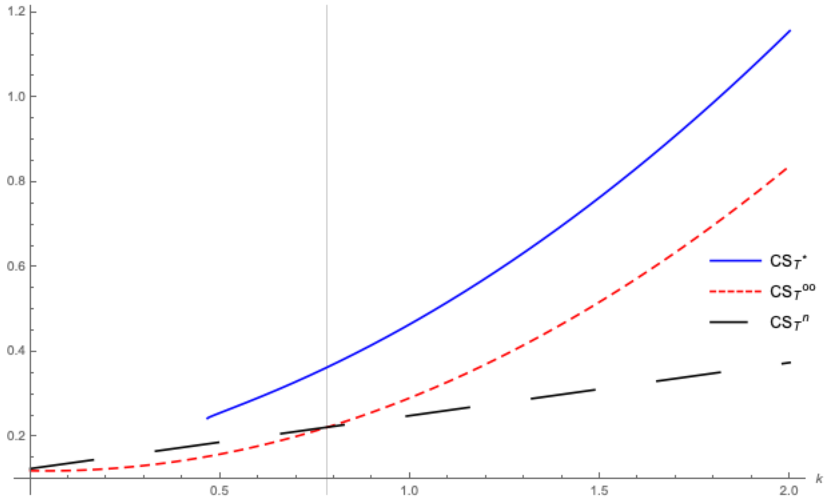
(a)

(b)

Fig. 4.15 In (a) $\bar{k} \in (0,1)$, and in (b) $\bar{k} \in (1,2)$.

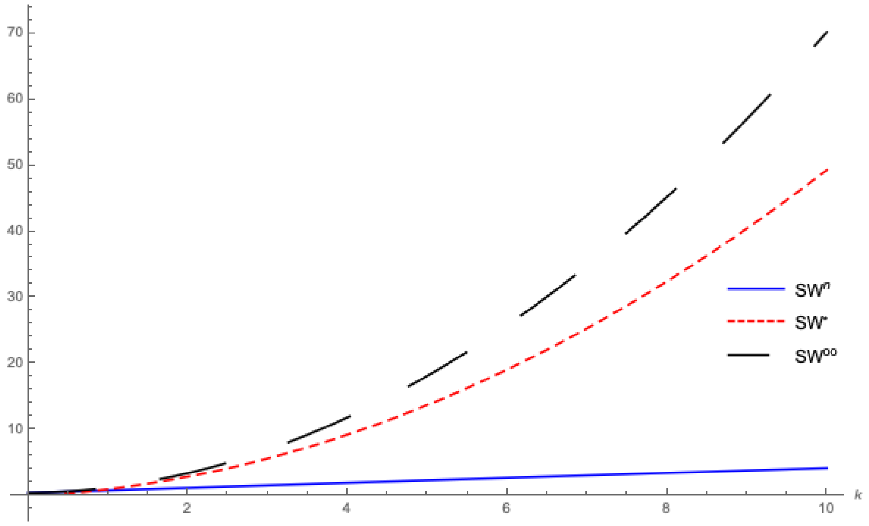
However, things go differently for the consumers' surplus under opt-out. In fact, consumers are better off under information selling than under opt-out. This is due to the effect of lower firm 0's prices. Figure 4.16 illustrates the levels of CS for different values of k. The vertical line shows the value of k, that is $\bar{k} = \frac{1}{24}\left(4\sqrt{6}+9\right)$, where the total consumer surplus from opt-out equals the total consumer surplus with no data-sharing policy. From that specific value of k, clearly the highest consumer surplus achieve is under data-sharing policy or the sale consumers' personal information.

Fig. 4.16 Consumer Surplus with Opt-Out option



Implications for social welfare, as can be seen in Figure 4.17, reaches the higher values with the opt-out option. This is due to the bigger effect of Firm 0's profits that more than compensated the consumers' effect. Consumers prefer info selling.

Fig. 4.17 Total Surplus with opt-out option



To better explain the intuition of the above result, we analyze next a simple example.

4.7 A more simple example

As above, consider two firms, Firms 0 and 1, which are monopolists in separate markets, but share a common pool of consumers. Therefore, there are 2 independent goods, each sold by a separate monopoly firm. Each consumer has value $v_0 \sim F[0,1]$ at upstream Firm 0 and $v_1 \varepsilon \{v_L, v_H\}$ at downstream Firm 1. The two types of consumer in market 1, have a mass of h for type v_H and of l for type v_L, with $h+l=1$.

The monopoly in the upstream market gathers information to sell it to the firm in the downstream market, where it is used to discriminate consumers. As above, this fact delivers endogenous demand for "hiding" (privacy) and model consequences in terms of economic primitives.

4.7.1 No information sharing benchmark

The upstream market

Let $F(v)$ be the fraction of v_0 with value below v and uncorrelated with downstream valuations. We assume that the $1-F(.)$ is strictly log-concave. Costs of production are suppressed for simplicity. For example, we could assume that $v_0 \sim U[0,1]$.[3] We also assume that when a consumer buys at Firm 0, then her type in market 1 is revealed and can be sold to Firm 1. With no information sharing, the equilibrium price in market 0 is simply the monopoly one that solve

$$p_0 = \frac{1-F(p_0)}{f(p_0)},$$

which in the case of the uniform distribution translates to $p=1/2$.

[3] Note that although consumers' valuations are uncorrelated between markets, information can still be used by firms.

The downstream market

With no information sharing, the downstream monopolist simply chooses: $p_1 = v_L$ (or $v_L > v_H h/(h+l)$) if $(h+l)v_L > hv_H$, and otherwise $p_1 = v_H$, or a mixed equilibrium.

To set the stage for the information analysis, suppose that Firm 0 were to sell information to Firm 1, and the information fully revealed the consumer's value in market 1. Then Firm 1 offers a perfectly discriminating full-surplus-extraction price to each consumer for whom it has information.

However, suppose for now that the price pair $\{p_0, p_1\}$ were fixed as above. Any consumer will now face the choice of hiding her information of her value for good 1 by not buying good 0, in the knowledge she would get no surplus from Good 1 should she buy Good 0. Then, let h^{NOT} the high types not outed, because they have not bought, or, indeed, are opting out of revealing, then, $p_1 = v_L$ if $v_L > v_H h^{NOT}/(h^{NOT} + l^{NOT})$. Note that the low types do not hide, therefore $l^{NOT} = lF(p_0))$.

The indifference condition will plays a key role in the Mixed Strategy equilibrium: second stage indifference requires that:

$$v_L(h^{NOT} + l^{NOT}) = v_H h^{NOT},$$

or

$$h^{NOT} = l^{NOT} v_L/(v_H - v_L).$$

4.7.2 The price of information

Now turn to the first stage, the information gathering in market 0, and selling it to the firm in market 1.

The price of information is the incremental profit to Firm 1, namely the extra it gets over not having information, which is $\pi_1^{NOINFO} = max\{v_L, hv_H\}$. Thus, Firm 0 offers a take-it-or-leave-it offer to Firm 1.

With the incremental profit identified as a transfer, Firm 0 makes a take it or leave it offer to Firm 1, and then we could analize the problem as if a single firm operates in both markets. However, this is not so. The wrinkle is that p_0 is set before p_1; consumers must rationally expect p_1 is set to maximize profits given how many consumers are left type-undetermined, and their composition.

4.7.3 Information sharing: Market 1 prices

As it is obvious, in market 1 there is no point to setting a price below v_L nor above v_H, or anywhere in between, though Firm 1 can randomize between v_L and v_H.

Let $Ep_1 = p_1^e$ be the price expected by consumers in market 1. This price must be accurately forecast in equilibrium, according to what Firm 1's incentives are, conditional upon the composition of unrevealed consumers.

Note that no L ever hides, that is, distort her purchases from Firm 0 to get a better surplus from Firm 1, either she is discriminated against, and gets all surplus extrated by firm 1, else she buys at price v_L and gets nothing then too.

To calculate the hiding H's, consider the gains of type H. They get either $v_0 - p_0$ and then 0 in market 1 because Firm 1 will charge discriminatorily $p_1 = v_H$, if they buy in market 0, or 0 if they do not buy in market 0 and then they will get (expect) $v_H - p_1^e$ in market 1. This defines the indifferent type, $v_0 = v_H - p_1^e + p_0$. Therefore, the fraction of H in the information gatheting market is $1 - F(v_0) = 1 - F(v_H - p_1^e + p_0)$, and the unreached H population has size: $h^{NOT} = hF(v_0) = h\left(F\left(v_H - p_1^e + p_0\right)\right)$.

4.7.4 Sub-game perfect bayesian equilibrium

We study subgame perfect (Bayesian) Nash equilibria of the model. For any subgame following a choice p_0, this implies that Firm 1's hidden price p_1 maximizes given correct beliefs about which consumers are hidden, and each consumer's decision at Firm 0 maximizes her total surplus, given correct beliefs about Firm 1's downstream pricing. At equilibrium, consumers' beliefs and firm 1's beliefs are correct.

In the first stage Firm 0 sets p_0. Consumers expect some p_1^e in market 1. In the second stage, Firm 1 wants to set that expected price, p_1^e. Let us show that there exists a unique p_1^e, which is in $[v_L, v_H]$. Also Fim 1 can mix between v_L and v_H if there is indifference between them. Recall that the indifference condition for Firm 1 is $v_H h^{NOT} = v_L(h^{NOT} + l^{NOT})$. If the left hand side is larger, then Firm 1 will prefer to set $p_1^e = v_H$, if the right hand side is greater, then Firm 1 will charge v_L. Rearranging the above indifference condition, we have $h^{NOT}/l^{NOT} = v_L/(v_H - v_L)$, and recalling that $l^{NOT} = lF(p_0)$ (i.e. L is indifferent to the price of Firm 1, since she gets zero surplus anyway) and that for the H's, $h^{NOT} = hF(v_0) = hF(v_H - p_1^e + p_0)$, then the indifference condition translates to:

$$h^{NOT}/l^{NOT} = hF(v_H - p_1^e + p_0)/lF(p_0) = v_L/(v_H - v_L),$$

that for the uniform distribution it specifies to:

$$h^{NOT}/l^{NOT} = h(v_H - p_1^e + p_0)/lp_0 = v_L/(v_H - v_L),$$

and hence the left hand side is decreasing in p_1^e (also decreasing in p_0)). Therefore, as a function of p_1^e in $[v_L, v_H]$:

If the left hand side is always above the line, then $p_1^e = v_H$; i.e., for $h/l > v_L/v_H - v_L$.

If the left hand side is always below the line, then $p_1^e = v_L$; i.e. for $h(v_H - p_1^e + p_0)/l(p_0) < v_L/v_H - v_L$ (and high p_0 can induce this regime-bring in relatively many Lows as hidden). Otherwise, an interior p_1^e and it decreases as p_0 rises to keep the ratio of non-purchasers constant).

Dowstream price

Once we have seen how the dowstream expected price reacts, we can look to the upstream one. Firm 0 chooses his price knowing how it affects the downstream one and which consumers are discovered for discrimination. Firm 0's problem is:

$$Max\pi = p_0(l(1-F(p_0))+h(1-F(v_0)))+ \\ v_Ll(1-F(p_0))+v_H(1-F(v_0))+p_1(p_0)\{IlF(p_0)+hF(v_0)\},$$

where $I = 1$ if $p_1(p_0) = v_L$ and $I = 0$ otherwise. Note that the first term is direct sales revenue, the second term is profits from direct discrimination and the third one is from the undetermined/unidentified. Also, note that the H's in the latter group buy if p_1 exceeds v_L. The function $p_1(p_0)$ encapsulates the second-stage incentives induced from the set of unouted. In equilibrium $p_1(p_0) = p_1^e$, as just seen.
Consider first the parameters inducing no mixing. That is $p_1(p_0) = v_L$ or $p_1(p_0) = v_H$. First $p_1(p_0) = v_L$.

Fishing for highs

Some H's want to hide strategically by not buying to Firm 0, even when they have positive surplus there: this is the lost sales effect. Firm 0 wants to harvest the H types to sell their information to Firm 1; it does it by reducing price -at least till we reach a point where the second stage incentive, with so many H in the hiding population, is to price above v_L (i.e., at v_H).

Replacing $p_1(p_0) = v_L$ in the firm maximization problem gives:

$$Max\pi = p_0(l(1-F(p_0)) + h(1-F(v_0))) + v_L l + h(1-F(v_0)) + v_L hF(v_0),$$

where in the second term, the same profit to Firm 1 comes from the L, who all buy at v_L one way ot the other, and the third term reflects the outed and hidden H's.
With the uniform distribution we have that the First Order Condition is:

$$l(1-p_0) + h(1-v_0) - (l+h)p_0 + hv_L - hv_H = 0,$$

with $v_H = (1 - 2h(v_H - v_L))/2$, which is decreasing in h: the monopolist in market 0 distorts choice on L's to harvest H's to sell its information to Firm 1. Therefore, the low type L's are happy, but not so clear for the high type H's. The H's are worse off through hiding costs and discriminated against, despite lower price in market 0. Also, we will see that Firm 0 also gets lower profits because of the hiding. In fact, the firm would like to commit "we will guarantee not to sell your information."

Notice too the end of this regime (highest h): where there are so many H's both hiding and in the population that Firm 0 will prefer to set a lower v_H to induce the mixed strategy regime.

Let π^{AUT} be the profits of the autarky regime (no information regime). With the uniform distribution $\pi^{AUT} = v_L + 1/4$ and $p_0 = 1/2$.

Recall that the high type H marginal consumer is $v_0 - p_0 = v_H - v_L \equiv T$. Then, write

$$\pi = h(p_0 + T)(1 - (p_0 + T)) + lp_0(1 - p_0) + v_L,$$

where the first T is an add-on value to getting each H-type. Hence, the First Order Condition gives: $h(1-2(p_0+T))+l(1-2p_0)=0$ or $p_0=1/2-hT$. Then, profits for Firm 0 become:

$$\pi^* = h(\frac{1}{4}-l^2T^2)+l(\frac{1}{4}-h^2T^2)+v_L \quad < \quad \pi^{AUT}.$$

Variants of this result appear in the behavioral-based price discrimination literature. Note also that π^* is decreasing in $h<1/2$.

On the other hand the high type consumers H are also hurt, despite the lower p_0. Let CS^{AUT} be the consumer surplus under autarky, then $CS^{AUT}=v_0-1/2+T$ if they buy, i.e., if $v_0>1/2$, they retain surplus in the later market, while $CS^{INFO}=v_0-1/2-hT$ if buy, again T if they do not. Thinking ahead to the opt-out regime, the H's choose to opt-out. Then, they scape the discriminatory pricing, but the firm has no incentive to fish for them. Therefore, the outcome is like autarky, with one crucial exception: as we will see below, the opt-out option induces a "quicker" change-over than autarky, to star fishing for the low types *Low* instead, so price goes up sooner to v_H! Therefore the opt-out can be worse for welfare! Does the lower p_0 enjoyed by the Lows exceed the lost profits and lowe h's CS. No, in the simulations.

Fishing for lows

Suppose now that there are many H in the population and that then, the downstream price is high, i.e., $p_1(p_0)=v_H$. Then, no H's wants to hide strategically by not buying at market 0, because they will never get a positive surplus from market 1.

However, Firm 0 wants to harvest L types to sell them to Firm 1. It does it by reducing price, but the more H's there are, the less it wants to reduce price because there are not many L's to profit from. Here no type gets any surplus in the second stage. Let $v_0=p_0$, the profit function becomes:

$$Max\pi = p_0(l+h)(1-F(p_0)) + v_L l(1-F(p_0)) + v_H h,$$

where the first term is market 0 direct revenue, the second term is discriminatoring profits from outed L's, and the third one is all the H's generated revenue v_H each.

The First Order Condition for the uniform is: $p_0 = (1-(1-h)v_L)/2$, increasing in h because fewer L's to try to attack.

Marriage made in heaven?

Note that h all better off than under autarky. Firm 0 sells information on Lows and then, market expansion means lower price p_0, benefitting all consumers. Higher profits from an extra consumer base and discriminatoy profits. The Lows's are not worse off from discrimination because otherwise they do not buy, they gain from lower p_0. No hiding in this regime. Terefore, this regime is good for all (especially for Firm 0), since the benefit from price discrimination that more are served.

What happens with "opting"? If consumers can opt-out, no-one strictly does it (even if in the limit the cost tends to zero).

Mixed strategy regime

We analyze lastly the regime of p_1 indifference. Here, the number of H's hiding depends on p_0 and p_1^e, which need to be consistent with inducing Firm 1 to mix. Firm 1 chooses optimally given this constraint. First, determine how many hiding: the indiffernce condition is: $v_0 - p_0 = v_H - p_1^e$, inducing $hF(v_0)$ hiders with $v_0 = v_H - p_1^e + p_0$, and then, Firm 1 has to be indifferent between the High and Low p_1^e's: $v_L(lF(p_0) + hF(v_0)) = v_H hF(v_0)$.

Solving for $v_0(p_0)$ and plogging it on the profit maximixation problem:

$$Max\pi = p_0(l(1-F(p_0)) + h(1-F(v_0)) + v_L l(1-F(p_0)) + v_H h,$$

where the last two terms come from the indifference propery of mixing. The First Order Condition for the uniform is:

$$l(1-p_0) + h(1-v_0) + p_0(-l - hdv_0/dp_0 - v_L l = 0,$$

and $v_L(lp_0 + hv_0) = v_H hv_0$ or $v_0 = p_0 v_L(1-h)/(v_H - v_L)$, which gives the price $p_0 = (v_H - v_L)(1 - v_L l)/2lv_H$. Notice that p_0 goes up with h and that v_0 is rising too, therefore, more hiding and more h population, so how are we indiffrent? Because the not-buying Low population is rising with h too! (recall that $h^{NOT} = l^{NOT} v_L/(v_H - v_L)$). To characterize the mixed strategy equilibrium note that we have p_1^e rising with h towards v_H and likewise p_0. Hence, from price behavior, CS is lower for H and L. This is because, H's exert negative preference externality on themselves and on L's. The H's opt out because they know they do not want to pay $p_1 = v_H$.

4.7.5 Which regime?

If mainly L's in the population, we have $p_1^e = v_H$. If mainly H's in the polulation, we have $p_1^e = v_L$. In the middle, we have a mixed strategy equilibrium. What happens to p_0 at regime switches?. Recall that p_0 drives the regime type through it effect on p_1^e. We have firsy a regime with $p_1 = v_L$, then jumps to the mixed strategy equilibrium (with p_1^e raising, and then $p_1 = v_H$. Then, first p_0 drops with h, then it takes a jump dpwn to the mixed strategy regime. It then rises with h through the mixed strategy equilibrium regime, and then rises slower in the $p_1 = v_H$ regime, but is continuous through the switch there.

Opt-out regime analysis

Proceeding as above, consider 2 regime types, low and high h, and that there in nothing in between (no mixed regime). Note that the H's always opt-out if they expect a price lower than v_H. If we have a high h: the same than the original regime, $p_1 = v_H$, with just the same price p_0: there are many H's and Firm 0 only want to harvest the Low. It is irrelevant whether the H's opt-out or not, since they get no surplus, and firm 1 gets v_H from each of them. Therefore, the outcomes are equivalent.

For low h, the H's opt-out, then, because this regime was formerly driven solely from harvesting H's there is no reason to drop price to get more of them to sell (they have no incremental value). Therefore the price is the monopoly price till the regime switches.

Switch-point under opt-out

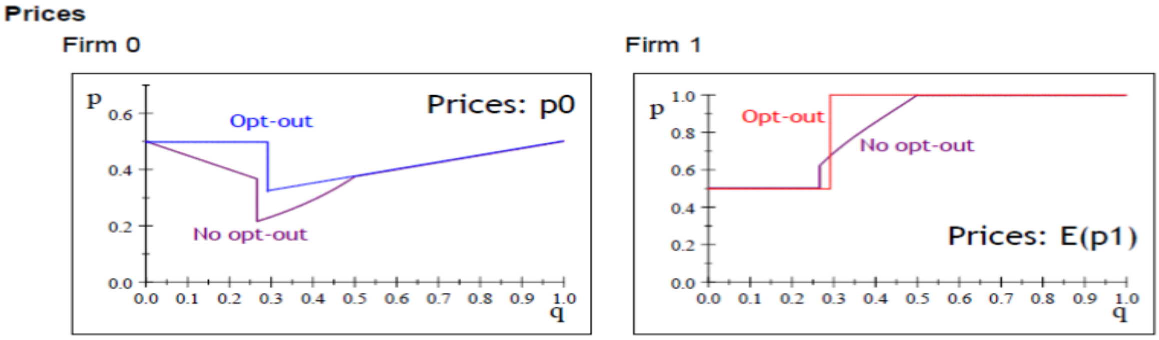
Compare to autarky: with opt-out, there is no fishing-for-higs, only fishing-for-lows, and the latter is more profitable than autarky (conditional on $p-1 = v-H$). Therefore, the switch-point is earlier than the autarky one. And, locally, lowers welfare because the negative externality on H's CS when switch and raise their price.

Pulling together

We summarize next the different regimes with some pictures coming from broad simulations. Let q be the proportion of high types. The diagrams below are equilibrium results, upstream and dowstream prices as a function of q, for $v_h = 1$ and $v_l = \frac{1}{2}$.

Figure 4.18 indicates that Firm 1 goes from low to high price, as q increases, with mixed strategy equilibrium for intermediate valuesof q. The autarky price is $p_1^e = 1/2 = v_L$ for $h < 1/2$, and $p_1^e = 1 = v_H$ otherwise. Thus, intermediate range has higher p_1^e under information-selling: hiding population has more H's. The no-opt-out strategy takes a jump up as switch into the mixed equilibrium regime (induced by a jump down in p_0 to fish for

Fig. 4.18 A more simple example: Prices



Highs). For Firm 0 the autarky price is $p_0 = 1/2$, therefore, information-gathering always lowers prices in market 0 to seek either lows (high h) or highs (low h) to sell. With no opt-out we see lower and decreasing prices at first; bringing in Highs to sell them.

Figure 4.19 shows the two-type consumer's surplus. Low types are happy with selling information since they gain from lower prices in the gathering market, and they get nothing anyway in the other. No opt-out is better for them because opt-out doesn't have fishing for Highs to sell (low h). Opt-out still beats autarky because then (high h) there is Fishing for Lows. The High types suffer when they are few from information-gathering, for they distort by hiding; even they are better off for high h (when there's Fishing for Lows).

Fig. 4.19 A more simple example: Consumers' surplus

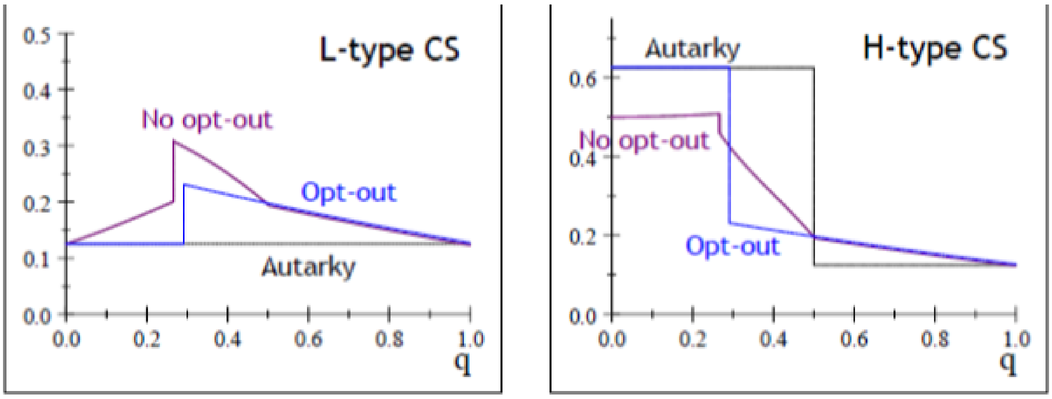
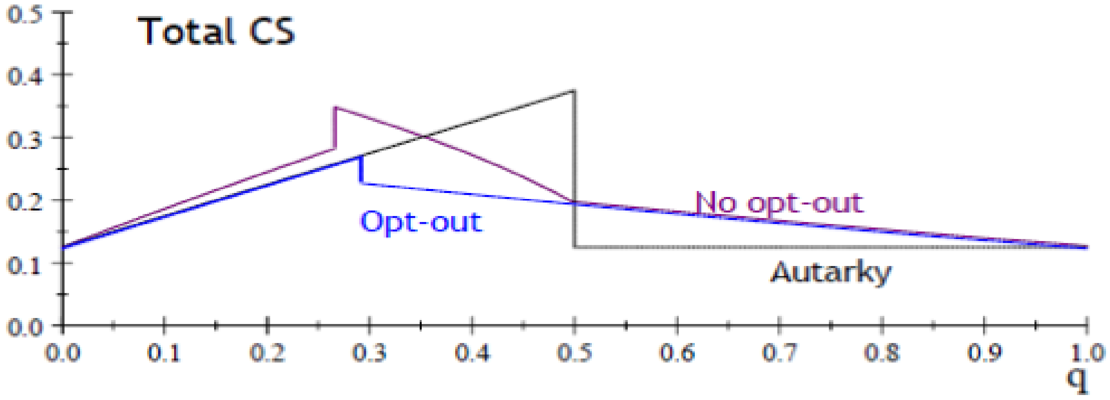


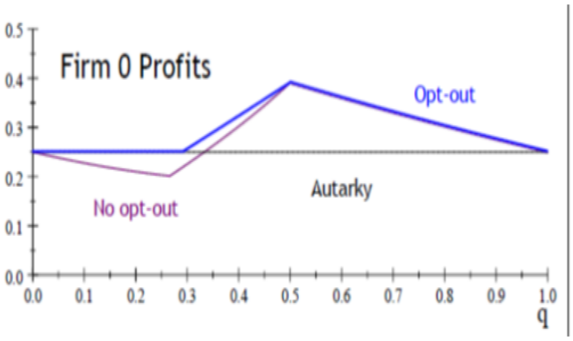
Figure 4.20 shows that everyone better off (high h) when information is sold. Also opt-out might hurt (relative to No opt-ot) and even relative to autarky. The reason is that opt-out

Fig. 4.20 A more simple example: Total Consumers' surplus



hurts in middle because firm switch "sooner" to v_H (because H's are opting out). Later is benefit from fishing for L's, gives low prices. Notice Opt-In (=autarky) can be best!

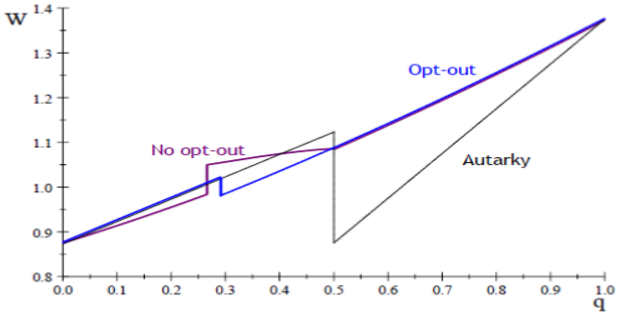
Fig. 4.21 A more simple example: Firm 0 profits



The display of Firm 0 profits in figure 4.21 says that no opt-out hurts Firm 0's profits at first relative to autarky, therefore, here firm would like to guarantee it will not sell your data, for fear of too much loss from hiding in the info-gathering market 0 (note that setting the autarky prices doesn't help, because consumers know they will still be sold, and therefore, avoid buying). Opt-out can actually raise profit, when the No-opt-out choice is in the mixed strategy regime. Never (strictly) prefers Opt-In.

With regard to the Total Welfare, note that each can be at their best: high h, selling information is good for all groups involved, but, low h, all are hurt. There is a conflict zone

Fig. 4.22 A more simple example: Total Welfare



in the middle range; firms like it, but (aggregate) consumers do not. They especialy dislike the opt-out regime, which firm prefers!

Summing up the upstream firm would like the following. In the first place, to guarantee not to sell data if the proportion of High's is low. This can be attained with opt-out. However, consumers of the Low type are happy if Firm 0 cannot commit since the firm Fishes for Highs by lowering the information-market price. However, the High ones are adversely impacted, either they hide or pay a high downstream market price, when they do not hide. In the second place, Firm 0 would like to sell information and use opt-out in the middle. Here, the$L$ types are happy, but the H types are hurt, especially under opt-out since they face a high price in the downstream market. Finally, Firm 0 wants to sell information for high H. In this case, consumers are happy too.

4.8 Conclusions

The first result that we conclude from the example is that information sharing is good for everyone when it expands the downstream market. Clearly, if high value types are common enough that the downstream firm would sell only to them, then information sharing will permit price discrimination that brings new consumers into the downstream market. By, itself this is good for welfare. And the incentive to profit on this information reduces to the upstream Firm to cut its price, expanding the upstream market, which is also good for welfare. This has been also seen in the general model.

Furthermore, the second result from the example is that information sharing, with or without opt-out, is a mixed bag when the downstream market already operates efficiently at autarky. For example, when low types are common, the downstream Firm would price low and sell to everyone. With information sharing, downstream welfare can only fall; upstream welfare may rise if the upstream Firm cuts its price, expanding the upstream market. One effect of the other can dominate.

The above result is clear under consumers' valuations uniformly distributed, where selling consumer information may make the upstream firm worse-off: the upstream Firm may wish it could commit to not selling consumer information. When this is true, the upstream Firm benefits from free opt-out (since this amounts to a type of commitment device.)

The fourth results coming from the example is that if the downstream market would otherwise be efficient, information sharing with no opt-out will act a bit like a transfer of consumer surplus from consumers with high downstream values to consumers with low downstream values. Loosely, the channel is that upstream prices falls and average downstream price rises. The latter hurts downstream high types relatively more, whether they face the "pool" price or a fully-extracting discriminatory price. And lower upstream prices help the downstream types relatively more.

Finally, set information sharing with no opt-out as a benchmark. Changing the rules to permit free opt-out never improves aggregate consumer surplus. Indeed, free opt-out reduces aggregate consumer surplus if the downstream market would be efficient under autarky. Expanding on this last point, it is possible that the option to opt-out may hurt all consumer types, including the high-value downstream consumers who exercise the option most eagerly.

Chapter 5

Conclusions

5.1 Conclusions

This thesis contributes to the study of the implications of privacy concerns in the optimal decisions of economic agents in digital markets, from a theoretical point of view. Given the great appearance of news on this topic and their impact in the society, we answer queries regarding to firms' retailing strategies, cybersecurity and trust when consumers have an argument inside in their utility function about their privacy concerns. Furthermore, we get insight about the implications of regulation policies (privacy policies) available to consumers and the social welfare coming from these regulations.

In Chapter 2, a monopolist operates in a dual-channel context, brick and click channels. She has to decide whether to practise price discrimination over channels or not. In particular, those consumers purchasing the product through the online channel have privacy concerns. Thus, in a dynamic setting, consumers and the monopolist are learning from the signals in the market. Signaling may distorts prices upwards or downwards with respect to the ones in the full information scenario. We find out that the monopolist gets higher expected profits under channel-based price discrimination. Furthermore, it does exist price dispersion over channels, much in line with the literature. Nevertheless, price dispersion depends on the average-population privacy concerns in the market, and there is not a clear behaviour in which channel the price is higher or lower. The existence of consumers' privacy can be understood as a possible explanation of the dispersion on prices, and a key factor for the design online. On the other hand, the existence of less experimented consumers in the market i.e., the presence of consumers that only have purchased in one period or are new in the market, may harm the social welfare. Indeed, the presence of more experienced consumers about their privacy concerns is social welfare improving, thus, the higher control that consumers have about their information, the more the welfare that can be achieved in the marketplace.

Chapter 3 analyzes the model in Chapter 2 assuming the monopolist's decision to invest in security in order to decrease consumers' privacy concerns, and as a way to increase profits. This study comes from the actual need for firms to signal their commitment in security and protection of consumers' information. The Chapter presents two investment approaches, a direct investment in security in period 1, and an investment in the signal precision. We get that the monopolist finds it profitable to invest in both approaches. Firstly, the first approach results in a transfer of the cost directly to consumers through the price. Secondly, investment in signal precision transfers the control of information in the market to the monopolist. We conclude that it would be preferable to grant the monopolist a certain power of information because doing so would result in lower prices. This power translates to market manipulation, specifically, of the signal's precision of the information in the market. Given this result, we also investigate when the monopolist's capacity to manipulate is higher when she faces different cost functions of investments. As a result, under linear cost function, the monopolist has greater incentives to manipulate the signal's precision, and it is possible to do so with c small (cheaper). However, if the monopolist faces convex cost functions, signaling lower signal's precision is more expensive, and therefore, manipulation is more costly.

Chapter 4 explores consumers' endogenous decision to remain "hidden" to not having their information sold. This possibility to opt-out and/or to opt-in are the main options that consumers have as a result of the different legislations nowadays, e.g., GDPR in Europe and particular regulations in the US. Furthermore, we render the acquisition and sale of information to be endogenous in a context of two successive monopolies: an upstream firm or a firm in market 0, and a downstream firm or in market 1. Three main privacy-policy are studied: autarky (no sale of information is permitted), data-sharing (sale of information is permitted), and opt-out option (consumers' endogenous decision to protect their info). We find that information sharing is good for everyone when it expands the downstream market. However, under consumers' valuations uniformly distributed, selling consumer information may make the upstream company worse off, thus, the upstream firm may wish it could commit to not selling consumer information when the willingness to pay for the upstream product is low. Interestingly, selling consumer information renders higher consumer surplus than no letting the sale of information to the market. Finally, changing the rules to permit free opt-out never improves aggregate consumer surplus, and it is possible that the opt-out may hurt all consumer types, as can be seen in the simple example. However, the existence of an opt-out option might improve social welfare, and thus, this may justify the final purpose of these regulations.

Our results emphasize the importance of privacy concerns in decision-making for all the participants in the market. Furthermore, our conclusions are consistent with the development of regulations and policies in order to construct safe digital markets. However, the enforcement of a set of rules (like GDPR or privacy shield in the US) may not actually be beneficial for consumers. On the other hand, if firms decide to invest in security, it may lead to abuse of position and market manipulation. The control of the information and regulations in the market are developed to guarantee consumers' privacy and protection of their information. However, the final outcomes derived from them are still subject to an economic and moral controversial. In words of Taylor and Wagman (2014), "regulation policies have to be individualized to each specific markets". Regulations, yes, but only for when it is really necessary and done in a controlled manner, and more importantly, for specific markets.

Conclusiones

Esta tesis contribuye al estudio de las implicaciones que las preocupaciones por la privacidad tienen en la toma de decisiones óptimas de los agentes económicos en los mercados digitales, desde un punto de vista teórico. Dada la gran emergencia de noticias sobre este tema, y el impacto que tienen en la sociedad, respondemos preguntas relacionadas con las estrategias de ventas de las empresas, ciberseguridad y confianza, cuando los consumidores presentan un argumento sobre estas inquietudes en su función de utilidad. Además, hemos obtenido una comprensión más profunda de las políticas de regulación (políticas de privacidad) disponibles para los consumidores, así como la implicación de las mismas en el bienestar social.

En el Capítulo 2, un monopolista opera en dos canales de venta, «brick and click channels», mercado tradicional y en Internet. El monopolista tiene que decidir si practicar discriminación de precios entre canales o no hacerlo. Bajo este marco, los consumidores que compran sus productos por Internet presentan un argumento en su utilidad que representa sus inquietudes por la privacidad. En un entorno dinámico, los consumidores y el monopolista aprenden de las señales del mercado. La presencia de dichas señales puede distorsionar los precios si los comparamos con los precios bajo un escenario de información completa. Obtenemos que el monopolista consigue mayores beneficios si practica discriminación de precios entre canales. Además, encontramos que existe dispersión de precios entre canales, muy en línea con la literatura. Esta dispersión en los precios depende de la privacidad media de los consumidores en el mercado, y no existe un claro comportamiento que indique que los precios en un canal sean mayores o menores que en el otro canal. La existencia de inquietudes por su privacidad, por los consumidores, puede ser entendido con una posible explicación de la dispersión en los precios, un factor clave para el diseño de precios en Internet. Por otro lado, la existencia de consumidores menos experimentados en relación con sus posibles inquietudes en este mercado, es decir, consumidores que solo han comprado en un periodo o son nuevos en el segundo periodo, puede perjudicar al bienestar social. De hecho, la presencia de consumidores que tengan más información acerca de sus valoraciones individuales por privacidad, incrementa el bienestar social. Por lo tanto, podemos concluir, que cuánto más control tengan los consumidores acerca de su información, y por tanto, de cuanto valoran su privacidad, mayor será el bienestar social que puede alcanzarse en el mercado.

El Capítulo 3 analiza el modelo presentado en el Capítulo 2, pero estudiando la decisión del monopolista de invertir en seguridad con la finalidad de atenuar las inquietudes por privacidad de los consumidores y, por tanto, aumentar sus beneficios. El análisis realizado en este capítulo responde a la actual necesidad que tienen las empresas de mostrar sus compromisos en seguridad y protección de la información de los consumidores. Este Capítulo presenta dos formas de inversión, i) una inversión directa en seguridad en el periodo 1, y ii) la inversión en la precisión de la información. Como resultado general, el monopolista encuentra beneficioso invertir en las dos formas de seguridad. Por un lado, la primera forma de inversión resulta en una transferencia del coste directamente a los consumidores a través del precio. Por otro lado, la segunda forma transfiere el control de la información en el mercado al monopolista. Concluimos que sería preferible otorgar al monopolista cierto poder de la información porque esto resultaría en un nivel menor de precios. Este poder se refiere a la manipulación de la señal de mercado, concretamente, manipulación en la precisión de dicha señal. Dado esto, investigamos además cómo es la capacidad manipuladora del monopolista cuando se enfrenta a diferentes estructuras de costes. En particular, cuando el monopolista se encuentra bajo unos costes de inversión en la precisión que son lineales, la manipulación en el mercado se puede conseguir de una manera más barata. Sin embargo, cuando el monopolista se encuentra bajo unos costes convexos, establecer un menor nivel en la precisión para poder así manipular el mercado, es mucho más costosa. En definitiva, la capacidad manipuladora se puede ver reducida.

Encontramos que los incentivos por manipular la información en el mercado pueden verse muy aminorados si el monopolista se enfrenta a determinadas funciones de costes convexas. Sin embargo, cuando el monopolista está sujeto a una función de costes lineal, los incentivos a elegir una precisión de la señal baja son muy grandes. Esta baja precisión da lugar a que los consumidores crean que la información que tiene el monopolista es peor de la que realmente es. Por tanto, con esto consigue que los consumidores den más importancia a su señal privada (experiencias previas en cuanto a privacidad) y menos a la señal pública (precios), y con ello, los ingresos marginales del monopolista se ven incrementados.

El Capítulo 4 explora la decisión endógena de los consumidores a permanecer "anónimos" para no vender su información. Esta posibilidad de optar o no optar por el anonimato son las principales opciones que los consumidores tienen como resultado de las diferentes legislaciones hoy en día, como por ejemplo, RGPD en Europa u otras legislaciones en los EE.UU. Además, modelizamos la adquisición y venta de la información de forma endógena en un contexto de dos monopolios sucesivos: una empresa «upstream» o en el mercado 0, y una empresa «downstream» o en el mercado 1. Contemplamos tres políticas de privacidad: autarquía (la venta de información no está permitida), política de intercambio de datos (la venta de información está permitida), y la posibilidad de optar por vender sus datos (decisión endógena de los consumidores para proteger su información). Obtenemos que el intercambio o venta de información es beneficioso para todos cuando expande el mercado «downstream» o mercado 1. Sin embargo, bajo el escenario de las valoraciones de los consumidores distribuidas uniformemente, vender la información de los consumidores podría empeorara la empresa en el mercado 0, por ello, la «upstream» preferiría no comprometerse a vender la información de los consumidores si la máxima valoración del consumidor por su producto fuera baja. Curiosamente, la venta de información de los consumidores da como resultado un mayor bienestar para los consumidores que en el caso de la no venta de información. Finalmente, cambiar las reglas en el mercado para permitir libre «opt-out option» nunca mejora el bienestar agregado de los consumidores, y es posible que esta política perjudique a todos los tipos posibles de consumidores, un resultado obtenido del ejemplo elaborado en este capítulo. Sin embargo, la existencia de una «opt-out option» puede aumentar el bienestar general, y esto, podría justificar el objetivo final de las regulaciones en el mercado.

Nuestros resultados enfatizan la importancia por las inquietudes por la privacidad en la toma de decisiones para todos los participantes en el mercado. Además, las conclusiones alcanzadas son consistentes con el desarrollo de regulaciones y políticas para construir un mercado digital seguro. Sin embargo, la aplicación de un conjunto de normas (por ejemplo, las desarrolladas en el RGPD o diferentes legislaciones de los EE.UU) podrían no ser en realidad beneficiosas para los consumidores. Por otro lado, si las empresas deciden en invertir en seguridad, podría dar lugar a una situación desfavorable para los consumidores, como puede ser abuso de poder y manipulación del mercado. El control de la información y las regulaciones en el mercado están siendo desarrolladas para garantizar la privacidad y protección de la información de los consumidores. No obstante, los resultados finales derivados de los mismos están todavía sujetos a controversia económica y moral. En palabras de Taylor and Wagman (2014), “las políticas de regulación tienen que ser individuales y específicas a cada tipo de mercado”. Podemos concluir diciendo sí a la regulación, pero sólo cuando sea realmente necesario, se lleve a cabo de manera controlada, y lo que es más importante, para mercados específicos.

References

Acquisti, A., Taylor, C., and Wagman, L. (2016). The Economics of Privacy. *J. Econ. Lit.*, 54(2):442–492.

Acquisti, A. and Varian, H. R. (2005). Conditioning Prices on Purchase History. *Mark. Sci.*, 24(3):367–381.

Ahmad, N. and Schreyer, P. (2016). Measuring GDP in a digitalisation economy. pages 22–26.

Anderson, R. (2001). Why Information Security is Hard. *Annual Computer Security Applications Conference*.

Angst, C. M., Block, E. S., and D'Arcy, John Kelley, K. (2017). When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches. *MIS Quarterly*, 41(3):893–916.

Armstrong, M. (2015). Search and ripoff externalities. *Review of Industrial Organization*, 47(3):273–302.

Belleflamme, P., Lam, W. M. W., and Vergote, W. (2017). Price discrimination and dispersion under asymmetric profiling of consumers.

Belleflamme, P. and Vergote, W. (2016). Monopoly price discrimination and privacy: The hidden cost of hiding. *Econ. Lett.*, 149:141–144.

Bergemann, D. and Bonatti, A. (2015). Selling cookies. *Am. Econ. J. Microeconomics*, 7(3):259–294.

Bounie, D., Dubus, A., and Waelbroeck, P. (2018). Selling strategic information in digital competitive markets.

Boyd, D. (2010). Social network sites as networked publics: Affordances, dynamics, and implications. In *A networked self*, pages 47–66. Routledge.

Brandeis, L. and Warren, S. (1890). The right to privacy. *Harvard law review*, 4(5):193–220.

Braulin, F. C. and Valletti, T. (2016). Selling customer information to competing firms. *Economics Letters*, 149:10–14.

Calzolari, G. and Pavan, A. (2006). On the optimality of privacy in sequential contracting. *J. Econ. Theory*, 2(2):168–204.

Campbell, M. C. and Campbell, C. (2010). Perceptions of Price Unfairness : Antecedents and. *J. Mark.*, 36(2):187–199.

Casadesus-Masanell, R. and Hervas-Drane, A. (2015). Competing with privacy. *Management Science*, 61(1):229–246.

Cases, A. S., Fournier, C., Dubois, P. L., and Tanner, J. F. (2010). Web Site spill over to email campaigns: The role of privacy, trust and shoppers' attitudes. *Journal of Business Research*, 63(9-10):993–999.

Cavallo, A. (2017). Are Online and Offline Prices Similar? Evidence from Large . *Am. Econ. Rev.*, 107(1):283–303.

Cavusoglu, H., Raghunathan, S., and Yue, W. T. (2008). Decision-theoretic and game-theoretic approaches to it security investment. *Journal of Management Information Systems*, 25(2):281–304.

Chaudhry, A., Crowcroft, J., Howard, H., Madhavapeddy, A., Mortier, R., Haddadi, H., and McAuley, D. (2015). Personal data: thinking inside the box. In *Proceedings of the fifth decennial Aarhus conference on critical alternatives*, pages 29–32. Aarhus University Press.

Chellappa, R. K. and Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management*, 15(5/6):358–368.

Chen, Y. and Zhang, Z. J. (2009). Dynamic targeted pricing with strategic consumers. *Int. J. Ind. Organ.*, 27(1):43–50.

Chen, Z., Choe, C., and Matsushima, N. (2018). Competitive personalized pricing.

Chiang, W.-y. K., Chhajed, D., and Hess, J. D. (2003). Direct Marketing, Indirect Profits: A Strategic Analysis of Dual-Channel Supply-Chain Design. *Manage. Sci.*, 49(1):1–20.

Choe, C., King, S., and Matsushima, N. (2017). Pricing with cookies: behavior-based price discrimination and spatial competition. *Management Science*, 64(12):5669–5687.

Conitzer, V., Taylor, C. R., and Wagman, L. (2012). Hide and Seek: Costly Consumer Privacy in a Market with Repeat Purchases. *Marketing Science*, 31(2):277–292.

Cuellar, S. S. and Brunamonti, M. (2014). Retail channel price discrimination. *J. Retail. Consum. Serv.*, 21(3):339–346.

Daniel, J. S. (2006). A taxonomy of privacy. *University of Pennsylvania law review*, 154(3):477–560.

DeGroot, M. H. (2005). *Optimal statistical decisions*, volume 82. John Wiley & Sons.

Dor, D. and Elovici, Y. (2016). A model of the information security investment decision-making process. *Computers and Security*, 63:1–13.

Eastlick, M. A., Lotz, S. L., and Warrington, P. (2006). Understanding online b-to-c relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research*, 59(8):877–886.

Esteves, R.-B. (2010). Pricing with customer recognition. *International Journal of Industrial Organization*, 28(6):669–681.

Fenz, S., Ekelhart, A., and Neubauer, T. (2011). Information security risk management: In which security solutions is it worth investing? *Article*, 28(1):329–356.

Fruchter, G. E. and Tapiero, C. S. (2005). Dynamic online and offline channel pricing for heterogeneous customers in virtual acceptance. *Int. Game Theory Rev.*, 07(02):137–150.

Fudenberg, D. and Tirole, J. (2000). Customer poaching and brand switching. *RAND Journal of Economics*, pages 634–657.

Fudenberg, D. and Villas-Boas, J. M. (2012). In the digital economy. *The Oxford handbook of the digital economy*, page 254.

Gordon, L. A. and Loeb, M. P. (2006). Budgeting process for information security expenditures. *Communications of the ACM*, 49(1):121–125.

Grubb, M. D. (2015). Behavioral Consumers in Industrial Organization: An Overview. *Rev. Ind. Organ.*, 47(3):247–258.

Hilbert, M. (2012). How Much Information is There in the information society? *Significance*, 9(4):8–12.

Holvast, J. (2007). History of privacy. *Hist. Inf. Secur.*, pages 737–769.

Hughes, T. and Saverice-Rohan, A. (2018). IAPP-EY Annual Privacy Governance Report 2018. *Iapp-Ey*, pages 1–132.

Iyer, G. and Soberman, D. (2000). Markets for product modification information. *Marketing science*, 19(3):203–225.

Johnson, G., Shriver, S., and Du, S. (2017). Consumer privacy choice in online advertising: Who opts out and at what cost to industry?

Judd, K. L. and Riordan, M. H. (1994). Price and Quality in a New Product Monopoly. *Rev. Econ. Stud.*, 61(4):773–789.

Kasneci, D. (2008). Data protection law: recent developments.

Kunreuther, H. and Heal, G. (2003). Interdependent security. *Journal of risk and uncertainty*, 26(2-3):231–249.

Li, G., Huang, F., Cheng, T. C., and Ji, P. (2015a). Competition between manufacturer's online customization channel and conventional retailer. *IEEE Trans. Eng. Manag.*, 62(2):150–157.

Li, Z. E., Lu, Q., and Talebian, M. (2015b). Online versus bricks-and-mortar retailing: A comparison of price, assortment and delivery time. *Int. J. Prod. Res.*, 53(13):3823–3835.

Manshaei, M. H., Zhu, Q., Alpcan, T., Bacşar, T., and Hubaux, J.-P. (2013). Game theory meets network security and privacy. *ACM Computing Surveys (CSUR)*, 45(3):25.

McCole, P., Ramsey, E., and Williams, J. (2010). Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns. *Journal of Business Research*, 63(9-10):1018–1024.

Montes, R., Sand-Zantman, W., and Valletti, T. (2018). The value of personal information in online markets with endogenous privacy. *Management Science*.

Moody, D. and Walsh, P. (1999). Measuring The Value Of Information: An Asset Valuation Approach. *Seventh Eur. Conf. Inf. Syst.*, pages 1–17.

Nagurney, A. and Nagurney, L. S. (2015). A game theory model of cybersecurity investments with information asymmetry. *NETNOMICS: Economic Research and Electronic Networking*, 16(1-2):127–148.

Ofek, E., Katona, Z., and Sarvary, M. (2011). "Bricks and Clicks": The Impact of Product Returns on the Strategies of Multichannel Retailers. *Mark. Sci.*, 30(1):42–60.

Olejnik, L., Castelluccia, C., and Janc, A. (2014). On the uniqueness of Web browsing history patterns. *Ann. des Telecommun. Telecommun.*, 69(1-2):63–74.

Peitz, M. and Waldfogel, J. (2012). *The Oxford handbook of the digital economy*. Oxford University Press.

Sarvary, M. and Parker, P. M. (1997). Marketing information: A competitive analysis. *Marketing science*, 16(1):24–38.

Schoeman, F. D. (1992). *Privacy and social freedom*. Cambridge university press.

Shy, O. and Stenbacka, R. (2016). Customer privacy and competition. *Journal of Economics & Management Strategy*, 25(3):539–562.

Smith, R. E. (2000). *Ben Franklin's web site: Privacy and curiosity from Plymouth Rock to the Internet*. Privacy Journal.

Solove, D. J. A taxonomy of privacy'(2006). *University of Pennsylvania law review*, 154(3).

Spiekermann, S., Korunovska, J., Bauer, C., Spiekermann, S., and Bauer, C. (2012). Psychology of ownership and asset defense: Why people value their personal information beyond privacy. *WP*, (September).

Tapscott, D. (1996). *The digital economy: Promise and peril in the age of networked intelligence*, volume 1. McGraw-Hill New York.

Taylor, C. (2004a). Privacy and Information Acquisition in Competitive Markets. *Law Econ. Work.*, (November).

Taylor, C. and Wagman, L. (2014). Consumer privacy in oligopolistic markets: Winners, losers, and welfare. *Int. J. Ind. Organ.*, 34(MAY 2014):80–84.

Taylor, C. R. (2004b). Consumer Privacy and the Market for Customer Information customer information. *RAND J. Econ.*, 35(4):631–650.

Urbano, A. (2018). 17. learning in markets. *Handbook of Game Theory and Industrial Organization, Volume I*, 1:486.

Valletti, T. M. and Wu, J. (2016). Consumer profiling with data requirements. *Available at SSRN 2760276*.

Varian, H. (2004). System reliability and free riding. In *Economics of information security*, pages 1–15. Springer.

Villas-Boas, J. M. (2004). Price cycles in markets with customer recognition. *RAND Journal of Economics*, pages 486–501.

Villas-Boas, J. M. (2014). Price Cycles in Markets with Customer Recognition. *RAND J. Econ.*, 35(3):486–501.

Weishäupl, E., Yasasin, E., and Schryen, G. (2018). Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. *Computers and Security*, 00:1–17.

Westin, A. F. and Ruebhausen, O. M. (1967). *Privacy and freedom*, volume 1. Atheneum New York.

Wolk, A. and Ebling, C. (2010). Multi-channel price differentiation: An empirical investigation of existence and causes. *Int. J. Res. Mark.*, 27(2):142–150.

Xiang, Y. and Sarvary, M. (2013). Buying and selling information under competition. *Quantitative Marketing and Economics*, 11(3):321–351.

Xiao, T., Choi, T. M., and Cheng, T. C. E. (2014). Product variety and channel structure strategy for a retailer-Stackelberg supply chain. *Eur. J. Oper. Res.*, 233(1):114–124.